Universidade Federal de Santa Catarina
Curso de Pós-Graduação em Matemática e
Computação Científica

Teoria Algébrica de Números, Extenções Ciclotômicas e o Último Teorema de Fermat: a demonstração de E. Kummer

Erwin Lavallière Torreão Dassen
Orientador: Oscar Ricardo Janesch

Florianópolis
Fevereiro de 2005

Universidade Federal de Santa Catarina
Curso de Pós-Graduação em Matemática e
Computação Científica

Teoria Algébrica de Números, Extenções Ciclotômicas e o Último Teorema de Fermat: a demonstração de E. Kummer

Dissertação apresentada ao Curso de Pós-Graduação em Matemática e Computação Científica, do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina, para a obtenção do grau de Mestre em Matemática com Área de Concentração Honors Magister em Álgebra.

Erwin Lavallière Torreão Dassen
Florianópolis
Fevereiro de 2005

Teoria Algébrica de Números, Extenções Ciclotômicas e o Último Teorema de Fermat: a demonstração de E. Kummer

por

Erwin Lavallière Torreão Dassen

Esta Dissertação foi julgada para a obtenção do Título de "Mestre", Área de Concentração Honors Magister em Álgebra, e aprovada em sua forma final pelo Curso de Pós-Graduação em Matemática e Computação Científica.

Igor E. Mozolevski
Coordenador

Comissão Examinadora

Prof. Dr. Oscar Ricardo Janesch (UFSC-Orientador)

Prof. Dr. Miguel Ferrero (UFRGS)

Prof. Dr. Eliezer Batista (UFSC)

Florianópolis, fevereiro de 2005.

Ao meu pai Gerardus, minha inspiração, (in memoriam).
À minha mãe Laura, minha força.
Ao meu irmão Eric meu apoio.
À minha namorada Juliana, meu amor.

AGRADECIMENTOS

Aos meus amigos Fernando Mortari e Gilles Gonçalves de Castro que sofreram comigo durante todos esses anos.

Aos meus professores Eliezer Batista e Ruy Exel por me mostrarem quais são os padrões que devo procurar atingir como professor e matemático.

Ao meu professor Paulo Henrique Viana de Barros (in memorian) por me introduzir ao fantástico mundo da teoria dos números.

Ao Conselho Nacional de Desenvolvimento Científico e Tecnológico pelo custeio parcial dos estudos.

Aos inúmeros técnicos e funcionários que de uma forma ou de outra ajudaram como puderam.

Sumário

Resumo

O Último Teorema de Fermat consiste da afirmação de que não existe solução inteira para a equação $a^n + b^n = c^n$ nas icógnitas a, b, c e para qualquer natural $n \geq 3$. A demonstração desta conjectura permaneceu uma inspeção caso a caso até que Kummer forneceu a primeira demonstração para uma classe de primos. Apesar de não se saber se existem uma infinidade de primos nesta classe (conhecida como os primos regulares) este foi o melhor resultado até que Wiles em 1995, respondeu a questão completamente utilizando a teoria das curvas elípticas. A matemática involvida no resultado de Kummer é tão importante e bonita que nos propomos, neste trabalho, a mostrar este resultado bem como construir a teoria necessária.

Abstract

Fermat Last Theorem is the assertion that there is no integer solution to the equation $a^n + b^n = c^n$ in the unknowns a, b, c and for any natural $n \geq 3$. This conjecture remained a case by case inspection until Kummer provided the first proof for a class of primes. Although it is not known if there are infinitely many primes in this class (known as the regular primes), this was by far the best result until Wiles, in 1995, answered the complete question using the theory of elliptic curves. The mathematics involved in Kummer's result is so important and beautiful that we intend, in this work, to show this result while also constructing the necessary theory.

Introdução

A teoria de números é a área da matemática que trata do estudo dos inteiros. Como sempre, resumir um campo inteiro da matemática em uma simples sentença é enganoso. Sendo tão velha quanto a geometria euclidiana, a teoria de números é ao contrário da primeira, uma área excepcionalmente ativa. Muitos dos seus problemas, novos e antigos, permanecem distantes de uma solução. Um aspecto cativante da teoria é o paradoxo entre a simplicidade de seus enunciados e a complexidade de suas demonstrações. O próprio Gauss considerava esta área a rainha da matemática.

Neste trabalho, tentaremos comprovar o parágrafo acima. Queremos demonstrar uma solução parcial[1] de uma conjectura de enunciado incrivelmente simples devida a Fermat[2]:

CONJECTURA. *Dado n um natural maior que 2, não existe solução no domínio dos inteiros para a equação*

$$X^n + Y^n = Z^n.$$

Observe que para $n = 2$ temos as infinitas ternas pitagóricas como solução. A idéia que essa simples generalização da equação não admite solução é realmente instigante e os meios de sua demonstração abismantes.

Esta conjectura ficou conhecida como o último teorema de Fermat e só foi resolvida em sua totalidade por A. Wiles em 1995. Como dito antes, vamos apresentar uma solução parcial, devida a E. Kummer, no século XIX, que foi a melhor solução obtida até a dada por Wiles. Mesmo esta solução parcial, em conjunto com resultados anteriores e contemporâneos de matemáticos como Gauss, Dirichlet, Dedekind, Liouville e Laplace motivou um dos maiores desenvolvimentos na área da teoria dos números: a teoria algébrica de números. No campo mais abrangente da álgebra, suas idéias foram sentidas e generalizadas a ponto de, no início do século XX, uma ponte ter sido estabelecia entre a teoria algébrica de números e a geometria algébrica de curvas via o que hoje é denominado Product Formula Fields, o que seria melhor traduzido para Corpos com a Fórmula Produto.

O título deste trabalho resume o caminho que seguiremos. Na primeira parte vamos expor a teoria algébrica de números em sua ampla generalidade, visto que muito entendimento das conexões existentes entre os diversos conceitos se ganha quando removemos

[1] O quão parcial se tornará preciso no último capítulo.

[2] Fermat advogava que ele tinha uma demonstração geral para a conjectura apesar de só ter publicado um caso muito restrito. Hoje em dia, acredita-se que sua prova estava simplesmente errada.

as distrações dos casos particulares. É claro que esta não foi a maneira apresentada por Kummer.

Na segunda parte nos concentramos nos chamados corpos numéricos, as extensões finitas dos racionais. Para estas extensões demonstraremos dois resultados fundamentais de finitude. Suas implicações só poderão ser apreciadas posteriormente. No entanto, é bom salientar que estes dois resultados são válidos no contexto geral dos Product Formula Fields.

Na terceira parte nos especializaremos ainda mais: estudaremos as denominadas extensões ciclotômicas dos racionais. Aqui, finalmente, começamos com a matemática de Kummer propriamente dita. Ele estudou estas extensões não essencialmente para demonstrar o último teorema de Fermat, mas com sua teoria ele obteve, entre outros, este incrível resultado exposto no capítulo 7.

O apêndice A trata de um problema um pouco periférico para o que faremos mas que devido a sua importância geral e beleza de resultados não hesitamos em incluir. Trata-se da classificação dos módulos finitamente gerados para domínios mais gerais que os principais, explicitamente, os domínios de Dedekind. Na famosa cadeia de implicações entre os domínios euclidianos, principais, fatoriais e de integridade, vista nos cursos de álgebra, estes situam-se entre os domínios de integridade e os domínios fatoriais.

No restante desta introdução iremos fixar a notação e fazer algumas observações sobre os resultados da teoria de grupos, anéis, módulos e de extensões de corpos que consideramos pré-requisitos. Também pressupomos conhecimento da teoria de Galois para extensões finitas (não necessariamente sobre os racionais).

Neste trabalho os anéis são sempre comutativos com unidade. A menos dito o contrário, A, B, C denotam anéis, K, L corpos e uma relação de inclusão entre eles denota uma extensão da estrutura. Isto é, $A \subseteq B$, $A \subseteq K$ são extensões de anéis, $K \subseteq L$ é uma extensão de corpo e etc..

Quando em uma destas extensões procuramos reservar as letras minúsculas gregas para denotar os elementos da estrutura maior e as letras minúsculas latinas para os elementos da estrutura menor. Seguindo a notação costumeira, os ideais dos anéis serão denotados com o alfabeto gótico. Parênteses ao redor de um subconjunto de um anel denota o ideal gerado por este conjunto e, no caso do conjunto ser unitário, escreveremos apenas o elemento deste conjunto entre os parênteses. Por exemplo, (p) é o ideal gerado por p.

Os símbolos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denotam, respectivamente, o semigrupo dos naturais, o domínio dos inteiros e os corpos racional, real e complexo. Reservamos o símbolo $:=$ para quando temos uma igualdade por definição. Um símbolo $^\times$ em um anel denota o subgrupo dos inversíveis neste anel. Por exemplo: $\mathbb{Z}^\times = \{-1, 1\}$. Também quando escrevermos $a|c$ para elementos de um anel queremos dizer que existe um (único) elemento b do mesmo anel tal que $c = ab$ e lemos "a divide c".

Escrevemos $\gcd(a,b)$, $\mathrm{lcm}(c,d)$ para o máximo divisor comum entre a e b e o mínimo múltiplo comum entre c e d respectivamente. Se A é um domínio denotamos seu corpo de frações por $\mathrm{ff}(A)$. Se $z \in \mathbb{C}$, $\Re(z)$, $\Im(z)$ denotam a parte real e imaginária de z.

A notação $A[X]$ indica a álgebra gerada por A e pela incógnita X. Esta álgebra é a polinomial em uma variável e ela coincide com a álgebra comutativa com coeficiente em A gerada livremente por X. Fica claro o que queremos dizer com $A[X_1, ..., X_n]$.

Sejam $K \subseteq L$ uma extensão de corpos e $\alpha \in L$. Defina a aplicação $\Phi : K[X] \longrightarrow L$ determinada pela correspondência $X \longmapsto \alpha$ (lembremos que $K[X]$ é livremente gerada por X). Pelo primeiro teorema do homomorfismo temos $K[X]/\operatorname{Ker}(\Phi) \cong \operatorname{Im}(\Phi)$. Denotaremos $K[X]/\operatorname{Ker}(\Phi)$ por $K[\alpha]$. Note que como $K[X]$ é domínio principal $\operatorname{Ker}(\Phi)$ é gerado por um único, a menos de multiplicação por elementos de K, polinômio e que se este polinômio é irredutível então $K[\alpha]$ é um subcorpo de L. Neste caso, dizemos que α é algébrico sobre K e denotamos este polinômio (que podemos tomar mônico) por $\operatorname{Irr}(\alpha, K)$.

Seja $f(X) \in K[X]$ irredutível. Dizemos que f é separável quando suas raízes, em uma extensão algebricamente fechada de K, são distintas. É claro que a inseparabilidade de f independe de K, no sentido que se $f(X) \in K'[X]$, onde $K' \subseteq K$, então f é separável com respeito a K' se e somente se é separável com respeito a K. Um elemento $\alpha \in L$, onde L é uma extensão de K, é dito separável se $\operatorname{Irr}(\alpha, K)$ é separável. Dizemos que $K \subseteq L$ é uma extensão separável quando L pode ser gerado por elementos separáveis de L. Está claro o que queremos dizer com polinômios, elementos e extensões inseparáveis. Um corpo K é dito perfeito se só admite extensões separáveis. Mostra-se em [**Rom95**, Seção 4.8, pg.94] que se a característica[3] de K é zero ou K é finito então K é perfeito. De maneira geral, uma extensão finita $K \subseteq L$ decompõe-se de maneira única como $K \subseteq L^s \subseteq L$ onde $K \subseteq L^s$ é maximalmente separável, ou seja, todo elemento de $L - L^s$ é inseparável. Conseqüentemente, $L^s \subseteq L$ é inseparável. Um extensão $K \subseteq L$ é dita puramente inseparável quando $L^s = K$.

Uma seqüência é um diagrama da forma

$$... \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M_{i+1} \longrightarrow ...$$

onde i varia em um conjunto finito ou enumerável de índices I, M_i é um anel, módulo ou álgebra e as flechas são homomorfismos $\phi_i : M_i \to M_{i+1}$ satisfazendo $\operatorname{Im}(\phi_i) \subseteq \operatorname{Ker}(\phi_{i+1})$. Uma seqüência é exata em M_i quando $\operatorname{Im}(\phi_i) = \operatorname{Ker}(\phi_{i+1})$ e a seqüência é dita exata quando é exata em todo M_i. Uma seqüência exata curta é uma seqüência exata do tipo

$$0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} P \longrightarrow 0.$$

Observamos que esta seqüência equivale a dizer que $\operatorname{Im}(\phi) = \operatorname{Ker}(\psi)$ com ϕ injetora e ψ sobrejetora.

[3] O gerador do ideal $\operatorname{Ker}(\iota)$ onde $\iota : \mathbb{Z} \longrightarrow K$ é determinado por $1_{\mathbb{Z}} \longmapsto 1_K$. Como a imagem deste homomorfismo é um subcorpo de K, pelo primeiro teorema do homomorfismo, segue que a característica de K ou é zero ou é um primo $p \in \mathbb{Z}$.

Por fim, vamos rever o conceito de produto tensorial. Dados um A-módulo[4] M e N, o produto tensorial de M e N por A, denotado por $M \otimes_A N$ é o grupo abeliano livre gerado pelos símbolos $m \otimes n$; $m \in M, n \in N$ quocientado pelo subgrupo gerado pelas relações

$$\big(m + m'\big) \otimes n - m \otimes n - m' \otimes n$$

$$m \otimes \big(n + n'\big) - m \otimes n - m \otimes n'$$

$$ma \otimes n - m \otimes an$$

onde $m, m' \in M$, $n, n' \in N$, $a \in A$. Vamos abusar da notação e denotar a classe de $m \otimes n$ por este mesmo símbolo notando que as classes satisfazem

$$\big(m + m'\big) \otimes n = m \otimes n + m' \otimes n$$

$$m \otimes \big(n + n'\big) = m \otimes n + m \otimes n'$$

$$ma \otimes n = m \otimes an.$$

O produto tensorial $M \otimes N$ tem estrutura de A-módulo dada por

$$a(m \otimes n) := (am) \otimes n = (ma) \otimes n = m \otimes (an) = m \otimes (na) =: (m \otimes n)a.$$

Além disso tem-se um isomorfismo canônico $A \otimes_A M \cong M$ dado por $a \otimes m \longmapsto am$.

Dado um par de morfismos de A-módulos $M \xrightarrow{\phi} N$, $P \xrightarrow{\psi} Q$ está definido um único morfismo $\phi \otimes \psi : M \otimes N \longrightarrow P \otimes Q$ tal que nos geradores temos $\phi \otimes \psi(m \otimes n) = \phi(m) \otimes \psi(n)$. Com esta definição de morfismo induzido mostra-se que o produto tensorial é exato à direita, isto é, se

$$N \xrightarrow{\phi} P \xrightarrow{\psi} Q \longrightarrow 0$$

é uma seqüência exata de A-módulos então para todo A-módulo T tem-se que

$$N \otimes T \xrightarrow{1_T \otimes \phi} P \otimes T \xrightarrow{1_T \otimes \psi} Q \otimes T \longrightarrow 0$$

onde 1_T denota a identidade em T, é exata.

Seja $\mathfrak{a}$ um ideal de A e considere a seguinte seqüência exata curta formada com a inclusão e a aplicação quociente:

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow \frac{A}{\mathfrak{a}} \longrightarrow 0.$$

Pelo discutido acima temos que

$$\mathfrak{a} \otimes M \longrightarrow M \longrightarrow \frac{A}{\mathfrak{a}} \otimes M \longrightarrow 0$$

é exata. A primeira flecha é o homomorfismo $a \otimes m \longmapsto am$ de forma que a imagem de $\mathfrak{a} \otimes M$ em M é o módulo gerado pelo conjunto $\{am : a \in \mathfrak{a}, m \in M\}$ denotado por $\mathfrak{a}M$.

[4]Como no nosso caso A é sempre comutativo, nossos A-módulos são em realidade A-A-bimódulos. Sendo assim, podemos ignorar a questão de lateralidade de nossos módulos.

Com isso temos o seguinte isomorfismo:

$$\frac{A}{\mathfrak{a}} \otimes M \cong \frac{M}{\mathfrak{a}M}. \tag{0.0.1}$$

Parte 1

Sobre a Teoria Algébrica de Números

Como dito na introdução, começamos nosso trabalho expondo a teoria algébrica de números. No primeiro capítulo vamos estudar algumas propriedades dos anéis de inteiros. No segundo capítulo pausamos para estudar, em abstrato o conceito de domínio de Dedekind e deduzimos as suas principais propriedades incluindo a fatorização única de ideais. Ainda no final ligamos os dois capítulos mostrando que os anéis de inteiros são exemplos de domínios de Dedekind.

CAPíTULO 1

Anéis de inteiros

Começaremos nosso estudo generalizando a idéia de inteiros. Isto é, dada uma extensão $K \geq \mathbb{Q}$ finita iremos definir o que são os inteiros de K. É sabido que $K = \mathbb{Q}[\alpha]$ para algum $\alpha \in K$, mas veremos que a definição correta de inteiros não corresponde necessariamente ao anel $\mathbb{Z}[\alpha]$. Ainda nesta seção construiremos o discriminante de uma extensão que será um invariante importante para a teoria que segue.

1.1. Definição e propriedades

DEFINIÇÃO 1.1.1. Sejam A um domínio (de integridade) e L um corpo contendo A. Dizemos que um elemento $\alpha \in L$ é inteiro sobre A se e somente se é raiz de um polinômio mônico com coeficientes em A. Isto é, satisfaz uma equação do tipo:

$$\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0 \ ; \ a_i \in A, \ \forall i. \tag{1.1.1}$$

Um polinômio $P(X_1, X_2, ..., X_n) \in A[X_1, X_2, ..., X_n]$ é dito simétrico (nas suas variáveis) se e somente se

$$P(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)}) = P(X_1, X_2, ..., X_n), \ \forall \sigma \in S_n. \tag{1.1.2}$$

Os polinômios $S_k := \sum_{i_1<i_2<...<i_k} X_{i_1}X_{i_2}...X_{i_k}$; $1 \leq k \leq n$ são simétricos e denominados polinômio simétricos elementares.

THEOREM 1.1.2. *(Teorema Função Simétrica) Sejam A um anel e $P(X_1, X_2, ..., X_n)$ um polinômio simétrico. Então P é um polinômio com variáveis nos polinômio simétricos elementares. Isto é, $P \in A[S_1, ..., S_n]$.*

DEMONSTRAÇÃO. Defina a seguinte ordem total nos monômios de $A[X_1, ..., X_n]$:

$$X_1^{i_1}X_2^{i_2}...X_n^{i_n} > X_1^{j_1}X_2^{j_2}...X_n^{j_n}$$

se $\sum_{k=1}^n i_k > \sum_{l=1}^n j_l$ ou, no caso de igualdade, temos para algum $s \in \{1, ..., n\}$, $i_k = j_k$ para $k < s$ e $i_s > j_s$. Seja $X_1^{k_1}...X_n^{k_n}$ o maior monômio de P com coeficiente $c \neq 0$. Como P é simétrico ele contém todos os monômios obtidos do acima por permutação das variáveis. Logo devemos ter $k_1 \geq k_2 \geq ... \geq k_n$. É claro que o maior monômio de S_i é $X_1...X_i$ e conseqüentemente, o maior monômio de $S_1^{d_1}...S_n^{d_n}$ é $X_1^{d_1+d_2+...+d_n}X_2^{d_2+...+d_n}...X_n^{d_n}$. Segue que $P(X_1, ..., X_n) - cS_1^{k_1-k_2}S_2^{k_2-k_3}...S_n^{k_n} < P(X_1, ..., X_n)$ (no sentido que o maior monômio do polinômio esquerdo é menor que o maior monômio do direito). Continuando o processo,

eventualmente o grau total diminui e, portanto, depois de uma quantidade finita de passos obtemos uma representação de P como um polinômio em S_i. □

OBSERVAÇÃO 1.1.3. Seja $f(X) = X^n + a_1X^{n-1} + ... + a_n \in A[X]$ e sejam $\alpha_1, ..., \alpha_n$ as raízes de f em algum anel contendo A. Então é claro que $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ neste anel maior. Agora, é fácil ver que $a_1 = -S_1(\alpha_1, ..., \alpha_n)$, $a_2 = S_2(\alpha_1, ..., \alpha_n)$, ..., $a_n = \pm S_n(\alpha_1, ..., \alpha_n)$. Isto demonstra o seguinte corolário.

COROLÁRIO 1.1.4. *Seja $f(X) \in A[X]$ e $\alpha_1, ..., \alpha_n$ as raízes de f em um anel $A' \supset A$. Se $P(X_1, ..., X_n) \in A[X_1, ..., X_n]$ é simétrico então $P(\alpha_1, ..., \alpha_n) \in A$.*

DEMONSTRAÇÃO. Pelo teorema 1.1.2, $P \in A[S_1, ..., S_n]$ e pela observação 1.1.3, $S_i(\alpha_1, ..., \alpha_n) \in A$ donde $P(\alpha_1, ..., \alpha_n) \in A$. □

THEOREM 1.1.5. *Os elementos de $L \supset A$ inteiros sobre A formam um anel.*

DEMONSTRAÇÃO. Sejam $\alpha, \beta \in L$ inteiros sobre A. Vamos mostrar que $\alpha + \beta$ é inteiro sobre A (a prova para $\alpha - \beta, \alpha\beta$ são análogas). Seja Ω um corpo algebricamente fechado contendo L. Por hipótese existem $f(X), g(X)$ polinômio mônicos com coeficientes em A tal que $f(\alpha) = 0, g(\beta) = 0$. Escreva

$$f(X) = \prod_{i=1}^{m}(X - \alpha_i),\ \alpha_i \in \Omega\ ;\ g(X) = \prod_{j=1}^{n}(X - \beta_j),\ \beta_j \in \Omega.$$

Sejam $\gamma_1, ..., \gamma_{mn}$ os números da forma $\alpha_i + \beta_j$. Afirmamos que o polinômio mônico $h(X) := \prod(X - \gamma_{ij})$ possui coeficientes em A, o que provará que $\alpha + \beta$ é inteiro sobre A. Mas de fato, observe que

$$h(X) = \prod(X - \gamma_{\sigma(i)j}),\ \forall \sigma \in S_m$$
$$h(X) = \prod(X - \gamma_{i\tau(j)}),\ \forall \tau \in S_n$$

o que equivale a dizer que os coeficientes de h são simétricos nos α_i e, independentemente, simétricos nos β_j. Assim, se $P(\alpha_1, ..., \alpha_m; \beta_1, ..., \beta_n)$ é um dos coeficientes de h então pelo corolário 1.1.4 $P(X_1, ..., X_m; \beta_1, ..., \beta_n) \in (A[\beta_1, ..., \beta_m])[X_1, ..., X_m]$. Agora, como este último polinômio é simétrico nos β_j, seus coeficientes são pelo teorema da função simétrica, polinômios em $S_k(\beta_1, ..., \beta_n)$, $1 \leq k \leq n$. Pela observação 1.1.3, $S_k(\beta_1, ..., \beta_n) \in A$ donde $P(X_1, ..., X_m; \beta_1, ..., \beta_n) \in A[X_1, ..., X_m]$.Então, novamente, pelo corolário 1.1.4 $P(\alpha_1, ..., \alpha_m; \beta_1, ..., \beta_n) \in A$ como queríamos demonstrar. □

DEFINIÇÃO 1.1.6. O anel do teorema acima é denominado o fecho inteiro de A em L que denotaremos por A_L.

PROPOSIÇÃO 1.1.7. *Seja $K = \mathrm{ff}(A)$ e $L \geq K$ uma extensão. Se $\alpha \in L$ é algébrico sobre K então existe $d \in A$, $d \neq 0$, tal que $d\alpha$ é inteiro sobre A.*

DEMONSTRAÇÃO. Por hipótese α satisfaz uma equação do tipo

$$\alpha^n + a_1\alpha^{n-1} + ... + a_n = 0,\ \alpha_i \in K.$$

Seja d um denominador comum para os a_i de modo que $da_i \in A\,\forall i$. Multiplicando por d^n obtemos

$$(d\alpha)^n + a_1 d(d\alpha)^{n-1} + ... + a_n d^n = 0.$$

Como $a_1 d, ..., a_n d^n \in A$ e $d\alpha$ é raiz deste polinômio mônico, segue o desejado. □

COROLÁRIO 1.1.8. *Seja $K = \mathrm{ff}(A)$ e $L \geq K$ uma extensão algébrica. Então $L = \mathrm{ff}(A_L)$.*

DEMONSTRAÇÃO. Ora, a proposição anterior mostra que todo elemento de L pode ser escrito como β/d, $\beta \in A_L, d \in A$. □

DEFINIÇÃO 1.1.9. Um domínio A é dito integralmente fechado se e somente se o fecho inteiro de A em $K = \mathrm{ff}(A)$ é o próprio A, isto é, $A_L = A$.

PROPOSIÇÃO 1.1.10. *Se A é um domínio de fatoração única então A é integralmente fechado.*

DEMONSTRAÇÃO. Seja $a/b \in \mathrm{ff}(A)$ inteiro sobre A e suponha por absurdo $b \notin A^\times$ (unidades de A). Então existe um irredutível $p \in A$, que é primo pois A é domínio de fatoração única, tal que $p \mid b$ mas $p \nmid a$. Por hipótese, temos

$$\left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + ... + a_n = 0\,;\ a_i \in A\,\forall i \implies a^n + a_1 a^{n-1} b + ... + a_n b^n = 0 \implies p \mid a^n \implies p \mid a$$

o que é absurdo. □

EXEMPLO 1.1.11. O fecho inteiro de $k[S_1, ..., S_n]$ em $k(X_1, ..., X_n)$ é $k[X_1, ..., X_n]$. De fato, seja $f \in k(X_1, ..., X_n)$ inteiro sobre $k[S_1, ..., S_n]$ então f é inteiro sobre $k[X_1, ..., X_n]$ pois $k[X_1, ..., X_n] \supset k[S_1, ..., S_n]$. Como $k[X_1, ..., X_n]$ é domínio de fatoração única ele é integralmente fechado. Agora, como $k(X_1, ..., X_n) = \mathrm{ff}(k[X_1, ..., X_n])$ segue que $f \in k[X_1, ..., X_n]$. Reciprocamente, se $f \in k[X_1, ..., X_n]$ considere o polinômio $\prod_{\sigma \in S_n} (T - f(X_{\sigma(1)}, ..., X_{\sigma(n)}))$ cujos coeficientes, pela observação 1.1.3 são polinômio simétricos elementares nas raízes $f(X_{\sigma(1)}, ..., X_{\sigma(n)})$. Como tomamos todo o S_n no produtório, tais coeficientes são simétricos nas variáveis $X_1, ..., X_n$, portanto, estão em $k[S_1, ..., S_n]$ como queríamos.

PROPOSIÇÃO 1.1.12. *Seja $K = \mathrm{ff}(A)$ e $L \geq K$ uma extensão finita. Suponha que A é integralmente fechado. Então um elemento $\alpha \in L$ é inteiro sobre A se e somente se seu polinômio mínimo sobre K tem coeficientes em A. Isto é,* $\mathrm{Irr}(\alpha, K) \in A[X]$.

DEMONSTRAÇÃO. Assuma que α é inteiro sobre A. Então α satisfaz uma equação do tipo (1.1.1). Seja α' um conjugado de α (raiz do mesmo polinômio mínimo). Por

resultados da teoria de Galois [**Mil98b**, pg.22, Proposição 2.1.(b)] existe um K-isomorfismo $\sigma : K[\alpha] \longrightarrow K[\alpha']$ tal que $\sigma(\alpha) = \alpha'$. Aplicando σ na equação em questão obtemos

$$\left(\alpha'\right)^n + a_1 \left(\alpha'\right)^{n-1} + ... + a_n = 0$$

o que mostra que α' é inteiro sobre A. Ou seja, os conjugados de α são inteiros sobre A. Pelo teorema 1.1.5 e da observação 1.1.3 segue que os coeficientes de $\mathrm{Irr}(\alpha, K)$ são inteiros sobre A. Como $\mathrm{Irr}(\alpha, K) \in K[X]$ e A é integralmente fechado segue que $\mathrm{Irr}(\alpha, K) \in A[X]$. Isto demonstra a ida do teorema. A volta é óbvia. □

Vamos agora colocar os resultados vistos até agora em uma linguagem mais moderna que simplificam os conceitos.

THEOREM 1.1.13. *Seja L um corpo contendo um domínio A. Um elemento $\alpha \in L$ é inteiro sobre A se e somente se existe um A-submódulo M de L, finitamente gerado, não-nulo, tal que $\alpha M \subseteq M$ (na realidade pode-se tomar $M = A[\alpha]$ a A-subálgebra gerada por α).*

DEMONSTRAÇÃO. Para a ida, suponha α satisfazendo (1.1.1). Então o A-submódulo gerado por $1, \alpha, ..., \alpha^{n-1}$ é não-nulo, finitamente gerado e com a propriedade que $\alpha M \subseteq M$. Para a volta, usaremos a regra de Cramer. Seja M um A-submódulo de L como no enunciado e sejam $v_1, ..., v_n$ um conjunto de geradores para M. Da hipótese que $\alpha M \subseteq M$ temos o seguinte sistema linear:

$$\alpha v_i = \sum a_{ij} v_j \quad a_{ij} \in A$$

que podemos reescrever como

$$\begin{aligned} (\alpha - a_{11})v_1 - a_{12}v_2 - a_{13}v_3 - ... &= 0 \\ -a_{21}v_1 + (\alpha - a_{22})v_2 - a_{23}v_3 - ... &= 0 \\ ... &= 0. \end{aligned}$$

Se C é a matriz dos coeficiente do sistema acima, a regra de Cramer nos diz que $\det(C)v_i = 0$, $\forall i$. Como pelo menos um dos v_i é não-nulo e estamos trabalhando em um corpo, segue que $\det(C) = 0$. Expandindo este determinante obtemos uma equação do tipo (1.1.1). □

Com esta nova linguagem podemos, demonstrar de uma maneira diferente, que os elementos inteiros de L sobre A formam um anel. Embora mais elegante, precisaremos posteriormente das técnicas dos polinômios simétricos, principalmente da observação 1.1.3 e, portanto, não podemos favorecer uma demonstração em detrimento da outra.

COROLÁRIO 1.1.14. *O conjunto dos elementos de L inteiros sobre A formam um anel.*

DEMONSTRAÇÃO. Pelo teorema 1.1.13, dados $\alpha, \beta \in L$ inteiros sobre A, existem $M, N \leq L$ A-submódulos, finitamente gerados, não-nulos tal que $\alpha M \subseteq M$, $\beta N \subseteq N$.

O A-submódulo $MN \leq L$ é finitamente gerado, não-nulo, e é fácil ver que $(\alpha\beta)MN \subseteq MN$, $(\alpha \pm \beta)MN \subseteq MN$ donde, pelo mesmo teorema, $\alpha\beta$, $\alpha \pm \beta$ são inteiros sobre A. □

LEMA 1.1.15. *Sejam $A \subseteq B \subseteq C$ anéis. Se B é finitamente gerado como A-módulo e C é finitamente gerado como B-módulo então C é finitamente gerado como A-módulo.*

DEMONSTRAÇÃO. Sejam $\{\beta_1, ..., \beta_m\}$ um conjunto de geradores de B como A-módulo e $\{\gamma_1, ..., \gamma_n\}$ um conjunto de geradores de C como B-módulo. Ora, $\{\beta_i\gamma_j\}$ é um conjunto de geradores de C como A-módulo. □

PROPOSIÇÃO 1.1.16. *Se $B \supseteq A$ é inteiro sobre A (cada elemento de B é inteiro sobre A) e é finitamente gerado como A-álgebra então A é finitamente gerado como A-módulo.*

DEMONSTRAÇÃO. Suponha inicialmente que B é gerado como A-álgebra por um único elemento digamos $B = A[\beta]$. Todo elemento de B é uma soma do tipo

$$c_0 + c_1\beta + c_2\beta^2 + ... + c_N\beta^N,\ c_i \in A, N \in \mathbb{N}$$

usando a fórmula (1.1.1) para β podemos trocar as potências de β maiores que $n-1$ por potências menores de modo que todo elemento de B passa a se escrever como

$$d_0 + d_1\beta + d_2\beta^2 + ... + d_{n-1}\beta^{n-1},\ d_i \in A$$

donde B é gerado como A-módulo por $\{1, \beta, ..., \beta^{n-1}\}$. No caso geral, suponha que $\{\beta_1, .., \beta_m\}$ geram B como A-álgebra. Considere a cadeia

$$A \subseteq A[\beta_1] \subseteq A[\beta_1, \beta_2] \subseteq ... \subseteq A[\beta_1, .., \beta_m] = B.$$

Vimos que $A[\beta_1]$ é finitamente gerado como A-módulo. Como $A[\beta_1, \beta_2] = (A[\beta_1])[\beta_2]$ e β_2 é inteiro sobre $A[\beta_1]$ (pois é inteiro sobre A) o mesmo raciocínio conclui que $A[\beta_1, \beta_2]$ é finitamente gerado como $A[\beta_1]$-módulo. Pelo lema anterior $A[\beta_1, \beta_2]$ é finitamente gerado como A-módulo. continuando assim, concluímos que B é finitamente gerado como A-módulo. □

PROPOSIÇÃO 1.1.17. *Sejam $A \subseteq B \subseteq C$ domínios tais que B é inteiro sobre A e C é inteiro sobre B então C é inteiro sobre A.*

DEMONSTRAÇÃO. Seja $\gamma \in C$. Por hipótese γ satisfaz:

$$\gamma^n + b_1\gamma^{n-1} + ... + b_n = 0\ ;\ b_i \in B\ \forall i.$$

Seja $B' = A[b_1, ..., b_n]$. Pela proposição 1.1.16 temos que B'é finitamente gerado como A-módulo. Além disso, γ é inteiro sobre B' donde $B'[\gamma]$ é finitamente gerado como A-módulo. Como $\gamma B'[\gamma] \subseteq B'[\gamma]$ segue que γ é inteiro sobre A. □

COROLÁRIO 1.1.18. *O fecho inteiro de A em uma extensão algébrica $L \geq \mathrm{ff}(A)$ é integralmente fechado. Isto é $(A_L)_L = A_L$.*

DEMONSTRAÇÃO. Sabemos do corolário 1.1.8 que $L = \mathrm{ff}(A_L)$. Se $\gamma \in L$ é inteiro sobre A_L então a proposição anterior mostra que γ é inteiro sobre A donde $\gamma \in A_L$. □

1.2. Traços e normas

DEFINIÇÃO 1.2.1. Sejam $A \subseteq B$ anéis com B um A-módulo livre de posto n. Para cada $b \in B$ temos a aplicação A-linear $x \longmapsto bx$ que fixada uma base de B sobre A pode ser representada por uma matriz $(a_{ij}) \in M_n(A)$. Definimos o traço e a norma de b na extensão $B \geq A$ como sendo o traço e a norma (determinante) desta matriz[1]. Isto é, $\mathrm{Tr}_{B/A}\, b := \sum a_{ii} \in A$, $\mathrm{Nm}_{B/A}\, b := \det(a_{ij}) \in A$.

OBSERVAÇÃO 1.2.2. É fácil ver que o traço é uma aplicação A-linear e tal que $\mathrm{Tr}_{B/A}\, 1 = n$ (posto de B sobre A). Também mostra-se facilmente que $\mathrm{Nm}_{B/A} : (B^\times, .) \longrightarrow (A^\times, .)$ é homomorfismo de grupos. Além disso temos as seguintes propriedades de transitividade: se $C \geq B \geq A$ são extensões de anéis então dado $c \in C$ vale que $\mathrm{Tr}_{C/A}\, c = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}\, c)$ e $\mathrm{Nm}_{C/A}\, c = \mathrm{Nm}_{B/A}(\mathrm{Nm}_{C/B}\, c)$.

PROPOSIÇÃO 1.2.3. *Seja $K \leq L$ uma extensão de corpo finita de grau n e seja $\beta \in L$. Seja $f(X)$ o polinômio mínimo de β sobre K e sejam $\beta_1 = \beta, \beta_2, ..., \beta_m$ as raízes de $f(X)$. Então*

$$\mathrm{Tr}_{L/K}\, \beta = r\left(\sum_{i=1}^{m} \beta_i\right) \ , \ \mathrm{Nm}_{L/K}\, \beta = \left(\prod_{i=1}^{m} \beta_i\right)^r$$

onde $r = [L : K[\beta]] = n/m$.

DEMONSTRAÇÃO. Suponha inicialmente $L = K[\beta]$ ($r = 1$, $n = m$). Se $f(X) = \prod(X - \beta_i) = X^n + a_1X^{n-1} + ... + a_n$, é fácil ver que a matriz da aplicação $x \longmapsto \beta x$ em relação a base $\{1, \beta, ..., \beta^{m-1}\}$ é da forma

$$M = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & 0 & ... \\ 0 & 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & ... & -a_1 \end{pmatrix}$$

donde fica claro que

$$\mathrm{Tr}_{L/K}\, \beta = -a_1 = \sum \beta_i$$

e

$$\mathrm{Nm}_{L/K}\, \beta = \det(M) = (-1)^{n+1}(-a_n) \det I_{n-1} = (-1)^{n+2}a_n = (-1)^n\left((-1)^n \prod \beta_i\right) = \prod \beta_i.$$

No caso geral basta usar a observação 1.2.2 nas extensões $L \geq K[\beta] \geq K$. □

[1] Lembremos que o traço e a norma são invariantes da transformação.

COROLÁRIO 1.2.4. *Seja $L \geq K$ uma extensão separável de grau n e seja $\sigma = \{\sigma_1, ..., \sigma_n\}$ o conjunto de K-homomorfismos de L em $\Omega \geq L$, onde Ω é alguma extensão Galoisiana de L. Então dado $\beta \in L$ tem-se* $\mathrm{Tr}_{L/K}\,\beta = \sum \sigma_i(\beta)$ *e* $\mathrm{Nm}_{L/K}\,\beta = \prod \sigma_i(\beta)$.

DEMONSTRAÇÃO. Dado $\beta \in L$ temos a cadeia $K \leq K[\beta] \leq L$ de extensões separáveis. Além disso $r = [L : K[\beta]] \mid n$. De **[Mil98b**, pg.33, Teorema 3.16] temos que se $\{\tau_1, ..., \tau_m\}$ são os K-homomorfismos de $K[\beta]$ em Ω então $m = n/r$ e os conjuntos $\widetilde{\tau_i} := \{\sigma_j : \sigma_j \mid_{K[\beta]} = \tau_i\}$, $1 \leq i \leq m$ formam uma partição de σ tal que $\#\widetilde{\tau_i} = r$, $\forall i$. Assim, pela proposição 1.2.3,

$$\mathrm{Tr}_{L/K}\,\beta = r\left(\sum_{i=1}^{m}\beta_i\right) = \sum_{i=1}^{m}\sum_{j=1}^{r}\beta_i = \sum_{i=1}^{m}\sum_{j=1}^{r}\tau_i(\beta) = \sum_{i=1}^{m}\sum_{\sigma_j\in\widetilde{\tau_i}}\sigma_j(\beta) = \sum_{i=1}^{n}\sigma_i(\beta)$$

e analogamente vê-se que $\mathrm{Nm}_{L/K}\,\beta = \prod \sigma_i(\beta)$. □

COROLÁRIO 1.2.5. *Seja A um domínio integralmente fechado e seja L uma extensão finita de $K = \mathrm{ff}(A)$. Se $\beta \in L$ é inteiro sobre A então* $\mathrm{Tr}_{L/K}\,\beta$, $\mathrm{Nm}_{L/K}\,\beta \in A$.

DEMONSTRAÇÃO. Se β é inteiro sobre A então seus conjugados também são (raízes do mesmo polinômio mínimo). Da proposição 1.2.3 e da observação 1.1.3 temos diretamente o resultado. Alternativamente, basta observar a demonstração da proposição mencionada onde mostramos que o traço e a norma são coeficientes do polinômio mínimo de β. □

1.3. Discriminante de uma extensão

DEFINIÇÃO 1.3.1. Seja M um A-módulo. Uma forma bilinear sobre M é uma aplicação $\psi : M \times M \longrightarrow A$ tal que para todo $m \in M$ temos $x \longmapsto \psi(m, x)$, $x \longmapsto \psi(x, m) \in \mathrm{Hom}(M, A)$. Dados elementos $\beta_1, ..., \beta_m \in M$ definimos seu discriminante, denotado por $\mathrm{D}_\psi(\beta_1, ..., \beta_m)$, como sendo o determinante $\det((\psi(\beta_i, \beta_j))_{ij}) \in A$. Quando M é livre de posto m, o discriminante de ψ em relação à base $e = \{e_i\}$ denotado por $\mathrm{disc}_e(\psi)$ é definido como sendo o discriminante $\mathrm{D}(e_1, ..., e_m)$.

Quando não houver risco de confusão, denotaremos o discriminante D_ψ apenas por D.

LEMA 1.3.2. *Nas condições da definição acima, se $\gamma_i = \sum a_{ij}\beta_j$, $a_{ij} \in A\ \forall i, j$ então* $\mathrm{D}(\gamma_1, ..., \gamma_m) = \det(a_{ij})^2\,\mathrm{D}(\beta_1, ..., \beta_m)$.

DEMONSTRAÇÃO. Diretamente da definição temos

$$\begin{aligned}\mathrm{D}(\gamma_1, ..., \gamma_m) = \det((\psi(\gamma_i, \gamma_j))_{ij}) &= \det\left(\psi\left(\sum_k a_{ik}\beta_k, \sum_l a_{jl}\beta_l\right)\right) = \\ &= \det\left(\sum_{k,l} a_{ik}\psi\left(\beta_k, \beta_l\right)a_{jl}\right) = \det\left((a_{ik})\,\psi(\beta_k, \beta_l)(a_{lj})^T\right) = \\ &= \det(a_{ij})^2\det((\psi(\beta_k, \beta_l))_{kl}) = \det(a_{ij})^2\,\mathrm{D}(\beta_1, ..., \beta_m).\end{aligned}$$

□

Dada $B \geq A$ uma extensão de anéis, a aplicação $(\alpha, \beta) \longmapsto \mathrm{Tr}_{B/A}(\alpha\beta)$ é uma forma bilinear em B. É sabido que se B é livre de posto m e $\{e_i\}$ e $\{f_j\}$ são bases de B sobre A então a mudança de base é dada por uma matriz (a_{ij}) tal que $\det(a_{ij}) \in A^\times$. Definindo em A a relação de equivalência $a \sim b \iff \exists u \in A^\times : a = u^2 b$, é fácil ver que o conjunto $A/\sim$ é um semigrupo com o produto $(\overline{a}, \overline{b}) \longmapsto \overline{ab}$. O lema acima nos permite fazer a seguinte definição:

A partir de agora, salvo dito em contrário, estaremos sempre nos referindo ao discriminante em relação à forma bilinear Tr.

DEFINIÇÃO 1.3.3. Seja $B \geq A$ uma extensão de anéis tal que B é um A-módulo livre de posto m. O discriminante desta extensão, que denotamos por $\mathrm{disc}(B/A)$, é o elemento de $A/\sim$ representado pelo discriminante $\mathrm{disc}_e(\mathrm{Tr}_{B/A})$ onde $e = \{e_i\}$ é uma base qualquer de B sobre A.

PROPOSIÇÃO 1.3.4. *Sejam $A \leq B$ domínios e suponha que B é um A-módulo livre de posto m e que* $\mathrm{disc}(B/A) \neq 0$. *Então um conjunto $\{\gamma_1, ..., \gamma_m\} \subset B$ forma uma base para B sobre A se e somente se* $(\mathrm{D}(\gamma_1, ..., \gamma_m)) = (\mathrm{disc}(B/A))$ *(como ideais de A)*[2].

DEMONSTRAÇÃO. Seja $\{\beta_1, ..., \beta_m\}$ uma base de B sobre A. Pelo lema anterior,

$$\mathrm{D}(\gamma_1, ..., \gamma_m) = \det(a_{ij})^2 \, \mathrm{D}(\beta_1, ..., \beta_m)$$

onde (a_{ij}) é a matriz definida por $\gamma_i = \sum a_{ij}\beta_j$. Agora,

$$(\mathrm{D}(\gamma_1, ..., \gamma_m)) = (\mathrm{disc}(B/A)) \iff (\mathrm{D}(\gamma_1, ..., \gamma_m)) = (\mathrm{D}(\beta_1, ..., \beta_m)) \iff$$

$$\iff \det(a_{ij})^2 \in A^\times \iff \det(a_{ij}) \in A^\times \iff B = \bigoplus_{i=1}^{m} A\gamma_i.$$

□

OBSERVAÇÃO 1.3.5. No caso $A = \mathbb{Z}$, temos que $\mathrm{disc}(B/\mathbb{Z})$ é um inteiro pois $(A^\times)^2 = \{1\}$. Neste caso, elementos $\gamma_1, ..., \gamma_m \in B$ geram um submódulo N de índice finito em B se e somente se $\mathrm{D}(\gamma_1, ..., \gamma_m) \neq 0$ e tem-se

$$\mathrm{D}(\gamma_1, ..., \gamma_m) = (B : N)^2 \, \mathrm{disc}(B/\mathbb{Z}). \tag{1.3.1}$$

Basta notar que ambos os lados da equação igualam-se à $\det(a_{ij})^2 \, \mathrm{D}(\beta_1, ..., \beta_m)$ onde $\{\beta_1, ..., \beta_m\}$ é uma base de B sobre $\mathbb{Z}$ e $\gamma_i = \sum a_{ij}\beta_j$ (ver [**Mil98a**, pg.26, Fórmula 2.21]).

Queremos mostrar que no caso em que B é um A-módulo livre de posto finito então o discriminante da extensão é não-nulo. Para isso vejamos um lema conhecido cuja demonstração se encontra em [**Mil98b**, pg.56, Teorema 5.14].

[2]Por definição, $\mathrm{disc}(B/A)$ é um conjunto de elementos que diferem por unidades. Sendo assim, o ideal $(\mathrm{disc}(B/A))$ gerado pelo discriminante é o mesmo que o gerado por qualquer um dos seus elementos, isto é, representantes do discriminante.

LEMA 1.3.6. *(Lema de Dedekind) Sejam G um grupo e Ω um corpo. Então toda família finita, $\sigma_1, ..., \sigma_m : G \longrightarrow \Omega^\times$, de homomorfismos distintos são independentes. Isto é,*

$$\sum c_i\sigma_i = 0 \ , \ c_i \in \Omega \implies c_i = 0 \, \forall i. \ \square$$

PROPOSIÇÃO 1.3.7. *Seja $L \geq K$ uma extensão separável e grau m e $\sigma_1, ..., \sigma_m : L \longrightarrow \Omega$ K-homomorfismos distintos em uma extensão $\Omega \geq L$ Galoisiana. Então dada uma base $\beta_1, ..., \beta_m$ de L sobre K temos:*

$$\mathrm{D}(\beta_1, ..., \beta_m) = \det((\sigma_i(\beta_j))_{ij})^2 \neq 0.$$

DEMONSTRAÇÃO. Pelo corolário 1.2.4 temos

$$\mathrm{D}(\beta_1, ..., \beta_m) = \det((\mathrm{Tr}\, \beta_i\beta_j)_{ij}) = \det\left(\left(\sum_k \sigma_k(\beta_i\beta_j)\right)_{ij}\right) =$$

$$= \det\left(\left(\sum_k \sigma_k(\beta_i)\sigma_k\left(\beta_j\right)\right)_{ij}\right) = \det\left(\left(\sigma_k(\beta_i)\right)_{ik}\left(\sigma_k(\beta_j)\right)_{kj}\right) = \det((\sigma_k(\beta_i))_{ik})^2.$$

Agora suponha que $\det((\sigma_k(\beta_i))_{ki}) = 0$ então existem $c_1, ..., c_m \in \Omega^\times$tal que $\sum_i c_i\sigma_i(\beta_j) = 0 \, \forall j$. Como $\{\beta_j\}$é base temos $\sum_i c_i\sigma_i(\beta) = 0 \, \forall \beta \in L$ o que pelo lema anterior é um absurdo. $\square$

COROLÁRIO 1.3.8. *Seja $K = \mathrm{ff}(A)$ e seja $L \geq K$ separável de grau m. Se A_L é livre de posto m sobre A então* $\mathrm{disc}(A_L/A) \neq 0$.

DEMONSTRAÇÃO. Pela proposição 1.3.7 temos $\mathrm{disc}(L/K) \neq 0$. Agora se $\beta = \{\beta_1, ..., \beta_m\}$ é base deA_L sobre A como A-módulo, então β é base de L sobre K como espaços vetoriais pois vimos que dado $a \in L$ existe $d \in A$ tal que $da \in A_L$ donde $da = \sum c_i\beta_i \iff a = \sum d^{-1}c_i\beta_i$ e segue o afirmado. Logo, $\mathrm{disc}(B/A) \subseteq \mathrm{disc}(L/K)$ (como classes de equivalência em $K/\sim$) e segue o desejado. $\square$

OBSERVAÇÃO 1.3.9. Se $K \leq L$ é finita mas inseparável então $\mathrm{disc}(L/K) = 0$. De fato, suponha inicialmente que a extensão é puramente inseparável, seja m seu grau e seja $\beta \in L$. De resultados conhecidos da teoria das extensões puramente inseparáveis então temos $\mathrm{char}\, K = p$ (primo) e, sendo $\beta_1, ..., \beta_n$ os conjugados de β, tem-se que cada β_i tem multiplicidade p^{k_i}, $k_i \in \mathbb{N}$. Então, da proposição 1.2.3 segue diretamente que $\mathrm{Tr}_{L/K}\, \beta = 0$ donde $\mathrm{disc}(L/K) = 0$. No caso geral, existe K_s corpo tal que $K \leq K_s \leq L$ sendo a primeira extensão separável e a segunda puramente inseparável. Pelo caso anterior e da transitividade do traço segue que, novamente $\mathrm{Tr}_{L/K} \equiv 0$ donde $\mathrm{disc}\,(L/K) = 0$.

Mostraremos a seguir um resultado fundamental: o fecho inteiro de anéis são módulos finitamente gerados.

THEOREM 1.3.10. *Seja A um domínio integralmente fechado. Seja $K = \mathrm{ff}(A)$ e seja B o fecho inteiro de A em uma extensão separável $L \geq K$ de grau m. Então B está*

contido em um A-módulo livre de posto m. Em particular B é finitamente gerado (como A-módulo). Se A é domínio principal então B é módulo livre de posto m.

DEMONSTRAÇÃO. Seja $\{\beta_1, ..., \beta_m\}$ base de L sobre K. Sabemos que existe $d \in A$ tal que $d\beta_i \in B \, \forall i$. Como $\{d\beta_1, ..., d\beta_m\}$ é ainda base de L sobre K. Assuma então $\{\beta_1, ..., \beta_m\} \subset B$. Como a extensão é separável, temos que $(\alpha, \beta) \longmapsto \mathrm{Tr}_{L/K}(\alpha\beta)$ é não-degenerada. Logo, existe uma base dual $\{\gamma_1, ..., \gamma_m\}$ de L sobre K no sentido que $\mathrm{Tr}_{L/K}(\beta_i\gamma_j) = \delta_{ij}$. Afirmamos que

$$A\beta_1 + A\beta_2 + ... + A\beta_m \subseteq B \subseteq A\gamma_1 + A\gamma_2 + ... + A\gamma_m.$$

A primeira inclusão é óbvia. Seja $\beta \in B$ então $\beta = \sum b_j\gamma_j \ , \ b_j \in K$. Vamos mostrar que $b_j \in A \, \forall j$. Ora, $\beta\beta_i \in B$ donde, pelo corolário 1.2.5 $\mathrm{Tr}_{L/K}(\beta\beta_i) \in A$ e temos

$$\mathrm{Tr}_{L/K}(\beta\beta_i) = \mathrm{Tr}_{L/K}\left(\left(\sum_j b_j\gamma_j\right)\beta_i\right) = \sum b_j \,\mathrm{Tr}_{L/K}(\gamma_j\beta_i) = \sum_j b_j\delta_{ij} = b_i$$

e temos o desejado. Por fim, se A é domínio principal, como ele contém e está contido em módulos livres de posto m ele mesmo é livre de posto m. □

COROLÁRIO 1.3.11. *O anel de inteiros de um corpo numérico L que é extensão finita de $\mathbb{Q}$ é seu maior subanel finitamente gerado como $\mathbb{Z}$-módulo.*

DEMONSTRAÇÃO. Pelo teorema 1.3.10, $\mathbb{Z}_K$ é finitamente gerado como $\mathbb{Z}$-módulo. Se B é outro subanel de L finitamente gerado como $\mathbb{Z}$-módulo então pelo teorema 1.1.13, todo elemento de B é inteiro sobre $\mathbb{Z}$ donde $B \subseteq \mathbb{Z}_K$. □

OBSERVAÇÃO 1.3.12. Se A não é principal, um submódulo de um módulo livre não é necessariamente livre. Por exemplo, tome $A = \mathbb{Z}[\sqrt{-5}]$ e os ideais $(2) \subsetneq (2, 1 + \sqrt{-5}) \subsetneq A$ que são A-módulos. O primeiro e o último são livres de posto 1 enquanto o segundo não é pois não é principal.

LEMA 1.3.13. *Sejam A um domínio, $K = \mathrm{ff}(A)$ e $L \geq K$ uma extensão Galoisiana. Então $\mathrm{Aut}_A A_L = \mathrm{Gal}(L/K)$.*

DEMONSTRAÇÃO. Seja $\tau \in \mathrm{Aut}_A A_L$. Como, pelo corolário 1.1.8, $L = \mathrm{ff}(A_L)$ podemos estender, de maneira única, τ para L fazendo $\widetilde{\tau}(\alpha/\beta) := \tau(\alpha)/\tau(\beta)$ de maneira que podemos identificar τ com $\widetilde{\tau} \in \mathrm{Gal}(L/K)$. Reciprocamente, se $\tau \in \mathrm{Gal}(L/K)$ só precisamos mostrar que $\tau|_{A_L}(A_L) = A_L$. Agora vimos que $A_L = \sum A\beta_i$ para uma família $\{\beta_i\}$ finita. Como $\tau(\beta_i) \in A_L$ pois $\tau(\beta_i)$ satisfaz a mesma equação integral, só precisamos mostrar que $\{\tau(\beta_i)\}$ gera A_L. Agora, se $\beta \in A_L$, como $\tau^{-1}(\beta) \in A_L$ temos $\tau^{-1}(\beta) = \sum \alpha_i\beta_i$, $\alpha_i \in A$ donde $\beta = \sum \alpha_i\tau(\beta_i)$ como queríamos. □

DEFINIÇÃO 1.3.14. Seja $K \geq \mathbb{Q}$ uma extensão finita. Uma base para $\mathbb{Z}_K$ como $\mathbb{Z}$-módulo é denominada base integral para $\mathbb{Q}$.

EXEMPLO 1.3.15. Usando a notação do teorema anterior, seja $C = \sum A\beta_i \subseteq B$ com $\{\beta_i\}$ base de L sobre K. Seja $C^* = \{\beta \in L : \mathrm{Tr}_{L/K}(\beta\gamma) \in A \,\forall \gamma \in C\}$. Por linearidade, $\beta \in C^* \iff \mathrm{Tr}_{L/K}(\beta\beta_i) \in A \,\forall i$ e, portanto, $\{\gamma_i\} \subset C^*$, ou seja, $\sum A\gamma_i \subseteq C^*$. Reciprocamente, dado $\beta \in C^*$, como $\{\gamma_i\}$ é base de L sobre K, temos $\beta = \sum c_i\gamma_i,\ c_i \in K$, mas da definição de C^* temos $A \ni \mathrm{Tr}_{L/K}(\beta\beta_j) = \sum c_i \mathrm{Tr}_{L/K}(\gamma_i\beta_j) = c_j$ e segue que $C^* = \sum A\gamma_i$. Portanto,

$$C = \sum A\beta_i \subseteq B \subseteq \sum A\gamma_i = C^*.$$

Suponha agora $A = \mathbb{Z}$ e, portanto, $K = \mathbb{Q}$ e seja $\beta \in L$ um elemento primitivo para a extensão $L \geq \mathbb{Q}$ e $f(X)$ o polinômio mínimo para β. Neste caso, $C = \mathbb{Z}[\beta] = \mathbb{Z}1 + \mathbb{Z}\beta + ... + \mathbb{Z}\beta^{m-1}$. Calculemos C^*. Mostra-se [**Fro91**, pg.128] que $\mathrm{Tr}_{L/K}(\beta^i/f'(\beta)) = 0 \,\forall 0 \leq i \leq m-2$ e $\mathrm{Tr}_{L/K}(\beta^{m-1}/f'(\beta)) = 1$. Assim, $\beta^i/f'(\beta) \in C^*$ e

$$\left(\mathrm{Tr}_{L/K}\left(\frac{\beta^{i+j}}{f'(\beta)}\right)\right)_{ij} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & \diagup & x \\ 1 & x & x \end{pmatrix} = M$$

donde $\det(M) = (-1)^m$. Seja $\{\gamma_i\}$ a base dual à $\{\beta_i\}$ então como $\mathrm{Tr}_{L/K}(\beta^i\gamma_j) = \delta_{ij}$ temos

$$\det(\mathrm{Tr}_{L/K}(\beta^i\gamma_j)_{ij}) = 1.$$

Escreva $\beta^i/f'(\beta) = \sum_j c_{ij}\gamma_j,\ c_{ij} \in A$ e teremos que $\beta^k\beta^i/f'(\beta) = \sum_j c_{ij}\beta^k\gamma_j$ donde

$$\begin{aligned}(-1)^m &= \det\left(\left(\mathrm{Tr}_{L/K}\left(\frac{\beta^k\beta^i}{f'(\beta)}\right)\right)_{ik}\right) = \\ &= \det\left(\left(\mathrm{Tr}_{L/K}\left(\sum_j c_{ij}\beta^k\gamma_j\right)\right)_{ik}\right) = \det\left(\left(\sum_j c_{ij}\,\mathrm{Tr}(\beta^k\gamma_j)\right)_{ik}\right) = \\ &= \det(c_{ij})\det(\left(\mathrm{Tr}_{L/K}(\beta^k\gamma_j)\right)^T_{kj}) = \det(c_{ij}).\end{aligned}$$

Portanto, $(c_{ij}) \in M_m(A)$ e é inversível em A donde $\{\beta^i/f'(\beta)\}$ é base de C^*. Ou seja, temos que

$$C = \mathbb{Z}[\beta] \subseteq \mathbb{Z}_K \subseteq f'(\beta)^{-1}\mathbb{Z}[\beta] = C^*.$$

PROPOSIÇÃO 1.3.16. *Seja K um corpo de característica zero e $L = K[\beta]$ para algum β algébrico sobre K. Seja $f(X)$ o polinômio mínimo de β sobre K e suponha que $f(X) = \prod_{i=1}^m (X - \beta_i)$ em alguma extensão Galoisiana de L. Então,*

$$\mathrm{D}(1, \beta, ..., \beta^{m-1}) = \prod_{1 \leq i < j \leq m} (\beta_i - \beta_j)^2 = (-1)^{\frac{m(m-1)}{2}} \mathrm{Nm}_{L/K}(f'(\beta)). \tag{1.3.2}$$

DEMONSTRAÇÃO. Pela proposição 1.3.7 temos

$$\mathrm{D}(1, \beta, ..., \beta^{m-1}) = \det((\sigma_i(\beta^j))_{ij})^2 = \det((\beta_i^j)_{ij})^2 = \left(\prod_{i<j}(\beta_i - \beta_j)\right)^2 = (*)$$

onde $\{\sigma_i\}$ são os K-homomorfismos distintos de L em Ω (alguma extensão Galoisiana de L) e usamos a fórmula de Vandermonde na última igualdade. Continuando,

$$(*) = (-1)^{\frac{m(m-1)}{2}} \prod_i \left(\prod_{j \neq i} (\beta_i - \beta_j) \right) = (-1)^{\frac{m(m-1)}{2}} \prod_j f'(\beta_j) = (-1)^{\frac{m(m-1)}{2}} \prod_j f'(\sigma_j(\beta)) =$$
$$= (-1)^{\frac{m(m-1)}{2}} \prod_j \sigma_j(f'(\beta)) = (-1)^{\frac{m(m-1)}{2}} \mathrm{Nm}_{L/K}(f'(\beta)).$$

□

OBSERVAÇÃO 1.3.17. O número acima é denominado discriminante do polinômio $f(X)$ que denotamos por $\mathrm{disc}\,(f\,(X))$. Ele pode ser alternativamente definido como o resultante de $f(X)$ e $f'(X)$. Está claro que o discriminante é nulo se e somente se $f(X)$ possui raízes repetidas e que é um polinômio simétrico nas raízes de f com coeficientes em A.

EXEMPLO 1.3.18. Calculemos o discriminante de $f(X) = X^n + aX + b\ ;\ a, b \in K$ que assumimos irredutível e separável. Seja β uma raiz de f e seja $\gamma = f'(\beta) = n\beta^{n-1} + a$. Calculemos $\mathrm{Nm}(\gamma)$. Temos

$$\beta^n + a\beta + b = 0 \implies n\beta^{n-1} = -na - nb\beta^{-1} \implies$$
$$\implies \gamma = -(n-1)a - nb\beta^{-1} \implies \beta = \frac{-nb}{\gamma + (n-1)a}.$$

Logo, $K[\beta] = K[\gamma]$. Em particular, o polinômio mínimo de γ sobre K tem grau n. Escreva

$$f\left(\frac{-nb}{X + (n-1)a}\right) = \frac{P(X)}{Q(X)} \implies \frac{P(\gamma)}{Q(\gamma)} = f(\beta) = 0 \implies P(\gamma) = 0.$$

Agora, depois de uma conta simples obtemos

$$f\left(\frac{-nb}{X + (n-1)a}\right) = \frac{(-1)^n n^n b^{n-1} - na(X + (n-1)a)^{n-1} + (X + (n-1)a)^n}{b^{-1}(X + (n-1)a)^n} \implies$$
$$\implies P(X) = (X + (n-1)a)^n - na(X + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}.$$

Note que P é mônico de grau n donde P é o polinômio mínimo de γ sobre K. Pela proposição 1.2.3, $\mathrm{Nm}(\gamma)$ é o produto das raízes de P e, portanto, $\mathrm{Nm}(\gamma) = (-1)^n a_n$ onde a_n é o coeficiente constante de P. Logo,

$$\mathrm{Nm}(\gamma) = (-1)^n[((n-1)a)^n - na^n(n-1)^{n-1} + (-1)^n n^n b^{n-1}] =$$
$$= n^n b^{n-1} + (-1)^{n-1} a^n (n-1)^{n-1}.$$

Assim, da proposição 1.3.16 obtemos:

$$\mathrm{disc}(f(X)) = (-1)^{\frac{n(n-1)}{2}} (n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n). \tag{1.3.3}$$

OBSERVAÇÃO 1.3.19. A estratégia geral para achar o anel de inteiros $\mathbb{Z}_K$ (K uma extensão finita de $\mathbb{Q}$) é escrever $K = \mathbb{Q}[\alpha]$ com α um inteiro sobre K e calcular $D(1, \alpha, ..., \alpha^{n-1})$. Se este inteiro for livre de quadrado da observação 1.3.5 e da proposição 1.3.4 temos que

$\{1, \alpha, ..., \alpha^{n-1}\}$ é base integral. Caso contrário, $\{1, \alpha, ..., \alpha^{n-1}\}$ pode ainda ser base integral. O próximo resultado nos dá um teste que podemos utilizar.

(1) Seja α raiz de $X^3 - X - 1$ que é irredutível em $\mathbb{Q}$ (pois o é em $\mathbb{Z}$) Da fórmula (1.3.3) obtemos $D(1, \alpha, \alpha^2) = -23$ que é livre de quadrado donde $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ e $\{1, \alpha, \alpha^2\}$ é base integral.

(2) Seja α raiz de $X^3 + X + 1$ que novamente é irredutível e $D(1, \alpha, \alpha^2) = -31$ donde $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

(3) Seja α raiz de $f(X) = X^3 + X^2 - 2X + 8$. Pode-se calcular (usando o Maple por exemplo) que $\text{disc}(f) = -4.503$. Mas mostra-se que $\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$ donde $\text{disc}(\mathbb{Z}_K : \mathbb{Z}) = -503$.

(4) Seja α raiz de $f(X) = X^5 - X - 1$ que é irredutível pois o é em $\mathbb{F}_3[X]$. Temos $\text{disc}(f) = 19.151$ donde novamente $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

PROPOSIÇÃO 1.3.20. *(Critério de Stickelberger) Seja K uma extensão finita de $\mathbb{Q}$. Então:*

(1) *o sinal de* $\text{disc}(K/\mathbb{Q})$ *é* $(-1)^s$ *onde* $2s$ *é o número de homomorfismos* $K \hookrightarrow \mathbb{C}$ *cuja imagem não está contida em* $\mathbb{R}$.

(2) *é válida a equação* $\text{disc}(\mathbb{Z}_K/\mathbb{Z}) \equiv 0, 1 \mod 4$.

DEMONSTRAÇÃO. (1) Seja $K = \mathbb{Q}[\alpha]$ e sejam $\alpha_1, \alpha_2, ..., \alpha_r$ os conjugados reais de α e $\alpha_{r+1}, \overline{\alpha}_{r+1}, ..., \alpha_{r+s}, \overline{\alpha}_{r+s}$ os conjugados complexos (evidentemente α está entre eles). Note primeiramente que $(\alpha_i - \alpha_j)^2 > 0 \forall 1 \leq i < j \leq r$. Olhando para a fórmula (1.3.2) da proposição 1.3.16 vemos que o sinal do discriminante da extensão só depende dos conjugados complexos de α. Mas observe que no produtório, com exceção dos termos da forma $(\alpha_{r+i} - \overline{\alpha}_{r+i})^2$, $1 \leq i \leq s$ os fatores aparecem em pares conjugados de forma que seu produto é um número real positivo. Assim, chegamos à fórmula:

$$\text{sign}(\text{disc}(1, ..., \alpha^{m-1})) = \text{sign}\left(\prod_{1 \leq i \leq s} (\alpha_{r+i} - \overline{\alpha}_{r+i})^2\right) = (-1)^s.$$

(2) Sejam $\sigma_1, ..., \sigma_m$ o conjunto dos $\mathbb{Q}$-homomorfismos de K em Ω (o fecho Galoisiano de K sobre $\mathbb{Q}$) e $\alpha_1, ..., \alpha_m$ uma base integral de $\mathbb{Z}_K$. Decorre da proposição 1.3.7 que $\text{disc}(\mathbb{Z}_K/\mathbb{Z}) = \det((\sigma_i(\alpha_j))_{ij})^2$. Seja P a soma dos termos da expansão do determinante correspondendo as permutações pares e $-N$ a soma dos termos correspondendo as permutações ímpares. Temos então que $\text{disc}(\mathbb{Z}_K/\mathbb{Z}) = (P - N)^2 = (P + N)^2 - 4PN$. Seja agora τ um elemento do grupo de Galois de Ω. Pela linearidade de τ segue que $\tau(\det((\sigma_i(\alpha_j))_{ij})) = \det((\tau(\sigma_i(\alpha_j)))_{ij})$. Mas note que $\tau \circ \sigma_i$ é um $\mathbb{Q}$-homomorfismo de K em Ω donde $\tau \circ \sigma_i = \sigma_k$ para algum k. Assim, τ permuta as linhas da matriz $(\sigma_i(\alpha_j))_{ij}$. Se a permutação for par teremos que $\tau(P) = P$ e $\tau(N) = N$, se a permutação for ímpar teremos $\tau(P) = N$ e $\tau(N) = P$ segue que τ fixa $P + N$ e PN. Como τ é arbitrário segue que $P + N, PN \in \mathbb{Q}$.Como eles são inteiros sobre $\mathbb{Q}$ (pois pela expressão do determinante,

eles são somas e produtos dos elementos inteiros $\sigma_i(\alpha_j))$ temos que $P+N, PN \in \mathbb{Z}$ pois $\mathbb{Z}$ é integralmente fechado. Logo,

$$\operatorname{disc}(\mathbb{Z}_K/\mathbb{Z}) \equiv (P+N)^2 \equiv 0,1 \mod 4.$$

□

EXEMPLO 1.3.21. Considere o corpo $\mathbb{Q}[\sqrt{m}]$ onde m é um inteiro livre de quadrado. Temos que $m \equiv 1,2,3 \mod 4$. Se $m \equiv 2,3 \mod 4$ temos $\mathrm{D}(1,\sqrt{m}) = \operatorname{disc}(X^2-m) = 4m$ pela fórmula (1.3.3). Pelo teorema de Stickelberger e da fórmula da observação 1.3.5 temos que $\operatorname{disc}(\mathbb{Z}_K/\mathbb{Z}) = 4m$ donde $\{1,\sqrt{m}\}$ é base integral de $\mathbb{Z}_K$. Caso $m \equiv 1 \mod 4$ note que $(1+\sqrt{m})/2$ é inteiro e que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[(1+\sqrt{m})/2]$ donde $\mathrm{D}(1,(1+\sqrt{m})/2) = m = \operatorname{disc}(\mathbb{Z}_K : \mathbb{Z})$ pois m é livre de quadrado. Assim, $\{1,(1+\sqrt{m})/2\}$ é base integral.

Para terminarmos esta seção apresentamos um resultado que refina o teorema 1.3.10.

PROPOSIÇÃO 1.3.22. *Seja A um domínio principal com corpo de frações K e seja $B \geq A$ o fecho inteiro de A em $L \geq K$ (uma extensão finita e separável de grau m). Sejam $\beta_1,...,\beta_m$ uma base de L sobre K constituída de elementos de B. Denote $d = \mathrm{D}(\beta_1,...,\beta_m)$. Então*

$$A\beta_1 + ... + A\beta_m \subseteq B \subseteq A\left(\frac{\beta_1}{d}\right) + ... + A\left(\frac{\beta_m}{d}\right).$$

DEMONSTRAÇÃO. Seja $\beta \in B$ e escreva $\beta = x_1\beta_1 + ... + x_m\beta_m$, $x_i \in K$. Denote por $\sigma_1,...,\sigma_m$ os K-homomorfismos distintos de L em uma extensão Galoisiana de L. Aplicando sucessivamente estes homomorfismos na equação obtemos o sistema:

$$\sigma_i\beta = x_1\sigma_i(\beta_1) + ... + x_m\sigma_i(\beta_m) \ , i = 1,...,m.$$

Pela regra de Cramer obtemos $x_i = \gamma_i/\delta$ onde $\delta = \det((\sigma_i\beta_j)_{ij})$ e γ_i é o determinante da mesma matriz mas com a i-ésima coluna trocada por $(\sigma_i(\beta))_i$. Da proposição 1.3.7 temos $\delta^2 = d$ donde

$$x_i = \gamma_i\delta/d \implies \gamma_i\delta = dx_i \in K$$

e ele é inteiro sobre A pois γ_i e δ tem expressão em temos de somas de produtos de elementos inteiros. Logo, $\gamma_i\delta \in A$ donde segue o desejado. □

CAPíTULO 2

Domínios de Dedekind

Nesta seção vamos definir o que são domínios de Dedekind, nosso principal objeto de estudo. Vamos demonstrar algumas de suas propriedades, entre elas a de que seus ideais se fatoram de maneira única. Como conseqüência, depois de generalizar o conceito de ideal para ideal fracionário, veremos que em um domínio de Dedekind, os ideais fracionários formam um grupo. Definiremos então o conceito fundamental que é o grupo de classes como sendo um quociente do grupo dos ideais fracionários. Por fim, veremos que os anéis de inteiros discutidos no capítulo anterior são domínios de Dedekind.

2.1. Anéis locais e localização

Esta primeira seção tem um caráter mais técnico no sentido que vamos introduzir uma ferramenta poderosa: o conceito de localização. Sua importância se tornará evidente no decorrer do capítulo.

DEFINIÇÃO 2.1.1. Um anel A é dito local se e somente se ele possui exatamente um ideal maximal $\mathfrak{m}$. Como todo ideal próprio está contido em um ideal maximal segue que neste caso $A^\times = A\backslash\mathfrak{m}$.

DEFINIÇÃO 2.1.2. Um sistema multiplicativo em um domínio A é um subconjunto $S \subseteq A$ tal que $0 \notin S$, $1 \in S$ e $ab \in S$, $\forall a, b \in S$. Neste caso definimos $S^{-1}A := \{a/b \in \mathrm{ff}(A) : b \in S\}$ que é obviamente um subanel de $\mathrm{ff}(A)$.

(1) Seja $t \in A$, A domínio, $t \neq 0$, e defina $S_t := \{1, t, t^2, ...\}$ que é um sistema multiplicativo em A. Neste caso costuma-se escrever A_t para $S_t^{-1}A = \{a/t^n \in \mathrm{ff}(A) : a \in A, n \in \mathbb{N}\}$.
(2) Se $\mathfrak{p}$ é um ideal primo de A então $S_\mathfrak{p} = A\backslash\mathfrak{p}$ é um sistema multiplicativo em A. Para este tipo de sistema multiplicativo escrevemos $A_\mathfrak{p}$ para $S_\mathfrak{p}^{-1}A$.

PROPOSIÇÃO 2.1.3. *Seja A um domínio e $S \subseteq A$ um sistema multiplicativo. Então as aplicações*

$$\mathfrak{a} \longmapsto S^{-1}\mathfrak{a} := \mathfrak{a}S^{-1}A = \{a/s \in S^{-1}A : a \in \mathfrak{a}\}$$

$$\mathfrak{b} \longmapsto A \cap \mathfrak{b}$$

entre os ideais de A e de $S^{-1}A$ estão bem definidas. Além disso,

$$\mathfrak{a} \in \mathrm{Spec}(A),\ \mathfrak{a} \cap S = \varnothing \implies S^{-1}\mathfrak{a} \in \mathrm{Spec}(S^{-1}A)$$

e

$$\mathfrak{b} \in \mathrm{Spec}(S^{-1}A) \implies A \cap \mathfrak{b} \in \mathrm{Spec}(A)$$

neste caso, estas aplicações constituem bijeções inversas.

DEMONSTRAÇÃO. A primeira parte é evidente, bem como as duas implicações. Verifiquemos a última parte, isto é, se $\mathfrak{p} \in \mathrm{Spec}(A)$ e $\mathfrak{q} \in \mathrm{Spec}(S^{-1}A)$ mostremos que $A \cap (S^{-1}\mathfrak{p}) = \mathfrak{p}$ e $S^{-1}(A \cap \mathfrak{q}) = \mathfrak{q}$.

(1) É claro que $\mathfrak{p} \subseteq A \cap (S^{-1}\mathfrak{p})$. Para a inclusão inversa seja $a/s \in A \cap (S^{-1}\mathfrak{p})$, $a \in \mathfrak{p}, s \in S$ e considere a equação $(a/s)s = a \in \mathfrak{p}$. Como $\mathfrak{p}$ é primo e $s \notin \mathfrak{p}$, pois $\mathfrak{p} \cap S = \varnothing$, segue que $a/s \in \mathfrak{p}$.

(2) Como $A \cap \mathfrak{q} \subseteq \mathfrak{q}$ e $\mathfrak{q}$ é um ideal em $S^{-1}A$ temos que $S^{-1}(A \cap \mathfrak{q}) \subseteq \mathfrak{q}$. Para a inclusão inversa seja $b \in \mathfrak{q}$. Podemos escrever $b = a/s$, $a \in A, s \in S$, então $a = s(a/s) \in A \cap \mathfrak{q}$ donde $b = a/s = (s(a/s))/s \in S^{-1}(A \cap \mathfrak{q})$.

□

EXEMPLO 2.1.4. Se $\mathfrak{p}$ é um ideal primo de A então, pela proposição acima, $A_{\mathfrak{p}}$ é um anel local pois

$$S_{\mathfrak{p}} = A \backslash \mathfrak{p} \implies \mathfrak{p} = A \backslash S_{\mathfrak{p}}$$

donde $\mathfrak{p}$ contem todos os ideais primos disjuntos de $S_{\mathfrak{p}}$.

OBSERVAÇÃO 2.1.5. Observe que no item 2. da proposição acima não foi usado o fato que $\mathfrak{q}$ é primo. Mais precisamente, dado um ideal $\mathfrak{a}$ de A, denote $\mathfrak{a}^e := S^{-1}\mathfrak{a}$ e dado um ideal $\mathfrak{b}$ de $S^{-1}A$, denote $\mathfrak{b}^c := A \cap \mathfrak{b}$ então temos: $\mathfrak{b}^{ce} = \mathfrak{b}$ para todo ideal de $S^{-1}A$ e $\mathfrak{a}^{ec} = \mathfrak{a}$ se $\mathfrak{a}$ é ideal primo de A disjunto de S.

2.2. O teorema chinês do resto

Nesta seção demonstramos um teorema fundamental: o teorema chinês do resto. Ele é usado em todo o trabalho como ferramenta apesar de não ser parte da teoria algébrica de números. O teorema nos dá garantia (sob hipóteses bastante razoáveis) que os sistema lineares de congruência em um anel sempre admitem uma e, essencialmente, única solução.

DEFINIÇÃO 2.2.1. Dois ideais $\mathfrak{a}_1, \mathfrak{a}_2 \subset A$ são ditos relativamente primos se e somente se $\mathfrak{a}_1 + \mathfrak{a}_2 = A$.

THEOREM 2.2.2. *(Teorema Chinês do Resto) Sejam $\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_n$ ideais de um anel A relativamente primos dois à dois. Dados elementos $x_1, x_2, ..., x_n \in A$ existe $x \in A$ que é solução do sistema $x \equiv x_i \pmod{\mathfrak{a}_i}$; $i = 1, ..., n$. Além disso, as demais soluções são dadas por $x + a$, $a \in \cap \mathfrak{a}_i$ e $\cap \mathfrak{a}_i = \prod \mathfrak{a}_i$. Em outras palavra temos a seguinte seqüência exata:*

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow \prod_{i=1}^{n} \frac{A}{\mathfrak{a}_i} \longrightarrow 0 \tag{2.2.1}$$

com $\mathfrak{a} = \cap \mathfrak{a}_i = \prod \mathfrak{a}_i$.

DEMONSTRAÇÃO. Suponha inicialmente que $n = 2$. Como $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, existem elementos $a_i \in \mathfrak{a}_i$ tais que $a_1 + a_2 = 1$. Tome $x = a_1x_2 + a_2x_1$ que tem as propriedades desejadas. No caso geral temos que para todo $i \geq 2$, existem $a_i \in \mathfrak{a}_1$ e $b_i \in \mathfrak{a}_i$ tais que $a_i + b_i = 1$. Agora note que $\mathfrak{a}_1 + \prod_{i\geq 2} \mathfrak{a}_i \ni \prod_{i\geq 2}(a_i + b_i) = 1$ donde $\mathfrak{a}_1 + \prod_{i\geq 2} \mathfrak{a}_i = A$ e aplicando o caso $n = 2$ obtemos um elemento $y_1 \in A$ tal que $y_1 \equiv 1 \mod \mathfrak{a}_1$ e $y_1 \equiv 0 \mod \prod_{i\geq 2} \mathfrak{a}_i$, que implica em $y_1 \equiv 1 \mod \mathfrak{a}_1$ e $y_1 \equiv 0 \mod \mathfrak{a}_i$, $i \geq 2$. Analogamente obtemos elementos $y_2, ..., y_n \in A$ tais que $y_i \equiv 1 \mod \mathfrak{a}_i$ e $y_i \equiv 0 \mod \mathfrak{a}_j$, $j \neq i$. O elemento $x := \sum x_i y_i$ satisfaz as propriedades desejadas. Resta-nos mostrar que $\cap\mathfrak{a}_i = \prod \mathfrak{a}_i$. É claro que $\cap\mathfrak{a}_i \supseteq \prod \mathfrak{a}_i$. No caso de $n = 2$, sendo $a_1 + a_2 = 1$ como antes, dado $c \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ temos $c = a_1c + a_2c \in \mathfrak{a}_1\mathfrak{a}_2$. Supondo o resultado válido para $n - 1$, podemos assumir que $\prod_{i\geq 2} \mathfrak{a}_i = \cap_{i\geq 2}\mathfrak{a}_i$. Vimos acima que $\mathfrak{a}_1$ e $\prod_{i\geq 2} \mathfrak{a}_i$ são primos entre si. Portanto, usando o caso $n = 2$ temos que $\mathfrak{a}_1 \prod_{i\geq 2} \mathfrak{a}_i = \mathfrak{a}_1 \cap \left(\prod_{i\geq 2} \mathfrak{a}_i\right) = \cap\mathfrak{a}_i$. □

COROLÁRIO 2.2.3. *Sejam $\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_n$ ideais de A, dois à dois relativamente primos, e seja M um A-módulo. Então, a seguinte seqüência é exata:*

$$0 \longrightarrow \mathfrak{a}M \longrightarrow M \longrightarrow \prod_{i=1}^{n} \frac{M}{\mathfrak{a}_i M} \longrightarrow 0 \tag{2.2.2}$$

com $\mathfrak{a} = \cap\mathfrak{a}_i = \prod \mathfrak{a}_i$.

DEMONSTRAÇÃO. Temos o isomorfismo $A/\mathfrak{a} \cong \prod A/\mathfrak{a}_i$. Tomando o produto tensorial com M obtemos o isomorfismo $(A/\mathfrak{a}) \otimes_A M \cong (\prod (A/\mathfrak{a}_i)) \otimes_A M \cong \prod ((A/\mathfrak{a}_i) \otimes_A M)$ onde o último isomorfismo vem da distributividade do produto tensorial sobre a soma direta. Usando o isomorfismo $(R/\mathfrak{i}) \otimes_R N \cong N/\mathfrak{i}N$ demonstrado na introdução (0.0.1) para um anel R, um ideal $\mathfrak{i}$ e um R-módulo N temos, por fim, $M/\mathfrak{a}M \cong \prod (M/\mathfrak{a}_i M)$ e o corolário está provado. □

THEOREM 2.2.4. *Sejam L uma extensão finita e separável de K e Ω uma extensão arbitrária de K. Então $L \underset{K}{\otimes} \Omega$ é o produto de uma quantidade finita de extensões separáveis de Ω: $L \underset{K}{\otimes} \Omega = \prod_{i=1}^{n} \Omega_i$. Além disso se α é um elemento primitivo para $K \leq L$ então, um conjugado α_i de α em Ω_i é um elemento primitivo para $\Omega \leq \Omega_i$ e se f e f_i são os polinômios mínimos para α e α_i então $f(X) = \prod_{i=1}^{n} f_i(X)$.*

DEMONSTRAÇÃO. Pelo teorema do elemento primitivo [**Mil98b**, pg.50, Teorema 5.1], temos $L = K[\alpha]$ para algum $\alpha \in L$. Seja $f = \mathrm{Irr}(\alpha, K)$. Isto significa que a aplicação $K[X]/(f(X)) \longrightarrow L$ dada por $\overline{g}(X) \longmapsto g(\alpha)$ é um isomorfismo. Tomando o produto tensorial com Ω, ou seja, estendendo os escalares para Ω, temos $L \otimes_K \Omega \cong (K[X]/(f(X))) \otimes_K \Omega \cong \Omega[X]/(f(X))$. Como L é separável sobre K, $f(X)$ tem raízes distintas donde em $\Omega[X]$, $f(X)$ fatora-se em polinômios mônicos irredutíveis $f(X) = f_1(X)...f_r(X)$ dois à dois primos entre si. Pelo teorema chinês do resto segue que $\Omega[X]/(f(X)) = \prod_{i=1}^{r} \Omega[X]/(f_i(X))$

e basta observar que $\Omega_i := \Omega[X]/(f_i(X))$ é finita e separável de grau igual ao grau de f_i. □

2.3. Anéis de valorização discreta

Esta seção, assim como a primeira, também introduz ferramentas que usaremos na próxima seção.

DEFINIÇÃO 2.3.1. Um anel de valorização discreta é um domínio principal A satisfazendo as seguintes afirmações equivalentes:

(1) A possui exatamente um ideal primo próprio e não-nulo.
(2) A menos de associados, A possui exatamente um elemento primo.
(3) A é local e não é um corpo.

EXEMPLO 2.3.2. $\mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} : p \nmid n\}$ é um anel de valorização discreta com elementos primos $\pm p$ e único ideal primo (p).

OBSERVAÇÃO 2.3.3. Note que em um anel de valorização discreta todo ideal não nulo é da forma (π^m), $m \in \mathbb{N}$ onde π é o único primo (a menos de associados).

PROPOSIÇÃO 2.3.4. *Um domínio de integridade A é um anel de valorização discreta se e somente se:*

(1) *A é Noetheriano*
(2) *A é integralmente fechado.*
(3) *A possui exatamente um ideal primo, próprio e não-nulo.*

DEMONSTRAÇÃO. ($\Longrightarrow$):Os ítens (1) e (3) são evidentes. O item (2) é um caso particular da proposição 1.1.10.

($\Longleftarrow$): Temos que mostrar que A é principal. Por (3) temos que A é local. Seja $c \in A\setminus(A^\times \cup \{0\})$ e considere o A-módulo $M := A/(c)$. Dado $m \in M\setminus\{0\}$ o conjunto $\mathrm{Ann}(m) := \{a \in A : am = 0\}$ é um ideal próprio de A. De (1) segue que o conjunto $\{\mathrm{Ann}(m) : m \in M\setminus\{0\}\}$ possui um elemento maximal $\mathfrak{p}$. Escreva $b + (c)$ para o elemento tal que $\mathrm{Ann}(b + (c)) = \mathfrak{p}$. Note que $c \in \mathfrak{p}$ donde $\mathfrak{p}$ é não-nulo. Note também que $\mathfrak{p} = \{a \in A : c \mid ab\}$.

Afirmamos que $\mathfrak{p}$ é primo (donde de 3. seguirá que $\mathfrak{p}$ é o único ideal maximal de A), senão existiriam $x, y \in A\setminus\mathfrak{p}$ tal que $xy \in \mathfrak{p}$ donde teríamos $yb + (c) \neq 0$ (senão $y \in \mathfrak{p}$) e $\mathrm{Ann}(yb+(c))$ seria um ideal próprio de A tal que $x \in \mathrm{Ann}(yb+(c))$, assim, $\mathfrak{p} \subsetneq \mathrm{Ann}(yb+(c))$ contrariando a maximalidade de $\mathfrak{p}$. Segue o afirmado.

Afirmamos agora que $c/b \in A$ e que $\mathfrak{p} = (c/b)$. Primeiro note que $b/c \notin A$ caso contrário $b = c(b/c) \in (c)$ donde $b + (c) = 0$. Da definição de $\mathfrak{p}$ temos que $\mathfrak{p}b \subseteq (c)$ donde $\mathfrak{p}\frac{b}{c} \subseteq A$. Se tivéssemos $\mathfrak{p}\frac{b}{c} \subseteq \mathfrak{p}$, como $\mathfrak{p}$ é finitamente gerado (por 1.), teríamos pelo teorema 1.1.13 que b/c é inteiro sobre A e por 2. seguiria que $b/c \in A$ o que vimos ser falso. Assim, temos um ideal de A que não está contido em nenhum ideal maximal. Logo, $\mathfrak{p}\frac{b}{c} = A$ donde

$(b/c)^{-1} = c/b \in \mathfrak{p}$ e temos que $(c/b) \subseteq \mathfrak{p}$. Por outro lado, $\mathfrak{p}b \subseteq (c)$ implica $\mathfrak{p} \subseteq (c/b)$ e segue o afirmado.

Denote $\pi = c/b$. Seja agora $\mathfrak{a}$ um ideal próprio e não-nulo de A. Considere a seguinte cadeia de subconjuntos de $\mathrm{ff}(A)$: $\mathfrak{a} \subseteq \mathfrak{a}\pi^{-1} \subseteq \mathfrak{a}\pi^{-2} \subseteq ....$ Note que se $\mathfrak{a}\pi^{-k} \subseteq A$ então este é um ideal de A. Agora, nesta cadeia as inclusões são estritas pois se $\mathfrak{a}\pi^{-k} = \mathfrak{a}\pi^{-(k+1)}$ então do teorema 1.1.13 segue que π^{-1} é inteiro sobre A donde, por 2., $\pi^{-1} \in A$ o que é absurdo. De 1., segue que esta cadeia não está contida em A. Seja $m \in \mathbb{N}$ tal que $\mathfrak{a}\pi^{-m} \subseteq A$ mas $\mathfrak{a}\pi^{-(m+1)} \nsubseteq A$. Segue que $\mathfrak{a}\pi^{-m} \nsubseteq \mathfrak{p} = (\pi)$ (senão $\mathfrak{a}\pi^{-(m+1)} \subseteq A$). Novamente temos um ideal que não está contido em um ideal maximal. Logo, $\mathfrak{a}\pi^{-m} = A$ e dessa igualdade segue que $\mathfrak{a} = (\pi^m)$ como queríamos. □

A seguir vamos definir o útil conceito de valorização discreta e ligá-la ao dos anéis de valorização discreta.

DEFINIÇÃO 2.3.5. Seja K um corpo. Uma valorização discreta em K é um homomorfismo não-nulo $v : K^\times \longrightarrow \mathbb{Z}$ tal que

$$v(a+b) \geq \min(v(a), v(b)),\ \forall a, b \in K.$$

Como v é não-nulo, $v(K)$ é um subgrupo não-nulo de $\mathbb{Z}$ e, portanto, da forma $m\mathbb{Z}$ para algum $m \in \mathbb{Z}$. Se $m = 1$ então v é sobrejetora e a valorização é dita estar normalizada. Caso contrário, $a \longmapsto m^{-1}v(a)$ será uma valorização discreta normalizada.

(1) Seja A um domínio principal e $K = \mathrm{ff}(A)$. Seja π um elemento primo de A. Então todo elemento de $c \in K^\times$ pode ser escrito como $c = \pi^m(a/b)$ com a e b primos com π. Defina $v(c) = m$. Então v é uma valorização discreta normalizada.
(2) Seja A um domínio de Dedekind, $K = \mathrm{ff}(A)$ e $\mathfrak{p}$ um ideal (inteiro) primo de A. Para qualquer $c \in K^\times$ seja $\mathfrak{p}^{v(c)}$ a potência de $\mathfrak{p}$ na fatorização de (c). Então v é uma valorização discreta normalizada.

OBSERVAÇÃO 2.3.6. Nos exemplos acima temos que se $v(a) > v(b)$ então $v(a+b) = v(b)$. Esta é, na realidade, uma propriedade geral das valorizações discretas. Primeiro note que $v(\zeta) = 0$ para todo elemento $\zeta \in K$ de ordem finita pois v é homomorfismo e $\mathbb{Z}$ não possui elementos de ordem finita. Logo, $v(-a) = v(-1) + v(a) = v(a)$ e se $v(a) > v(b)$ temos

$$v(b) = v(a+b-a) \geq \min(v(a+b), v(a)) \geq \min(v(a), v(b)) = v(b) \implies v(a+b) = v(b)$$

pois $\min(v(a+b), v(a)) = v(a+b)$.

O exemplo (1) acima mostra que um anel de valorização discreta gera uma valorização discreta no seu corpo de frações. O resultado seguinte é a recíproca desta afirmação.

THEOREM 2.3.7. *Seja v uma valorização discreta em um corpo K. Então $A := \{a \in K : v(a) \geq 0\}$ é um anel de valorização discreta com ideal maximal $\mathfrak{m} = \{a \in K : v(a) > 0\}$. Sendo $m \in \mathbb{Z}$ tal que $v(K^\times) = m\mathbb{Z}$ tem-se que $\mathfrak{m}$ é gerado por qualquer elemento π tal que $v(\pi) = m$.*

DEMONSTRAÇÃO. Em primeiro lugar, é claro que A é anel e que $\mathfrak{m}$ é ideal de A. Afirmamos que $A^\times = A\backslash\mathfrak{m} = \{a \in K : v(a) = 0\}$. De fato, $A^\times \subseteq A\backslash\mathfrak{m}$ pois as unidades são elementos de ordem finita e v é homomorfismo. Por outro lado, seja $a \in K$ tal que $v(a) = 0$. Então,

$$0 = v(1) = v(aa^{-1}) = v(a) + v(a^{-1}) = v(a^{-1}) \implies a^{-1} \in A \implies a \in A^\times$$

e temos o afirmado. Assim, A é local que não é corpo. Resta-nos mostrar que A é domínio principal. Primeiro vejamos que $\mathfrak{m}$ é maximal. Temos $\varnothing \neq v(\mathfrak{m}) \subseteq \mathbb{N}^*$. Pelo princípio da boa ordem, existe $m \in v(\mathfrak{m})$ mínimo. Seja $a \in \mathfrak{m}$ tal que $v(a) = m$. Afirmamos que $\mathfrak{m} = (a)$. É claro que $\mathfrak{m} \supseteq (a)$. Por outro lado, dado $b \in \mathfrak{m}$ temos que $v(b) = qm + r,\ 0 \leq r < m$. Mas então, $v(ba^{-q}) = r < m$. Se $r = 0$ então

$$ba^{-q} \in A^\times \implies ba^{-q}x = 1,\ x \in A^\times$$

donde

$$b = a^q x^{-1} \implies a \mid b \implies b \in (a).$$

Como $r > 0$ é um absurdo (pois contraria a minimalidade de m) temos o desejado.

Se $\mathfrak{a}$ é um ideal arbitrário de A temos da mesma forma, $\mathfrak{a} = (a')$ para $a' \in \mathfrak{a}$ tal que $v(a') = \min\{v(\mathfrak{a})\}$. De fato, seja tal $a' \in \mathfrak{a}$. Então $(a') \subseteq \mathfrak{a}$ e por outro lado, se $b \in \mathfrak{a}$ temos $v(b) = qv(a') + r,\ 0 \leq r < v(a')$. Assim, $v(ba'^{-q}) = r < v(a')$. Se $r = 0$ segue que $a' \mid b$ donde $b \in (a')$. Se $r > 0$ temos $r = pm + s,\ 0 \leq s < m$. Assim $v(ba'^{-q}a^{-p}) = s < m$, novamente como $s > 0$ é absurdo temos $v(ba'^{-q}a^{-p}) = 0$ donde $ba'^{-q}a^{-p}x = 1,\ x \in A^\times$ donde

$$b = a'^q a^p x^{-1} \implies a' \mid b$$

provando que $b \in (a')$ e o teorema. □

2.4. Domínios de Dedekind

Nesta seção iremos definir o principal objeto de estudo do trabalho: os domínios de Dedekind e vamos mostrar que o anéis de inteiros vistos na seção anterior satisfazem essa nova definição.

Primeiro, uma definição que generaliza para ideais o conceito de primalidade entre elementos e que usaremos muito no decorrer do trabalho.

DEFINIÇÃO 2.4.1. Um domínio de Dedekind é um domínio A, que não é corpo, tal que:

(1) A é Noetheriano.
(2) A é integralmente fechado.
(3) Todo ideal primo próprio e não-nulo de A é maximal.

OBSERVAÇÃO 2.4.2. A Proposição 2.3.4 nos diz que um domínio local é domínio de Dedekind se e somente se ele é um anel de valorização discreta.

PROPOSIÇÃO 2.4.3. *Seja A um domínio de Dedekind e S um sistema multiplicativo em A. Então $S^{-1}A$ ou é um domínio de Dedekind ou um corpo.*

DEMONSTRAÇÃO. Na observação 2.1.5 vimos que se $\mathfrak{a}$ é um ideal em $S^{-1}A$ então $\mathfrak{a} = \mathfrak{a}^{ce}$ donde $\mathfrak{a}$ é gerado por qualquer conjunto de geradores de $\mathfrak{a}^c$. Como A é Noetheriano segue que $S^{-1}A$ o é. Seja agora $\alpha \in \mathrm{ff}(S^{-1}A) = \mathrm{ff}(A)$ inteiro sobre $S^{-1}A$. Então α satisfaz uma equação do integral com coeficientes $a_i \in S^{-1}A,\ 1 \leq i \leq n$, para cada $i \in \{1, ..., n\}$ existe $s_i \in S$ tal que $s_i a_i \in A$. Tome $s = s_1 ... s_n \in S$ e teremos $(s\alpha)^n + sa_1(s\alpha)^{n-1} + ... + s^n a_n = 0$ donde $s\alpha$ é inteiro sobre A. Segue que $s\alpha \in A$ donde $\alpha = s(\alpha/s) \in S^{-1}A$ e $S^{-1}A$ é integralmente fechado. Por fim, a condição 3. na definição de domínio de Dedekind nos diz que entre ideais primos não existe relação de inclusão e a proposição 2.1.3 afirma que tal propriedade é preservada pelo processo de localização. Segue que se $S^{-1}A$ tiver algum ideal próprio não-nulo então ele é um domínio de Dedekind caso contrário ele é um corpo. □

COROLÁRIO 2.4.4. *Sejam A um domínio de Dedekind e $\mathfrak{p}$ um ideal primo de A. Então $A_{\mathfrak{p}}$ é um anel de valorização discreta.*

DEMONSTRAÇÃO. A Proposição 2.1.3 afirma que $A_{\mathfrak{p}}$ é anel local. Pela proposição anterior, $A_{\mathfrak{p}}$ é um domínio de Dedekind e de acordo com a observação 2.4.2 segue que $A_{\mathfrak{p}}$ é anel de valorização discreta. □

Caminhamos para demonstrar o principal resultado sobre domínios de Dedekind: seus ideais fatoram-se de maneira única em produto de ideais primos. Precisaremos de alguns lemas.

LEMA 2.4.5. *Seja A um anel Noetheriano. Então todo ideal não-nulo de A contém algum produto de ideais primos não-nulos.*

DEMONSTRAÇÃO. Suponha que não. Como A é Noetheriano podemos escolher um contra-exemplo maximal $\mathfrak{a}$. É claro que $\mathfrak{a}$ não é primo donde existem $x, y \in A \backslash \mathfrak{a}$ tais que $xy \in \mathfrak{a}$. Agora, $\mathfrak{a} + (x), \mathfrak{a} + (y) \supsetneq \mathfrak{a}$ mas $(\mathfrak{a} + (x))(\mathfrak{a} + (y)) \subseteq \mathfrak{a}$. Pela maximalidade de $\mathfrak{a}$, $\mathfrak{a} + (x), \mathfrak{a} + (y)$ contém, cada um, algum produto de ideais primos não-nulos. Segue que $\mathfrak{a}$ contém ele mesmo um produto de ideais primos não-nulos o que é absurdo. □

LEMA 2.4.6. *Seja A um anel e $\mathfrak{a}, \mathfrak{b}$ ideais não-nulos relativamente primos em A. Então para todos $m, n \in \mathbb{N}$ tem-se que $\mathfrak{a}^m, \mathfrak{b}^n$ são primos entre si.*

DEMONSTRAÇÃO. Suponha que não, então $\mathfrak{a}^m + \mathfrak{b}^n$ é um ideal próprio de A e está, portanto, contido em algum ideal maximal (primo) $\mathfrak{p}$. Como $\mathfrak{p}$ é primo e $\mathfrak{p} \supseteq \mathfrak{a}^m, \mathfrak{b}^n$ segue que $\mathfrak{p} \supseteq \mathfrak{a}, \mathfrak{b}$ donde $A \neq \mathfrak{p} \supseteq \mathfrak{a} + \mathfrak{b}$ contrariando o fato que $\mathfrak{a}, \mathfrak{b}$ são primos entre si. □

OBSERVAÇÃO 2.4.7. A condição (3) da definição de domínio de Dedekind implica que seus ideais primos são primos entre si. Isto e o lema acima implicam que quaisquer potências de ideais primos em um domínio de Dedekind são primos entre si.

LEMA 2.4.8. *Sejam A, B anéis. Todo ideal de $A \times B$ é da forma $\mathfrak{a} \times \mathfrak{b}$ onde $\mathfrak{a}$ e $\mathfrak{b}$ são ideais em A e B, respectivamente. Além disso, os ideais primos (maximais) de $A \times B$ são da forma $\mathfrak{p} \times B$ ou $A \times \mathfrak{p}$ com $\mathfrak{p}$ primo (maximal) em A ou B respectivamente.*

DEMONSTRAÇÃO. É claro que $\mathfrak{a} \times \mathfrak{b}$ é ideal em $A \times B$. Reciprocamente, seja $\mathfrak{c}$ um ideal em $A \times B$ e sejam $\mathfrak{a} = \{a \in A : (a, 0) \in \mathfrak{c}\}, \mathfrak{b} = \{b \in B : (0, b) \in \mathfrak{c}\}$. É claro que $\mathfrak{a} \times \mathfrak{b} \subseteq \mathfrak{c}$, por outro lado, dado $(a, b) \in \mathfrak{c}$ temos $(a, 0) = (a, b)(1, 0) \in \mathfrak{c}$ e $(0, b) = (a, b)(0, 1) \in \mathfrak{c}$ donde $a \in \mathfrak{a}, b \in \mathfrak{b}$ e $(a, b) \in \mathfrak{a} \times \mathfrak{b}$. Para a segunda parte do lema, lembremos que $\mathfrak{a} \times \mathfrak{b} \subseteq A \times B$ é um ideal primo (maximal) se e somente se $(A \times B)/(\mathfrak{a} \times \mathfrak{b})$ é domínio (corpo). Agora, o produto de dois anéis não-nulos sempre possui divisores de zero de modo que do isomorfismo $(A \times B)/(\mathfrak{a} \times \mathfrak{b}) \cong A/\mathfrak{a} \times B/\mathfrak{b}$ temos que este último é domínio (corpo) se e somente se ou $\mathfrak{a} = A$ ou $\mathfrak{b} = B$. Suponha sem perda de generalidade o último, então $(A \times B)/(\mathfrak{a} \times \mathfrak{b}) \cong A/\mathfrak{a} \times (0) \cong A/\mathfrak{a}$ e este é domínio (corpo) se e somente se $\mathfrak{a}$ é primo (maximal). □

OBSERVAÇÃO 2.4.9. O lema acima generaliza-se de maneira óbvia para o produto finito de anéis.

LEMA 2.4.10. *Seja $\mathfrak{p}$ um ideal maximal de um anel A e $\mathfrak{q}$ o ideal que ele induz em $S^{-1}A$. Isto é, $\mathfrak{q} = S^{-1}\mathfrak{p}$. Dado $m \in \mathbb{N}$, a aplicação $\pi : A/\mathfrak{p}^m \longrightarrow A_{\mathfrak{p}}/\mathfrak{q}^m$ dada por $a + \mathfrak{p}^m \longmapsto a + \mathfrak{q}^m$ é um isomorfismo.*

DEMONSTRAÇÃO. Vamos mostrar que $\operatorname{Ker}\pi = (0)$ o que equivale a mostrar que $\mathfrak{q}^m \cap A = \mathfrak{p}^m$ onde $\mathfrak{q}^m = S^{-1}\mathfrak{p}^m$. É claro que $\mathfrak{q}^m \cap A \supseteq \mathfrak{p}^m$. Reciprocamente, um elemento de $\mathfrak{q}^m \cap A$ é da forma $a = b/s;\ a \in A, b \in \mathfrak{p}^m, s \in S$. Então $as \in \mathfrak{p}^m$. Vamos mostrar que s é inversível em $A/\mathfrak{p}^m$ donde segue que $a \in \mathfrak{p}^m$. Agora, o único ideal maximal que contém $\mathfrak{p}^m$ é $\mathfrak{p}$ pois como todo maximal é primo teríamos que se um maximal $\mathfrak{m} \supseteq \mathfrak{p}^m$ implica $\mathfrak{m} \supseteq \mathfrak{p}$, mas $\mathfrak{p}$ é maximal donde $\mathfrak{p} = \mathfrak{m}$. Assim, pelo 2^o teorema do homomorfismo, o único ideal maximal em $A/\mathfrak{p}^m$ é $\mathfrak{p}/\mathfrak{p}^m$. Em particular, $A/\mathfrak{p}^m$ é local e $(A/\mathfrak{p}^m)^\times = (A/\mathfrak{p}^m) \setminus (\mathfrak{p}/\mathfrak{p}^m)$. Como $s + \mathfrak{p}^m \notin \mathfrak{p}/\mathfrak{p}^m$ segue o desejado.

Mostremos a sobrejetividade: seja $a/s + \mathfrak{q}^m \in A_{\mathfrak{p}}/\mathfrak{q}^m$. Como $s \notin \mathfrak{p}$ e $\mathfrak{p}$ é maximal temos que $(s) + \mathfrak{p} = A$,isto é, (s) e $\mathfrak{p}$ são primos entre si. Pelo lema 2.4.6 $(s) + \mathfrak{p}^m = A$ donde existem $b \in A$ e $t \in \mathfrak{p}^m \subseteq \mathfrak{q}^m$ tais que $bs + t = 1$ donde

$$\pi(bs + \mathfrak{p}^m) = \pi(1 + \mathfrak{p}^m) = 1 + \mathfrak{q}^m \implies \pi(b + \mathfrak{p}^m)\pi(s + \mathfrak{p}^m) = 1 + \mathfrak{q}^m \implies$$

$$\implies \pi(b + \mathfrak{p}^m) = \pi(s + \mathfrak{p}^m)^{-1} = s^{-1} + \mathfrak{q}^m.$$

Logo, $\pi(ba + \mathfrak{p}^m) = \pi(b + \mathfrak{p}^m)\pi(a + \mathfrak{p}^m) = s^{-1}a + \mathfrak{q}^m$ como queríamos. □

OBSERVAÇÃO 2.4.11. Reforçando a observação 2.1.5 temos que $\mathfrak{a}^{ec} = \mathfrak{a}$ também no caso que $\mathfrak{a}$ é uma potência de um ideal maximal $\mathfrak{p}$ e $S = A \backslash \mathfrak{p}$.

THEOREM 2.4.12. *Seja A um domínio de Dedekind. Então todo ideal de A é da forma $\mathfrak{p}_1^{r_1} ... \mathfrak{p}_m^{r_m}$ para únicos ideais primos $\mathfrak{p}_i$ e $r_i \in \mathbb{N}^*$.*

DEMONSTRAÇÃO. Seja $\mathfrak{a} \neq 0$ um ideal de A. Pelo lema 2.4.5, $\mathfrak{a} \supseteq \mathfrak{p}_1^{r_1}...\mathfrak{p}_m^{r_m} =: \mathfrak{b}$ com $\mathfrak{p}_i \neq \mathfrak{p}_j$, $\forall i \neq j$. Pela observação 2.4.7, $\mathfrak{p}_i^{r_1} + \mathfrak{p}_j^{r_j} = A$, $\forall i \neq j$. Assim, pelo teorema chinês do resto e do lema 2.4.10, temos que

$$\frac{A}{\mathfrak{b}} \cong \frac{A}{\mathfrak{p}^{r_1}} \times ... \times \frac{A}{\mathfrak{p}^{r_m}} \cong \frac{A_{\mathfrak{p}_1}}{(\mathfrak{p}_1 A_{\mathfrak{p}_1})^{r_1}} \times ... \times \frac{A}{(\mathfrak{p}_m A_{\mathfrak{p}_m})^{r_m}}$$

pela aplicação $a + \mathfrak{b} \longmapsto (a + (\mathfrak{p}_1 A_{\mathfrak{p}_1})^{r_1}, ..., a + (\mathfrak{p}_m A_{\mathfrak{p}_m})^{r_m})$. Agora, $\mathfrak{a}/\mathfrak{b}$ é um ideal de $A/\mathfrak{b}$ que pelo lema 2.4.8 e do segundo teorema do homomorfismo corresponde através do isomorfismo acima a um ideal da forma

$$\frac{\mathfrak{a}_1}{(\mathfrak{p}_1 A_{\mathfrak{p}_1})^{r_1}} \times ... \times \frac{\mathfrak{a}_m}{(\mathfrak{p}_m A_{\mathfrak{p}_m})^{r_m}}$$

com $\mathfrak{a}_i$ ideal de $A_{\mathfrak{p}_i}$. Como estes últimos são anel de valorização discreta temos $\mathfrak{a}_i = (\mathfrak{p}_i A_{\mathfrak{p}_i})^{s_i}$, $s_i \leq r_i$, $1 \leq i \leq m$. Agora o ideal

$$\frac{(\mathfrak{p}_1 A_{\mathfrak{p}_1})^{s_1}}{(\mathfrak{p}_1 A_{\mathfrak{p}_1})^{r_1}} \times ... \times \frac{(\mathfrak{p}_m A_{\mathfrak{p}_m})^{s_m}}{(\mathfrak{p}_m A_{\mathfrak{p}_m})^{r_m}}$$

também é imagem, pelo isomorfismo acima, do ideal $\mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m}/\mathfrak{b}$ donde $\mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m} + \mathfrak{b} = \mathfrak{a} + \mathfrak{b}$ (como ideais de $A/\mathfrak{b}$). Como ambos contém $\mathfrak{b}$, novamente pelo 2^o teorema do homomorfismo, $\mathfrak{a} = \mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m}$. Resta-nos mostrar a unicidade. Agora, suponha $\mathfrak{a} = \mathfrak{q}_1^{r_1}...\mathfrak{q}_n^{r_n}$. Então

$$(0) = \frac{\mathfrak{a}}{\mathfrak{a}} \cong \frac{(\mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m})\, A_{\mathfrak{q}_j}}{(\mathfrak{q}_1 A_{\mathfrak{q}_1})^{r_1}} \times ... \times \frac{(\mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m})\, A_{\mathfrak{q}_j}}{(\mathfrak{q}_n A_{\mathfrak{q}_n})^{r_n}}$$

donde $(\mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m})\, A_{\mathfrak{q}_j} / \left(\mathfrak{q}_j A_{\mathfrak{q}_j}\right)^{r_j} = 0 \, \forall j$. Agora, fixado j_0, se $\mathfrak{p}_i \neq \mathfrak{q}_{j_0}\, \forall i$ então existe um elemento de $\prod \mathfrak{p}_i$ que é inversível em $A_{\mathfrak{q}_{j_0}}$ e conseqüentemente em $A_{\mathfrak{q}_{j_0}} / \left(\mathfrak{q}_{j_0} A_{\mathfrak{q}_{j_0}}\right)^{r_{j_0}}$ donde

$$(\mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m})\, A_{\mathfrak{q}_{j_0}} / \left(\mathfrak{q}_{j_0} A_{\mathfrak{q}_{j_0}}\right)^{r_{j_0}} = A_{\mathfrak{q}_{j_0}} / \left(\mathfrak{q}_{j_0} A_{\mathfrak{q}_{j_0}}\right)^{r_{j_0}} \neq (0)\,.$$

Portanto, devemos ter $\mathfrak{p}_{i_0} = \mathfrak{q}_{j_0}$ para algum i_0. Segue que para este par (i_0, j_0) temos $s_{i_0} = r_{j_0}$. Continuando assim vemos que $m = n$ e $\mathfrak{q}_j = \mathfrak{p}_{\tau(j)}$, $r_j = s_{\tau(j)}$ para algum $\tau \in S_n$. □

OBSERVAÇÃO 2.4.13. Usando a notação do teorema anterior, temos que

$$\mathfrak{a} \subseteq \mathfrak{p}_i \iff r_i > 0 \iff \mathfrak{a} A_{\mathfrak{p}_i} \neq A_{\mathfrak{p}_i}.$$

COROLÁRIO 2.4.14. *Sejam $\mathfrak{a}, \mathfrak{b}$ ideais em um domínio de Dedekind A. Então $\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a} A_{\mathfrak{p}} \subseteq \mathfrak{b} A_{\mathfrak{p}}$, $\forall \mathfrak{p} \in \mathrm{Spec}(A)$. Em particular, $\mathfrak{a} = \mathfrak{b} \iff \mathfrak{a} A_{\mathfrak{p}} = \mathfrak{b} A_{\mathfrak{p}}$, $\forall \mathfrak{p} \in \mathrm{Spec}(A)$.*

DEMONSTRAÇÃO. A necessidade é óbvia. Para a suficiência, escreva $\mathfrak{a} = \mathfrak{p}_1^{r_1}...\mathfrak{p}_m^{r_m}$, $\mathfrak{b} = \mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m}$; $r_i, s_i \in \mathbb{N}$. Então

$$\mathfrak{a} A_{\mathfrak{p}_i} \subseteq \mathfrak{b} A_{\mathfrak{p}_i} \iff r_i \geq s_i$$

pois $A_{\mathfrak{p}_i}$ é anel de valorização discreta. Agora,

$$r_i \geq s_i,\ \forall i \implies \mathfrak{a} \subseteq \mathfrak{b}.$$

□

COROLÁRIO 2.4.15. *Seja A um domínio com um conjunto finito de ideais primos. Então A é domínio de Dedekind se e somente se A é domínio principal.*

DEMONSTRAÇÃO. É claro que se A é domínio principal então ele é domínio de Dedekind. Suponha A um domínio de Dedekind. Pelo teorema 2.4.12 é suficiente mostrarmos que os ideais primos são principais. Sejam $\mathfrak{p}_1 ... \mathfrak{p}_m$ os ideais primos de A. Seja $x_1 \in \mathfrak{p}_1 \setminus (\mathfrak{p}_1)^2$. Pelo teorema chinês do resto, existe $x \in A$ tal que $x \equiv x_1 \mod (\mathfrak{p}_1)^2$ e $x \equiv 1 \mod \mathfrak{p}_i,\ i \neq 1$. Afirmamos que $\mathfrak{p}_1$ e (x) geram os mesmos ideais em $A_{\mathfrak{p}_i}$ o que pelo corolário 2.4.14 demonstra que eles são iguais. De fato, temos $x = x_1 + a_1,\ a_1 \in (\mathfrak{p}_1)^2$ donde $x \in \mathfrak{p}_1 \setminus (\mathfrak{p}_1)^2$. Logo, $(\mathfrak{p}_1 A_{\mathfrak{p}_1})^2 \subsetneq (x)A_{\mathfrak{p}_1} \subseteq \mathfrak{p}_1 A_{\mathfrak{p}_1}$. Como $A_{\mathfrak{p}_1}$ é anel de valorização discreta temos que $(x)A_{\mathfrak{p}_1} = \mathfrak{p}_1 A_{\mathfrak{p}_1}$. Para $i \neq 1$ temos que $x = 1 + a_i,\ a_i \in \mathfrak{p}_i$ donde $x \in S_{\mathfrak{p}_i} = A \setminus \mathfrak{p}_i$ e temos que $x \in (A_{\mathfrak{p}_i})^\times$. Assim, $(x)A_{\mathfrak{p}_i} = A_{\mathfrak{p}_i}$ e segue o afirmado. Repetindo o processo para os demais ideais primos, o resultado está provado. □

COROLÁRIO 2.4.16. *Sejam $\mathfrak{a} \supseteq \mathfrak{b} \neq (0)$ dois ideais em um domínio de Dedekind. Então $\mathfrak{a} = \mathfrak{b} + (a)$ para algum $a \in A$.*

DEMONSTRAÇÃO. Escreva $\mathfrak{a} = \mathfrak{p}_1^{s_1} ... \mathfrak{p}_m^{s_m},\ \mathfrak{b} = \mathfrak{p}_1^{r_1} ... \mathfrak{p}_m^{r_m};\ r_i, s_i \in \mathbb{N}$. Como $\mathfrak{a} \supseteq \mathfrak{b}$ temos $s_i \leq r_i,\ 1 \leq i \leq m$. Para cada i seja $x_i \in \mathfrak{p}_i^{s_i} \setminus (\mathfrak{p}_i)^{s_i+1}$. Pelo teorema chinês do resto, existe $a \in A$ tal que $a \equiv x_i \mod (\mathfrak{p}_i)^{r_i},\ \forall i$. Afirmamos que $(\mathfrak{b} + (a))\, A_{\mathfrak{p}_i} = \mathfrak{a} A_{\mathfrak{p}_i},\ \forall i$ de onde o resultado segue. De fato, se $\mathfrak{p} \notin \{\mathfrak{p}_1, ..., \mathfrak{p}_m\}$ então da observação 2.4.13, $\mathfrak{b} A_{\mathfrak{p}} = A_{\mathfrak{p}}$ donde $(\mathfrak{b}+(a))\, A_{\mathfrak{p}} = \mathfrak{b} A_{\mathfrak{p}} + (a) A_{\mathfrak{p}} = A_{\mathfrak{p}} = \mathfrak{a} A_{\mathfrak{p}}$. Agora temos que $a = x_i + y_i,\ y_i \in \mathfrak{p}_i^{r_i} \implies a \in \mathfrak{p}_i^{s_i} \setminus (\mathfrak{p}_i)^{s_i+1}$ donde $(a)A_{\mathfrak{p}_i} = \mathfrak{p}_i^{s_i} A_{\mathfrak{p}_i}$. Assim, $(\mathfrak{b} + (a))\, A_{\mathfrak{p}_i} = \mathfrak{b} A_{\mathfrak{p}_i} + (a) A_{\mathfrak{p}_i} = \mathfrak{p}_i^{r_i} A_{\mathfrak{p}_i} + \mathfrak{p}_i^{s_i} A_{\mathfrak{p}_i} = \mathfrak{a} A_{\mathfrak{p}_i}$ como queríamos. □

COROLÁRIO 2.4.17. *Seja $\mathfrak{a}$ um ideal não-nulo em um domínio de Dedekind e seja $\mathfrak{a} \ni a \neq 0$ arbitrário então existe $b \in \mathfrak{a}$ tal que $\mathfrak{a} = (a, b)$.*

DEMONSTRAÇÃO. Basta aplicar o corolário anterior nos ideais $\mathfrak{a} \supseteq (a)$. □

COROLÁRIO 2.4.18. *Seja $\mathfrak{a}$ um ideal não-nulo em um domínio de Dedekind. Então existe um ideal não-nulo $\mathfrak{a}^*$ de A tal que $\mathfrak{a}\mathfrak{a}^*$ é principal. Este ideal pode ser tomado de maneira que $\mathfrak{a}\mathfrak{a}^* = (a)$ para um $a \in \mathfrak{a}$ arbitrário ou pode ser tomado de maneira que ele seja primo com um ideal arbitrário $\mathfrak{c}$.*

DEMONSTRAÇÃO. Seja $a \in \mathfrak{a},\ a \neq 0$. Então $\mathfrak{a} \supseteq (a)$ donde $(a) = \mathfrak{p}_1^{r_1} ... \mathfrak{p}_m^{r_m}$ e $\mathfrak{a} = \mathfrak{p}_1^{s_1} ... \mathfrak{p}_m^{s_m}$ com $s_i \leq r_i$. Tomando $\mathfrak{a}^* = \mathfrak{p}_1^{r_1 - s_1} ... \mathfrak{p}_m^{r_m - s_m}$ teremos $\mathfrak{a}\mathfrak{a}^* = (a)$. Mostremos que $\mathfrak{a}^*$ pode ser tomado primo com $\mathfrak{c}$. Temos $\mathfrak{a} \supseteq \mathfrak{a}\mathfrak{c}$ donde pelo corolário 2.4.16 existe $a \in \mathfrak{a}$ tal que $\mathfrak{a} = \mathfrak{a}\mathfrak{c} + (a)$. Como $\mathfrak{a} \supseteq (a)$ temos pelo argumento acima que $(a) = \mathfrak{a}\mathfrak{a}^*$ para algum ideal $\mathfrak{a}^*$. Agora, $\mathfrak{a}(\mathfrak{c} + \mathfrak{a}^*) = \mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}$ e pela unicidade da fatoração em ideais primos segue que $\mathfrak{c} + \mathfrak{a}^* = A$ como queríamos. □

PROPOSIÇÃO 2.4.19. *Um domínio de integridade A é um domínio principal se e somente se ele é domínio de Dedekind e de fatoração única.*

DEMONSTRAÇÃO. É claro que um domínio principal é domínio de Dedekind. Que ele é domínio de fatoração única mostra-se nos cursos básicos de álgebra.

Para a volta, é suficiente mostrarmos que os ideais primos são principais. Seja $\mathfrak{p} \neq (0)$, um ideal primo. Um elemento não-nulo de $\mathfrak{p}$, por pertencer a um domínio de fatoração única, se escreve como produto de irredutíveis. Como $\mathfrak{p}$ é primo ele contém pelo menos um de seus fatores irredutíveis que denotaremos por π. Pelo corolário 2.4.18, existe um ideal $\mathfrak{p}^*$tal que $\mathfrak{p}\mathfrak{p}^* = (\pi)$. Mostraremos que $\mathfrak{p}^* = A$ de onde segue o resultado. Pelo mesmo corolário existem ideais $\mathfrak{q}, \mathfrak{q}^*$ tais que $\mathfrak{p}\mathfrak{q} = (a)$, $\mathfrak{q} + \mathfrak{p}^* = A$, $\mathfrak{q}\mathfrak{q}^* = (b)$ e $\mathfrak{q}^*+\mathfrak{p} = A$ para $a, b \in A$. Como $(\pi b) = \mathfrak{p}\mathfrak{p}^*\mathfrak{q}\mathfrak{q}^* = (a)\mathfrak{p}^*\mathfrak{q}^*$ temos que $a \mid \pi b$ donde $ac = \pi b,\ c \in A$. Como em um domínio de fatoração única irredutível é primo temos que $\pi \mid a$ ou $\pi \mid c$. Se $\pi \mid a$ então $a/\pi \in A$ e $(a/\pi)\mathfrak{p}^* = \mathfrak{q}$ donde $\mathfrak{q} \subseteq \mathfrak{p}^*$ e como $\mathfrak{q} + \mathfrak{p}^* = A$ temos que $\mathfrak{p}^* = A$. Analogamente, se $\pi \mid c$ então $(c/\pi)\mathfrak{p} = \mathfrak{q}^* \implies \mathfrak{q}^* \subseteq \mathfrak{p}$ e então $\mathfrak{q}^*+\mathfrak{p} = A \implies \mathfrak{p} = A$ o que é absurdo e este caso não acontece. □

DEFINIÇÃO 2.4.20. Seja A um domínio de Dedekind. Um ideal fracionário de A é um A-submódulo $\mathfrak{a}$ de $K = \mathrm{ff}(A)$ tal que $d\mathfrak{a} := \{da : a \in \mathfrak{a}\} \subseteq A$ para algum $d \in A$, $d \neq 0$ (ou equivalentemente em K).

Note que um ideal fracionário não é, necessariamente um ideal. Quando necessário, para evitar confusão, nos referiremos aos ideais de A como ideais inteiros de A. O conjunto dos ideais fracionários de A será denotado por $\mathrm{Id}(A)$.

OBSERVAÇÃO 2.4.21. Podemos equivalentemente definir ideais fracionários como sendo os A-submódulos $\mathfrak{a}$ de K, não-nulos, finitamente gerados. De fato, um múltiplo comum dos denominadores dos geradores de $\mathfrak{a}$ satisfaz a condição da definição. Reciprocamente, se $\mathfrak{a}$ é um ideal fracionário então $d\mathfrak{a}$ é um A-submódulo de A (um ideal) e, portanto, finitamente gerado. por, digamos, $x_1, ..., x_m \in A$. Segue que $d^{-1}x_1, ..., d^{-1}x_m \in K$ é um conjunto de geradores para $\mathfrak{a}$.

Todo elemento não-nulo $x \in K$ define o ideal fracionário $(x) := Ax = \{ax : a \in A\}$. Tais ideais fracionários são denominados principais.

Dados ideais fracionários $\mathfrak{a}, \mathfrak{b}$ de A está definido o produto $\mathfrak{a}\mathfrak{b} := \{\sum a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ que é novamente um ideal fracionário. De fato, $\mathfrak{a}\mathfrak{b}$ é um A-submódulo de K, não-nulo, finitamente gerado. Note que no caso de ideais (fracionários) principais, $(a)(b) = (ab)$ e que $(a)\mathfrak{b} = a\mathfrak{b} = \{ab : b \in \mathfrak{b}\}$.

EXEMPLO 2.4.22. Seja A um anel de valorização discreta com ideal maximal (π) e $K = \mathrm{ff}(A)$. os elementos não-nulos de K se escrevem de forma única como $a = u\pi^m;\ u \in A^\times, m \in \mathbb{N}$. Seja $\mathfrak{a}$ um ideal fracionário de A. Então $d\mathfrak{a} \subseteq A$ para algum $d \in A$. Podemos supor $d = \pi^n$. Então $\pi^n\mathfrak{a}$ é um ideal inteiro de A e tem, portanto, a forma $(\pi^m),\ m \in \mathbb{N}$.

Afirmamos que $\mathfrak{a} = (\pi^{m-n})$. De fato, como $\pi^n\mathfrak{a} = (\pi^m)$ temos que $\pi^m = \pi^n a,\ a \in \mathfrak{a}$ donde $\pi^{m-n} \in \mathfrak{a}$ e $(\pi^{m-n}) \subseteq \mathfrak{a}$. Reciprocamente, dado $a \in \mathfrak{a}$, $\pi^n a = x\pi^m,\ x \in A$ donde $a = x\pi^{m-n} \in (\pi^{m-n})$ e segue o afirmado. Portanto, os ideais fracionários de A são da forma $(\pi^m),\ m \in \mathbb{Z}$. Do que foi visto, eles formam um grupo abeliano livre de posto 1 e a aplicação $\mathbb{Z} \longrightarrow \mathrm{Id}(A)$ dada por $m \longmapsto (\pi^m)$ é um isomorfismo.

THEOREM 2.4.23. *Seja A um domínio de Dedekind. Então o conjunto $\mathrm{Id}(A)$ é o grupo abeliano livre gerado pelos ideais primos de A.*

DEMONSTRAÇÃO. Vimos na observação anterior que o produto está bem definido e é obviamente comutativo. A associatividade vem do fato que

$$(\mathfrak{ab})\mathfrak{c} = \left\{\sum (a_ib_i)c_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, c_i \in \mathfrak{c}\right\} = \left\{\sum a_i(b_ic_i)\right\} = \mathfrak{a}(\mathfrak{bc}).$$

O elemento neutro será evidentemente A. Mostremos a existência de inversos: se $\mathfrak{a}$ é ideal inteiro então, pelo corolário 2.4.18 existe um ideal inteiro $\mathfrak{a}^*$ e $a \in A$ tal que $\mathfrak{aa}^* = (a)$. Assim, da observação anterior temos

$$\mathfrak{a}(a^{-1}\mathfrak{a}^*) = \mathfrak{a}(a^{-1})\mathfrak{a}^* = (a^{-1})\mathfrak{aa}^* = (a^{-1})(a) = A.$$

No caso geral, temos $d\mathfrak{a}$ um ideal inteiro com $d \in A$ assim:

$$\mathfrak{a}(d(d\mathfrak{a})^{-1}) = (\mathfrak{a}(d))(d\mathfrak{a})^{-1} = (d\mathfrak{a})(d\mathfrak{a})^{-1} = A$$

e temos o desejado. Resta-nos mostrar que $\mathrm{Id}(A)$ é gerado livremente pelos ideais inteiros primos de A. Seja $\mathfrak{a} \in \mathrm{Id}(A)$ então $d\mathfrak{a}$ é ideal inteiro de A com $d \in A$. Logo, podemos escrever $(d)\mathfrak{a} = d\mathfrak{a} = \mathfrak{p}_i^{r_1}...\mathfrak{p}_m^{r_m}$ e $(d) = \mathfrak{p}_1^{s_1}...\mathfrak{p}_m^{s_m}$ com $r_i, s_i \in \mathbb{N}$. Assim,

$$\mathfrak{a} = (d)^{-1}(d)\mathfrak{a} = \mathfrak{p}_1^{r_1-s_1}...\mathfrak{p}_m^{r_m-s_m};\ \mathfrak{p}_i^{-k} := (\mathfrak{p}_i^k)^{-1}.$$

A unicidade vem do fato que se tivéssemos $\mathfrak{p}_1^{r_1}...\mathfrak{p}_m^{r_m} = \mathfrak{q}_1^{s_1}...\mathfrak{q}_n^{s_n};\ r_i, s_j \in \mathbb{Z}$ com fatorações distintas então sendo $\mathfrak{a} = \mathfrak{p}_1^{|r_1|}...\mathfrak{p}_m^{|r_m|}\mathfrak{q}_1^{|s_1|}...\mathfrak{q}_n^{|s_n|}$ temos $\mathfrak{a}\mathfrak{p}_1^{r_1}...\mathfrak{p}_m^{r_m} = \mathfrak{a}\mathfrak{q}_1^{s_1}...\mathfrak{q}_n^{s_n}$ como ideais inteiros contrariando a já estabelecida unicidade da fatoração destes ideais. □

OBSERVAÇÃO 2.4.24. Reciprocamente, E. Noether mostrou que um domínio de integridade cujos ideais fracionários formam um grupo sob o produto de ideais é um domínio de Dedekind.

DEFINIÇÃO 2.4.25. Seja A um domínio de Dedekind e K seu corpo de frações. Definimos o grupo das classes de ideais como sendo o quociente $\mathrm{Cl}\,(K) = \mathrm{Cl}(A) := \mathrm{Id}(A)/\,\mathrm{P}(A)$ onde $\mathrm{P}(A)$ é o subgrupo dos ideais fracionários principais. O número de classe de A (de K), denotado por h_K é a ordem de $\mathrm{Cl}(A)$.

Seja S um sistema multiplicativo em A, domínio de Dedekind, e $A_S = S^{-1}A$ que vimos ser ou domínio de Dedekind ou um corpo. De qualquer forma, $\mathrm{ff}(A_S) = \mathrm{ff}(A)$. Para todo ideal $\mathfrak{a}$, $S^{-1}\mathfrak{a} := \{a/s : a \in \mathfrak{a},\ s \in S\}$ é facilmente visto ser um ideal de A_S. Também é evidente que dados ideais fracionários $\mathfrak{a}, \mathfrak{b}$, tem-se $S^{-1}(\mathfrak{ab}) = \left(S^{-1}\mathfrak{a}\right)\left(S^{-1}(\mathfrak{b})\right)$. Queremos

mostrar que $S^{-1}\left(\mathfrak{a}^{-1}\right) = S^{-1}\left(\mathfrak{a}\right)^{-1}$. Como $S^{-1}\left(A\right) = A_S$ temos que S^{-1} manda elemento neutro em elemento neutro. Assim, $A_S = S^{-1}\left(A\right) = S^{-1}\left(\mathfrak{a}^{-1}\mathfrak{a}\right) = S^{-1}\left(\mathfrak{a}^{-1}\right)S^{-1}\left(\mathfrak{a}\right)$ donde $S^{-1}\left(\mathfrak{a}^{-1}\right) = S^{-1}\left(\mathfrak{a}\right)^{-1}$.

COROLÁRIO 2.4.26. *Seja A um domínio de Dedekind e S um sistema multiplicativo em A. Então a aplicação $\mathfrak{a} \longmapsto S^{-1}\mathfrak{a}$ define um isomorfismo entre o subgrupo de* $\mathrm{Id}(A)$ *gerado pelos ideais (inteiros) primos de A que não intersectam S e o grupo* $\mathrm{Id}(S^{-1}A)$.

DEMONSTRAÇÃO. Que esta aplicação é um morfismo de grupo segue da construção acima e da proposição 2.1.3 segue que ela é uma bijeção entre os geradores e, portanto, um isomorfismo. □

COROLÁRIO 2.4.27. *Seja A um domínio de Dedekind com número de classe finito. Sejam $\mathfrak{a}_1, ..., \mathfrak{a}_m$ um conjunto de representantes para o grupo de classes de ideais formado por ideais inteiros e seja $b \in \cap\mathfrak{a}_i$. Então sendo $S = \{b^n : n \in \mathbb{N}\}$ tem-se que A_S é domínio principal.*

DEMONSTRAÇÃO. Por hipótese, todo ideal inteiro $\mathfrak{a} \in \mathrm{Id}(A)$ pode ser escrito como $\mathfrak{a} = (a)\mathfrak{a}_i;\ a \in \mathrm{ff}(A)^{\times}, 1 \leq i \leq m$. Então $S^{-1}\mathfrak{a} = (a)S^{-1}\mathfrak{a}_i$ onde, agora, (a) denota o ideal fracionário gerado por a em A_S. Como $S^{-1}\mathfrak{a}_i$ é inteiro e ele contem uma unidade, b, ele é o anel inteiro. Logo, $S^{-1}\mathfrak{a}$ é principal para todo ideal inteiro $\mathfrak{a} \in \mathrm{Id}(A)$. Agora pela observação 2.1.5 todo ideal inteiro de A_S é desta forma donde segue o desejado. □

Antes de continuarmos vejamos uma caracterização de $\mathfrak{a}^{-1}$ que nos será útil. Defina $\mathfrak{a}' = \{a \in \mathrm{ff}(A) : a\mathfrak{a} \subseteq A\}$. Vamos mostrar que $\mathfrak{a}' = \mathfrak{a}^{-1}$. É fácil ver que este é um A-submódulo de $\mathrm{ff}(A)$. Dado $d \in \mathfrak{a}$, da definição de $\mathfrak{a}'$ temos que $d\mathfrak{a}' \subseteq A$ donde $\mathfrak{a}\mathfrak{a}' \subseteq A$. Este é um A-modulo contido em A e, portanto, um ideal de A. Suponha que $\mathfrak{a}\mathfrak{a}' \subsetneq A$. Então $\mathfrak{a}\mathfrak{a}' \subseteq \mathfrak{p}$ para algum ideal primo de A. Passando para $A_{\mathfrak{p}}$ (que é domínio de Dedekind) obtemos a inclusão $\mathfrak{b}\mathfrak{b}' \subseteq \mathfrak{q}$ onde $\mathfrak{q} = S^{-1}\mathfrak{p}$, $\mathfrak{b} = S^{-1}\mathfrak{a}$ e $\mathfrak{b}' = S^{-1}\mathfrak{a}'$.

Afirmamos que $\mathfrak{b}' = \{a \in \mathrm{ff}(A_S) = \mathrm{ff}(A) : a\mathfrak{b} \subseteq A_{\mathfrak{p}}\} =: \mathfrak{i}$. É claro que $\mathfrak{b}' \subseteq \mathfrak{i}$. Para a inclusão contrária note que se $x \in \mathfrak{i}$ e $\mathfrak{a} = \alpha_1 A + ... + \alpha_n A$, $\alpha_i \in \mathfrak{a} \subseteq \mathfrak{b}$ temos por hipótese $x\alpha_i = a_i/s_i,\ a_i \in A, s_i \in S$. Seja $s = \prod s_i$ então dados $\lambda_1, ..., \lambda_n \in A$ temos

$$xs\left(\sum \lambda_i\alpha_i\right) = \sum \lambda_i\widehat{s}_i a_i \in A;\ \widehat{s}_i = s/s_i.$$

Logo, $xs \in \mathfrak{a}'$ donde $x = xs/s \in \mathfrak{b}'$ e segue o afirmado.

Agora também temos $\mathfrak{q} = (\pi)$ onde π é um primo de $A_{\mathfrak{p}}$ e $\mathfrak{b} = (\pi^m)$, $m \in \mathbb{Z}$. Afirmamos que $\mathfrak{b}' = (\pi^{-m})$ o que implicará que $\mathfrak{q} = \mathfrak{b}\mathfrak{b}' = A_{\mathfrak{p}}$ o que é absurdo donde seguirá que $\mathfrak{a}\mathfrak{a}' = A$ e $\mathfrak{a}' = \mathfrak{a}^{-1}$. De fato, note que $\pi^{-m}\mathfrak{b} = \pi^{-m}(\pi^m) \subseteq A_{\mathfrak{p}}$ donde $\pi^{-m} \in \mathfrak{b}'$ e $(\pi^{-m}) \subseteq \mathfrak{b}'$. Reciprocamente, dado $a \in \mathfrak{b}'$ temos $\pi^m \in \mathfrak{b}$ donde

$$a\pi^m = b \in A_{\mathfrak{p}} \implies a = b\pi^{-m} \in (\pi^{-m})$$

e segue o afirmado.

2.5. Fechos inteiros de domínios de Dedekind

Nesta seção provaremos que o fecho inteiro de um domínio de Dedekind sobre uma extensão finita e separável de seu corpo de frações é, ainda, um domínio de Dedekind. Precisamos de dois lemas. O primeiro é bem conhecido dos cursos básicos de álgebra e omitiremos a demonstração.

LEMA 2.5.1. *Seja A um anel Noetheriano. Então todo R-módulo finitamente gerado é Noetheriano.*□

LEMA 2.5.2. *Um domínio de integridade A contendo um corpo K e algébrico sobre este corpo é, ele mesmo, um corpo.*

DEMONSTRAÇÃO. Seja $\beta \in A$, $\beta \neq 0$. Mostremos que ele possui inverso em A. Como A é algébrico sobre K, $K[\beta]$ tem dimensão finita como K-espaço vetorial. Agora a aplicação $\beta : K[\beta] \longrightarrow K[\beta]$ dada por $x \longmapsto \beta x$ é injetora (pois A é domínio). Da álgebra linear segue que β é sobrejetora e existe $\beta' \in K[\beta] \subseteq A$ tal que $\beta\beta' = 1$ como queríamos. □

THEOREM 2.5.3. *Seja A um domínio de Dedekind com corpo de frações K. Seja $L \geq K$ uma extensão finita e separável. Então A_L é domínio de Dedekind.*

DEMONSTRAÇÃO. Por 1.3.10, A_L está contido em um A-módulo finitamente gerado B. Do primeiro lema sabemos que B é Noetheriano. Assim, seus ideais são todos finitamente gerados como A-módulos e, conseqüentemente, como A_L-módulos (ideais). Portanto, A_L é anel Noetheriano.

Já provamos em 1.1.18 que A_L é integralmente fechado. Resta-nos mostrar que todo ideal primo $\mathfrak{q}$, não-nulo, de A_L é maximal. Seja $\beta \in \mathfrak{q}$, $\beta \neq 0$. Como β é inteiro sobre A, ele satisfaz uma equação do tipo

$$\beta^n + b_1\beta^{n-1} + ... + b_n = 0,\ b_i \in A$$

que podemos supor ser de grau mínimo, ou seja, podemos supor $b_n \neq 0$. Como $b_n \in \beta A_L \cap A$ temos que $\mathfrak{q} \cap A \neq (0)$. Agora, é claro que este é um ideal primo e, portanto, maximal de A. Então $A/(\mathfrak{q} \cap A)$ é um corpo e$A_L/\mathfrak{q}$ é um domínio. O primeiro está naturalmente imerso no segundo pela aplicação $x + \mathfrak{q} \cap A \longmapsto x + \mathfrak{q}$. Afirmamos que $A_L/\mathfrak{q}$ é algébrico sobre $A/(\mathfrak{q} \cap A)$. De fato, dado $\alpha + \mathfrak{q} \in A_L/\mathfrak{q}$, como A_L é inteiro sobre A, temos uma equação

$$\alpha^m + a_1\alpha^{m-1} + ... + a_m = 0,\ a_i \in A$$

que composta com a projeção nos dá

$$(\alpha + \mathfrak{q})^m + (a_1 + \mathfrak{q})(\alpha + \mathfrak{q})^{m-1} + ... + (a_m + \mathfrak{q}) = 0,\ a_i + \mathfrak{q} \in A/(\mathfrak{q} \cap A)$$

o que mostra que $\alpha + \mathfrak{q}$ é algébrico sobre $A/(\mathfrak{q} \cap A)$ donde segue o afirmado. Do segundo lema, agora, temos que $A_L/\mathfrak{q}$ é corpo e, portanto, que $\mathfrak{q}$ é maximal. □

2.6. Ramificações

Seja A um domínio de Dedekind com corpo de frações K, $L \geq K$ uma extensão finita e separável e $B = A_L$. Um ideal primo $\mathfrak{p}$ de A gera o ideal $\mathfrak{p}B$ em B que deve, pelos teoremas 2.4.12 e 2.5.3, fatora-se de maneira única como:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g};\ \mathfrak{P}_i \in \mathrm{Spec}(B),\ e_i \geq 1. \tag{2.6.1}$$

Se $g > 1$ dizemos que $\mathfrak{p}$ decompõe-se em B. Se $e_i > 1$ para algum i, dizemos que $\mathfrak{p}$ ramifica-se em B (ou L). Quando $\mathfrak{P}$ aparece na fatoração de $\mathfrak{p}B$ dizemos que $\mathfrak{P}$ divide $\mathfrak{p}$ e denotamos $\mathfrak{P} \mid \mathfrak{p}$. Os números e_i são chamados índices de ramificação e denotamos $e(\mathfrak{P}/\mathfrak{p})$. Observe que $B/\mathfrak{P}$ é um A-módulo e que se $\mathfrak{P} \mid \mathfrak{p}$ então $\mathfrak{p}\left(B/\mathfrak{P}\right) = \left(\mathfrak{p}B\right)/\mathfrak{P} = (0)$ donde $B/\mathfrak{P}$ é um $A/\mathfrak{p}$-espaço vetorial. Ou seja, $A/\mathfrak{p}$ pode ser naturalmente identificado como um subcorpo de $B/\mathfrak{P}$ através da aplicação $a + \mathfrak{p} \longmapsto a + \mathfrak{P}$. O número (provaremos ser finito) $f(\mathfrak{P}/\mathfrak{p}) := [B/\mathfrak{P} : A/\mathfrak{p}]$ é denominado índice de inércia de $\mathfrak{P}$ sobre $\mathfrak{p}$.

Lema 2.6.1. *Na notação acima, um ideal primo $\mathfrak{P}$ de B divide $\mathfrak{p}$ se e somente se $\mathfrak{p} = \mathfrak{P} \cap K$.*

Demonstração. Se $\mathfrak{P} \mid \mathfrak{p}$ então é claro que $\mathfrak{p} \subseteq \mathfrak{P} \cap K$ e este último é um ideal de A. Mas $\mathfrak{P} \cap K \neq A$ $(1 \notin \mathfrak{P} \cap K)$ logo, pela maximalidade de $\mathfrak{p}$, temos $\mathfrak{p} = \mathfrak{P} \cap K$. Para a volta, se $\mathfrak{p} \subseteq \mathfrak{P}$ então $\mathfrak{p}B \subseteq \mathfrak{P}$ o que pela observação 2.4.13, implica que $\mathfrak{P}$ aparece na fatoração de $\mathfrak{p}B$. □

Theorem 2.6.2. *Seja d o grau da extensão separável $L \geq K$ e sejam $\mathfrak{P}_1, ..., \mathfrak{P}_g \in \mathrm{Spec}(B)$ os primos dividindo o primo $\mathfrak{p} \in \mathrm{Spec}(A)$. Então*

$$\sum_{i=1}^{g} e_i f_i = d;\ e_i = e(\mathfrak{P}_i/\mathfrak{p}),\ f_i = f\left(\mathfrak{P}_i/\mathfrak{p}\right).$$

Se L é Galoisiano sobre K então todos os índices de ramificação são iguais, todos os graus das classes de resíduo são iguais e temos, portanto

$$efg = d.$$

Demonstração. Para provarmos a primeira parte mostraremos que

$$\sum e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}] = d.$$

Para a primeira igualdade observe que pelo teorema chinês do resto, $B/\mathfrak{p}B = B/\prod \mathfrak{P}_i^{e_i} \cong \prod B/\mathfrak{P}_i^{e_i}$ e só precisamos mostrar que $[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}] = e_i f_i$, $1 \leq i \leq g$. Agora, fixado i, para cada $0 \leq r_i \leq e_i - 1$, temos que $\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1}$ é um $B/\mathfrak{P}_i$-espaço vetorial (pois $\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1}$ é um B-módulo e $\mathfrak{P}_i(\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1}) = (0)$) Afirmamos que $\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1} \cong B/\mathfrak{P}_i$. De fato, escolha $x \in \mathfrak{P}_i^{r_i} \backslash \mathfrak{P}_i^{r_i+1}$ e defina a aplicação $\psi : B \longrightarrow \mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1}$ dada por $b \longmapsto bx + \mathfrak{P}_i^{r_i+1}$. Note que pelo 2^o teorema do homomorfismo, o ideal gerado por x em $\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1}$ é todo o anel, isto é, $(\overline{x}) = \mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1}$. Portanto, ψ é sobrejetora. Note também

que $\mathfrak{P}_i \subseteq \operatorname{Ker}\psi$. Como $\psi \neq 0$ e $\ker\psi$ é ideal, por maximalidade temos que $\mathfrak{P}_i = \ker\psi$. Pelo 1º teorema do homomorfismo segue o afirmado. Agora observe que

$$\frac{\left(\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{e_i}\right)}{\left(\mathfrak{P}_i^{r_i+1}/\mathfrak{P}_i^{e_i}\right)} \cong \frac{\mathfrak{P}_i^{r_i}}{\mathfrak{P}_i^{r_i+1}} \cong \frac{B}{\mathfrak{P}_i},\ 0 \leq r_i \leq e_i - 1$$

donde

$$\dim_{B/\mathfrak{P}_i}\left(\frac{\mathfrak{P}_i^{r_i}}{\mathfrak{P}_i^{e_i}}\right) = \dim_{B/\mathfrak{P}_i}\left(\frac{\mathfrak{P}_i^{r_i+1}}{\mathfrak{P}_i^{e_i}}\right) + 1,\ 0 \leq r_i \leq e_i - 1 \implies \dim_{B/\mathfrak{P}_i}\left(\frac{B}{\mathfrak{P}_i^{e_i}}\right) = e_i.$$

Como, por definição, a dimensão de $B/\mathfrak{P}_i$ sobre $A/\mathfrak{p}$ é f_i segue que $\dim_{A/\mathfrak{p}}\left(B/\mathfrak{P}_i^{e_i}\right) = e_i f_i$.

Vamos à segunda igualdade. Ela é válida quando A é principal pois neste caso, B é A-módulo livre de posto d e então

$$B \cong A^d \implies A/\mathfrak{p} \otimes B \cong A/\mathfrak{p} \otimes A^d \implies B/\mathfrak{p}B \cong (A/\mathfrak{p})^d.$$

No caso geral, seja $S = A\backslash\mathfrak{p}$ e note que $S \cap \mathfrak{P}_i = (S \cap A) \cap \mathfrak{P}_i = S \cap \mathfrak{p} = \varnothing$ usando o lema anterior. Note também que S é sistema multiplicativo para B e assim pelo corolário 2.4.26,

$$S^{-1}(\mathfrak{p}B) = S^{-1}\left(\prod \mathfrak{P}_i^{e_i}\right) = \prod \left(S^{-1}\mathfrak{P}_i\right)^{e_i}.$$

Como $S^{-1}A$ é principal segue do argumento acima que

$$\sum e_i f_i' = \left[\frac{S^{-1}B}{S^{-1}(\mathfrak{p}B)} : \frac{S^{-1}A}{S^{-1}\mathfrak{p}}\right] = d.$$

Resta-nos mostrar que $f_i = f\left(S^{-1}\mathfrak{P}_i/S^{-1}\mathfrak{p}\right) = f\left(\mathfrak{P}_i/\mathfrak{p}\right) = f_i$. Agora, vimos no lema 2.4.10 que $S^{-1}A/S^{-1}\mathfrak{p} \cong A/\mathfrak{p}$, portanto

$$\left[\frac{S^{-1}B}{S^{-1}\mathfrak{P}_i} : \frac{S^{-1}A}{S^{-1}\mathfrak{p}}\right] = \left[\frac{S^{-1}B}{S^{-1}\mathfrak{P}_i} : \frac{A}{\mathfrak{p}}\right].$$

Vejamos que $\left[S^{-1}B/S^{-1}\mathfrak{P}_i : A/\mathfrak{p}\right] = \left[B/\mathfrak{P}_i : A/\mathfrak{p}\right]$. Seja $\{[\beta_1], ..., [\beta_n]\}$ base de $S^{-1}B/S^{-1}\mathfrak{P}_i$ como $A/\mathfrak{p}$-espaço vetorial. Podemos supor $\beta_i \in B$. Considere $\overline{\beta_i} \in B/\mathfrak{P}_i$ e note que $\overline{\beta_i} \neq \overline{0}$. Afirmamos que $\left\{\overline{\beta_1}, ..., \overline{\beta_n}\right\}$ é base de $B/\mathfrak{P}_i$ como $A/\mathfrak{p}$-espaço vetorial. De fato, se $\overline{\lambda_1}, ..., \overline{\lambda_n} \in A/\mathfrak{p}$ são tais que $\sum \overline{\lambda_i\beta_i} = \overline{0}$ então como $\mathfrak{P}_i \subseteq S^{-1}\mathfrak{P}_i$ temos $\sum \overline{\lambda_i}\,[\beta_i] = [0]$ e então $\overline{\lambda_1}, ..., \overline{\lambda_n} = \overline{0}$. Agora seja $\overline{\beta} \in B/\mathfrak{P}_i$. Temos $[\beta] = \sum \overline{\lambda_i}\,[\beta_i]$, $\overline{\lambda_i} \in A/\mathfrak{p}$. Ou seja, temos $\beta - \sum \lambda_i\beta_i \in S^{-1}\mathfrak{P}_i$. Como $\beta - \sum \lambda_i\beta_i \in B$ e $S^{-1}\mathfrak{P}_i \cap B = \mathfrak{P}_i$ temos que $\beta - \sum \lambda_i\beta_i \in \mathfrak{P}_i$ donde $\overline{\beta} = \sum \overline{\lambda_i\beta_i}$ provando o afirmado. Isto conclui a primeira parte do teorema.

Assuma agora que L é Galoisiano sobre K. É claro que B é estável sob a ação de $\operatorname{Gal}(L/K)$, isto é, $\sigma B = B$, $\forall \sigma \in \operatorname{Gal}(L/K)$ (se $b \in B$ e $\sigma \in \operatorname{Gal}(L/K)$, como b é inteiro sobre A segue que σb é inteiro sobre A. Como $B = A_L$ segue que $\sigma b \in B$). Por esta razão, se $\mathfrak{P}$ é um ideal primo de B então $\sigma\mathfrak{P}$ também é (se $xy \in \sigma\mathfrak{P}$ então $\sigma^{-1}(x)\,\sigma^{-1}(y) \in \mathfrak{P}$

donde x ou y está em $\sigma\mathfrak{P}$). Agora se $\mathfrak{P} \mid \mathfrak{p}$ então $\sigma\mathfrak{P} \mid \mathfrak{p}$ pois do lema anterior,

$$\mathfrak{p} = \mathfrak{P} \cap K \implies \mathfrak{p} = \sigma\mathfrak{p} = \sigma(\mathfrak{P} \cap K) = \sigma\mathfrak{P} \cap K$$

e novamente do lema, $\sigma\mathfrak{P} \mid \mathfrak{p}$. Como σ é um isomorfismo de K-álgebras devemos ter $e(\sigma\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$ e $f(\sigma\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$ e assim basta mostrarmos que $\mathrm{Gal}(L/K)$ age transitivamente nos ideais primos de B que dividem $\mathfrak{p}$.

Suponha, por absurdo, que $\mathfrak{P}$ e $\mathfrak{Q}$ dividem $\mathfrak{p}$ mas não são conjugados, isto é, para todo $\sigma \in \mathrm{Gal}(L/K)$, $\sigma\mathfrak{P} \neq \mathfrak{Q}$. Seja $\mathcal{R} = \{\sigma\mathfrak{P} : \sigma \in \mathrm{Gal}(L/K)\}$. Então, pelo teorema chinês do resto, existe $\beta \in \mathfrak{Q}$ tal que $\beta \notin \mathfrak{a}, \forall \mathfrak{a} \in \mathcal{R}$. Seja $b = \mathrm{Nm}(\beta) = \prod \sigma\beta$. Então $b \in A \cap \mathfrak{Q} = \mathfrak{p}$ (pelo lema). Por outro lado, para todo $\sigma \in \mathrm{Gal}(L/K)$, $\beta \notin \sigma^{-1}\mathfrak{P}$, ou seja, $\sigma\beta \notin \mathfrak{P}$, $\forall \sigma \in \mathrm{Gal}(L/K)$. Assim o fato que $\prod \sigma\beta = b \in \mathfrak{p} \subseteq \mathfrak{P}$ contraria a primalidade de $\mathfrak{P}$ demonstrando a última parte do teorema. □

Procederemos agora para um resultado que nos dá uma resposta objetiva sobre quais primos ramificam-se em uma extensão finita e separável.

LEMA 2.6.3. *Seja $A \leq B$ uma extensão de anéis tal que B é um A-módulo livre de posto m. Seja $e = \{e_1, ..., e_m\}$ uma base de B sobre A. Então para todo ideal $\mathfrak{a}$ de A, $\overline{e} = \{e_1 + \mathfrak{a}B, ..., e_m + \mathfrak{a}B\}$ é uma base do $A/\mathfrak{a}$-módulo $B/\mathfrak{a}B$ e $\mathrm{disc}_{\overline{e}}\left(\mathrm{Tr}_{(B/\mathfrak{a}B)/(A/\mathfrak{a})}\right) \equiv \mathrm{disc}_e\left(\mathrm{Tr}_{B/A}\right) \mod \mathfrak{a}$.*

DEMONSTRAÇÃO. A primeira parte do teorema já foi vista na demonstração do teorema 2.6.2. Para a segunda parte, vamos mostrar que $\mathrm{Tr}_{(B/\mathfrak{a}B)/(A/\mathfrak{a})}(e_ie_j + \mathfrak{a}B) \equiv \mathrm{Tr}_{B/A}(e_ie_j) \mod \mathfrak{a}$. Para isso, sejam (a_{kl}) e $(b_{kl} + \mathfrak{a}B)$ as matrizes correspondentes às aplicações $x \longmapsto (e_ie_j)x$ e $x + \mathfrak{a}B = (e_ie_j + \mathfrak{a}B)(x + \mathfrak{a}B)$. Então temos

$$(e_ie_j)e_k = \sum_l a_{kl}e_l \;\; ; \;\; (e_ie_j + \mathfrak{a}B)(e_k + \mathfrak{a}B) = \sum_l (b_{kl} + \mathfrak{a}B)(e_l + \mathfrak{a}B)$$

substituindo obtemos

$$\sum_l (a_{kl} + \mathfrak{a}B)(e_l + \mathfrak{a}B) = \sum_n (b_{mn} + \mathfrak{a}B)(e_n + \mathfrak{a}B)$$

como $\overline{e}$ é base podemos igualar os índices e obter

$$(a_{kl} + \mathfrak{a}B)(e_l + \mathfrak{a}B) = (b_{kl} + \mathfrak{a}B)(e_l + \mathfrak{a}B),\ \forall k, l \implies (a_{kl} - b_{kl})e_l \in \mathfrak{a}B,\ \forall k, l$$

e como e também é base devemos ter

$$a_{kl} - b_{kl} \in \mathfrak{a},\ \forall k, l$$

donde segue o desejado. □

LEMA 2.6.4. *Seja A um anel e $B_1, ..., B_g$ extensões de A (de anéis) tais que cada B_i é um A-módulo livre de posto finito. Então* $\mathrm{disc}\left(\left(\prod B_i\right)/A\right) = \prod \mathrm{disc}\,(B_i/A)$.

DEMONSTRAÇÃO. Sejam $e_i = \{e_{i1}, ..., e_{ij_i}\}$ bases de B_i e $\iota_i : B_i \longrightarrow \prod B_i$ as injeções canônicas no produto cartesiano. É claro que $\cup \iota_i(e_i)$ e base de $\prod B_i$. Assim sendo temos

$$\operatorname{disc}\left(\left(\prod B_i\right)/A\right) = \overline{\det\left(\left(\left(\operatorname{Tr}_{(\prod B_i)/A}(\iota_k(e_{kl})\iota_m(e_{mn}))\right)_{ln}\right)_{km}\right)}.$$

Agora como $\iota_k(e_{kl})\iota_m(e_{mn}) = \begin{cases} 0, & k \neq m \\ \iota_k(e_{kl}e_{kn}), & k = m \end{cases}$ é fácil ver que a matriz por blocos acima tem a forma

$$\begin{pmatrix} \left(\operatorname{Tr}_{B_1/A}(e_{1l}e_{1n})\right)_{ln} & 0 & ... & 0 \\ 0 & \left(\operatorname{Tr}_{B_2/A}(e_{2l}e_{2n})\right)_{ln} & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & ... & 0 & \left(\operatorname{Tr}_{B_g/A}(e_{gl}e_{gn})\right)_{ln} \end{pmatrix}_{g\times g}$$

donde

$$\operatorname{disc}\left(\left(\prod_{i=1}^{g} B_i\right)/A\right) = \prod_{i=1}^{g} \overline{\det\left(\left(\left(\operatorname{Tr}_{B_i/A}(e_{il}e_{in})\right)_{ln}\right)_{km}\right)} = \prod_{i=1}^{g} \operatorname{disc}\left(B_i/A\right).$$

□

DEFINIÇÃO 2.6.5. Um elemento a de um anel A é dito nilpotente se e somente se $a^k = 0$ para algum $k \in \mathbb{N}^*$. O anel A é dito reduzido se e somente se ele não possui elementos nilpotentes não-nulos.

LEMA 2.6.6. *Seja K um corpo perfeito e seja B uma K-álgebra de dimensão finita. Então B é reduzido se e somente se* $\operatorname{disc}(B/K) \neq 0$.

DEMONSTRAÇÃO. Suponha que exista $\beta \neq 0$ um elemento nilpotente de B e seja $\{e_1, ..., e_m\}$ uma base de B com $e_1 = \beta$. Então βe_i é nilpotente para todo i e, portanto, a aplicação K-linear $x \longmapsto \beta e_i x$ é nilpotente. Em particular, a matriz que a representa é nilpotente. Como uma matriz nilpotente tem traço nulo, segue que a primeira linha da matriz $(\operatorname{Tr}_{B/K}(e_i e_j))_{ij}$ é nula e, portanto, seu determinante também.

Reciprocamente, suponha que B é reduzido. Primeiro vamos mostrar que a intersecção, $\mathfrak{R}$, de todos os ideais primos de B é nulo. Para isso, seja $b \in B,\ b \neq 0$ e seja Σ o conjunto dos ideais de B que não contém nenhuma potência de b. Como b não é nilpotente (por hipótese) $(0) \in \Sigma \neq \varnothing$. Como B é Noetheriano, Σ possui um elemento maximal $\mathfrak{p}$. Vamos mostrar que $\mathfrak{p}$ é primo. Com isso, e do fato que $b \notin \mathfrak{p}$ seguirá que $b \notin \mathfrak{R}$. Sejam $x, y \in B\backslash\mathfrak{p}$. Então $\mathfrak{p} + (x),\ \mathfrak{p} + (y) \supsetneq \mathfrak{p}$. Pela maximalidade de $\mathfrak{p}$ temos $b^m \in \mathfrak{p} + (x),\ b^n \in \mathfrak{p} + (y)$ para algum $m, n \in \mathbb{N}$. Escreva $b^m = p + cx,\ b^n = q + dy;\ p, q \in \mathfrak{p},\ c, d \in B$. Então $b^{m+n} = pq + pdy + qcx + cdxy \in \mathfrak{p} + (xy)$ donde $\mathfrak{p} + (xy) \notin \Sigma$. Em particular, $\mathfrak{p} + (xy) \neq \mathfrak{p}$ donde $xy \notin \mathfrak{p}$. Logo, $\mathfrak{p}$ é primo e temos o desejado. Como b é arbitrário segue que $\mathfrak{R} = (0)$.

Agora, seja $\mathfrak{p}$ um ideal primo arbitrário de B. Então $B/\mathfrak{p}$ é um domínio que, pelo fato que B tem dimensão finita sobre K, é algébrico sobre K. Pelo lema 2.5.2, $B/\mathfrak{p}$ é um corpo

e, portanto, $\mathfrak{p}$ é maximal. Sejam $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_r$ ideais primos distintos de B. Como todos são maximais pelo argumento acima, eles são todos primos entre si. O teorema chinês do resto então nos diz que

$$B/\bigcap_{i=1}^{r}\mathfrak{p}_i = \prod_{i=1}^{r} B/\mathfrak{p}_i. \tag{2.6.2}$$

Agora observe que

$$\dim_K B \geq \dim_K (B/\cap\, \mathfrak{p}_i) = \sum \dim_K (B/\mathfrak{p}_i) \geq r.$$

Portanto, B possui apenas uma quantidade finita de ideais primos, digamos, $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_g$ onde $g \leq \dim_K B$. Do que vimos temos $\cap_{i=1}^{g}\mathfrak{p}_i = \mathfrak{R} = (0)$ e fazendo $r = g$ na equação (2.6.2) temos

$$B = \prod_{i=1}^{g} B/\mathfrak{p}_i.$$

Para cada i, $B/\mathfrak{p}_i$ é um corpo e é uma extensão finita de K. Como K é perfeito, esta é uma extensão separável. Pela proposição 1.3.7, $\mathrm{disc}((B/\mathfrak{p}_i)/K) \neq 0$ para cada i. Pelo lema anterior, $\mathrm{disc}(B/K) \neq 0$. □

THEOREM 2.6.7. *Seja A um domínio de Dedekind com um corpo numérico K (extensão finita de $\mathbb{Q}$) como corpo de frações e seja $L \geq K$ uma extensão finita. Assuma que $B = A_L$ é um A-módulo livre. Então um primo $\mathfrak{p}$ ramifica-se em L se e somente se $\mathfrak{p} \mid (\mathrm{disc}(B/A))$ (ideal gerado). Em particular, apenas uma quantidade finita de ideais primos ramificam-se.*

DEMONSTRAÇÃO. Seja $\mathfrak{p}$ um ideal primo de A. Pelo lema 2.6.3 temos que

$$\mathrm{disc}(B/A) \mod \mathfrak{p} \equiv \mathrm{disc}\left((B/\mathfrak{p}B)\,/\,(A/\mathfrak{p})\right) \quad .$$

Da hipótese segue que $A/\mathfrak{p}$ é extensão finita de $\mathbb{F}_p$ onde $p = \mathfrak{p} \cap \mathbb{Z}$ e é portanto perfeito [**Rom95**, pg.94]. Do lema 2.6.6, $\mathrm{disc}\left((B/\mathfrak{p}B)\,/\,(A/\mathfrak{p})\right) = 0$ se e somente se $B/\mathfrak{p}B$ não é reduzido. Seja $\mathfrak{p}B = \prod \mathfrak{P}_i^{e_i}$. Então $B/\mathfrak{p}B \cong \prod (B/\mathfrak{P}_i^{e_i})$ e é claro que este último é reduzido se e somente se cada um dos seus fatores é reduzido que por sua vez são reduzidos se e somente se seus respectivos $e_i = 1$. □

Vejamos agora um resultado que ajuda no cálculo da fatoração de um ideal em uma extensão. Em seguida veremos alguns exemplos de fatorações de ideais.

THEOREM 2.6.8. *Seja A um domínio de Dedekind com corpo de frações K e seja B o fecho inteiro de A em uma extensão finita e separável $L \geq K$. Escreva $B = A[\alpha]$ e seja $f(X)$ o polinômio mínimo de α sobre K. Seja $\mathfrak{p}$ um ideal primo de A e sejam $g_1(X), ..., g_r(X) \in A[X]$ distintos e irredutíveis módulo $\mathfrak{p}$ tais que $f(X) \equiv \prod g_i(X)^{e_i} \mod \mathfrak{p}$. Então*

$$\mathfrak{p}B = \prod (\mathfrak{p}, g_i(\alpha))^{e_i}$$

é a fatoração de $\mathfrak{p}B$ em produto de potência de ideais primos distintos. Além disso, o corpo resíduo $B/(\mathfrak{p}, g_i(\alpha)) \cong ((A/\mathfrak{p})[X])/(\overline{g_i})$ de modo que o índice de inércia $f_i((\mathfrak{p}, g_i(\alpha))/\mathfrak{p})$ é igual ao grau de g_i.

DEMONSTRAÇÃO. Por hipótese, a aplicação $A[X]/(f(X)) \longrightarrow B$ dada por $X \longmapsto \alpha$ é um isomorfismo. Tomando o produto tensorial com $A/\mathfrak{p}$ obtemos o isomorfismo

$$K[X]/(\overline{f}(X)) \longrightarrow B/\mathfrak{p}B;\ X \longmapsto \alpha$$

onde $K = A/\mathfrak{p}$. É claro que $(\overline{g_1}), (\overline{g_2}), ..., (\overline{g_r})$ são ideais maximais de $K[X]/(\overline{f}(X))$. Na realidade, estes são todos os ideais maximais pois, pelo segundo teorema do homomorfismo, um ideal maximal de $K[X]/(\overline{f}(X))$ deve corresponder a um ideal $(\overline{h}(X)) \supseteq (\overline{f}(X))$ (lembre-se que $K[X]$ é principal) e, portanto, $h \mid f \mod \mathfrak{p}$ e $h \equiv g_i \mod \mathfrak{p}$ para algum i. Agora, o ideal $(\overline{g_i})$ em $K[X]/(\overline{f}(X))$ corresponde ao ideal $(g_i(\alpha)) + \mathfrak{p}B$ em $B/\mathfrak{p}B$ que, por sua vez, corresponde ao ideal $(g_i(\alpha), \mathfrak{p})$ em B. Como a maximalidade é preservada por estas correspondências segue que $(g_i(\alpha), \mathfrak{p}),\ 1 \leq i \leq r$ são todos os ideais maximais (primos) de B contendo $\mathfrak{p}$. Ou seja, são todos os ideais primos que dividem $\mathfrak{p}$.

Agora note que $\prod (\overline{g_i}(X))^{e_i} = \left(\overline{f}(X)\right) = (0)$ em $K[X]/(f(X))$ e que nenhum produto com expoentes menores é nulo. Escreva $\mathfrak{p}B = \prod (g_i(\alpha), \mathfrak{p})^{e_i'}$ e note que os e_i' são caracterizados pelo fato que $\mathfrak{p}B \supseteq \prod (g_i(\alpha), \mathfrak{p})^{e_i'}$ mas $\mathfrak{p}B$ não contem nenhum produto com qualquer e_i' substituído por algum valor menor. Isto é, e_i' são os menores expoentes tais que $\prod (g_i(\alpha), \mathfrak{p})^{e_i'} = (0)$ em $B/\mathfrak{p}B$. Como $K[X]/\left(\overline{f}(X)\right) \cong B/\mathfrak{p}B$ com as substituições $(\overline{g_i}(\alpha)) \longleftrightarrow (g_i(\alpha), \mathfrak{p})$ segue que $e_i' = e_i\ \forall i$.

O restante do teorema (que $B/(g_i(\alpha), \mathfrak{p}) \cong K[X]/(\overline{g_i}(X))$) está implícito do demonstrado acima. □

OBSERVAÇÃO 2.6.9. Observe que o teorema acima, quando aplicável (os elementos primitivos podem não ser inteiros), pode ser usado para provar os teoremas 2.6.2 e 2.6.7. De fato, sabemos que $d = \deg(f)$ e, portanto, a equação $d = \sum e_i f_i$ é, pelo teorema anterior, apenas a equação $\deg(f) = \sum e_i \deg(g_i)$. Também, $\operatorname{disc}(B/A) = \operatorname{disc}(f(X))$ e este é divisível por $\mathfrak{p}$ se e somente se

$$\operatorname{disc}(f(X)) \equiv 0 \mod \mathfrak{p} \iff \operatorname{disc}(\overline{f}(X)) = 0$$

o que ocorre se e somente se $\overline{f}(X)$ tem fatores repetidos, isto é, algum $e_i > 1$. Note também que o teorema acima apesar de ser em certo sentido uma especialização do teorema 2.6.7, ele ainda é válido no contexto de corpos de funções coisa que não é verdade neste último.

Note que se $B = A[\alpha]$ então B é livre e $\mathrm{D}\left(1, \alpha, ..., \alpha^{m-1}\right) = \operatorname{disc}(B/A)$ $(m = [L : K])$. Agora, a conclusão do teorema acima ainda é válida no caso em que B não é livre (em particular, $B \neq A[\alpha],\ \forall \alpha \in B$) mas existe $\alpha \in B$ tal que $\mathrm{D}\left(1, \alpha, ..., \alpha^{m-1}\right) = \mathfrak{a} \operatorname{disc}(B/A)$ com $\mathfrak{a}$ ideal de A não-divisível por $\mathfrak{p}$. A demonstração não é difícil [**Mil98a**, pg.53, Observação 3.45].

Vejamos agora alguns exemplos.

EXEMPLO 2.6.10. Seja $m \neq 1$ um inteiro livre de quadrado. Consideremos as possíveis fatorações de inteiros primos de $K = \mathbb{Q}[\sqrt{m}]$. Lembremos que do exemplo 1.3.21 temos $\mathrm{D}(1, \sqrt{m}) = 4m$ e que $\mathrm{disc}(\mathbb{Z}_K/\mathbb{Z}) = \mathrm{D}(1, \sqrt{m})$ se $m \equiv 2, 3 \mod 4$ e $\mathrm{disc}(\mathbb{Z}_K/\mathbb{Z}) = \mathrm{D}(1, \sqrt{m})/4$ se $m \equiv 1 \mod 4$. De qualquer maneira, pela observação anterior podemos olhar para $\mathrm{Irr}(\sqrt{m}, \mathbb{Q}) = X^2 - m$ para decidirmos sobre a fatoração de um primo $p \in \mathbb{Z}$ ímpar ($\neq 2$). O teorema 2.6.2 nos dá três possibilidades:
(p) ramifica-se ($(p) = \mathfrak{p}^2;\ e = 2,\ f = 1,\ g = 1$)
(p) permanece primo ($(p) = \mathfrak{p};\ e = 1,\ f = 2,\ g = 1$)
(p) decompõe-se ($(p) = \mathfrak{p}_1\mathfrak{p}_2;\ e = 1,\ f = 1,\ g = 2$)
Se $p \mid \mathrm{disc}(\mathbb{Z}_K/\mathbb{Z})$ temos do teorema 2.6.7 que p ramifica-se. Se $p \nmid \mathrm{disc}(\mathbb{Z}_K/\mathbb{Z})$ então $p \nmid m$ e é fácil ver que p decompõe-se se e somente se $m \equiv n^2 \mod p$. Caso contrário, $X^2 - m$ é irredutível módulo p e p permanece primo. Para o caso $p = 2$ e $m \equiv 1 \mod 4$ já sabemos que p não ramifica-se. Afirmamos que p decompõe-se se e somente se $m \equiv 1 \mod 8$ e p permanece primo se e somente se $m \equiv 5 \mod 8$. Para vermos isso usamos que $B = A[\alpha]$ onde (já vimos) $\alpha = (1 + \sqrt{m})/2$. Temos que $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^2 - X + (1 - m)/4$. Se $m \equiv 1 \mod 8$ então $\mathrm{Irr}(\alpha, \mathbb{Q}) \equiv X^2 + X \mod 2$ que fatora-se em $X(X + 1)$ donde $(2) = (2, \alpha)(2, 1 + \alpha)$. Se $m \equiv 5 \mod 8$ então $\mathrm{Irr}(\alpha, \mathbb{Q}) \equiv X^2 + X + 1 \mod 2$ que é irredutível donde $(2) = (2, 1 + \alpha + \alpha^2) = (2)$.

É sabido que $\mathbb{Z}[i]$ é um domínio principal (um domínio euclidiano em realidade). Afirmamos que para um primo $p \in \mathbb{Z}$ tem-se $p \equiv 1 \mod 4$ se e somente se (p) decompõe-se em $\mathbb{Z}[i]$ ou ainda, existem inteiros a e b tais que $p = a^2 + b^2$. De fato, pelo exemplo anterior, (p) decompõe-se se e somente se $-1 \equiv n^2 \mod p$ então $n \mod p$ é uma raiz quarta da unidade. Ou seja, $\mathbb{F}_p^\times$ contém um elemento de ordem 4. Como este último é um grupo cíclico de ordem $p - 1$ temos que isto acontece se e somente se $4 \mid p - 1$. Para a segunda equivalência observe que se $(p) = \mathfrak{p}_1\mathfrak{p}_2$ em $\mathbb{Z}[i]$ então $\mathfrak{p}_1 = (a + ib)$, $\mathfrak{p}_2 = (a - ib)$ pois $\mathbb{Z}[i]$ é principal. Logo, $p \equiv u^2(a^2 + b^2),\ u \in \mathbb{Z}[i]^\times$. A recíproca é evidente.

2.7. Extensões de Eisenstein

Lembremos que o critério de Eisenstein dizia que se um polinômio

$$X^m + a_1X^{m-1} + ... + a_m,\ a_i \in \mathbb{Z}$$

é tal que, para algum primo $p \in \mathbb{Z}$, $p \mid a_i$, $\forall i$ e $p^2 \nmid a_m$ então este polinômio é irredutível em $\mathbb{Q}[X]$. Nesta seção vamos generalizar este resultado.

Seja A um domínio de Dedekind e, como de costume, B seu fecho inteiro em uma extensão finita e separável L de seu corpo de frações K. Seja $\mathfrak{p}$ um primo de A e $\mathfrak{P}$ um primo de B que divide $\mathfrak{p}$. Sendo $e = e(\mathfrak{P}/\mathfrak{p})$ e $v_\mathfrak{p}$, $v_\mathfrak{P}$ as valorizações discretas normalizadas associadas a $\mathfrak{p}$ e $\mathfrak{P}$ é fácil ver que $v_\mathfrak{P}|_K = ev_\mathfrak{p}$.

LEMA 2.7.1. *Mantendo a notação acima, e sendo* $a_1, ..., a_n \in B$ *tais que* $\sum a_i = 0$ *tem-se que o valor mínimo de* $\{v_{\mathfrak{P}}(a_i)\}_{i=1}^n$ *é atingido pelo menos duas vezes.*

DEMONSTRAÇÃO. Suponha que não. Sem perda de generalidade, podemos supor que $v_{\mathfrak{P}}(a_1) < v_{\mathfrak{P}}(a_i)\,, \forall i > 1$. Mas então

$$v_{\mathfrak{P}}(a_1) = v_{\mathfrak{P}}(-a_1) = v_{\mathfrak{P}}\left(\sum_{i=2}^{n} a_i\right) \geq \min_{2\leq i\leq n}\left(v_{\mathfrak{P}}(a_i)\right) > v_{\mathfrak{P}}(a_1)$$

e temos um absurdo. □

DEFINIÇÃO 2.7.2. Seja A um domínio de Dedekind e $\mathfrak{p}$ um primo de A. Um polinômio $X^m + a_1X^{m-1} + ... + a_m,\ a_i \in A$ é dito ser de Eisenstein relativo a $\mathfrak{p}$ se e somente se $v_{\mathfrak{p}}(a_i) > 0,\ 1 \leq i \leq m-1$ e $v_{\mathfrak{p}}(a_m) = 1$.

THEOREM 2.7.3. *Seja* A *um domínio de Dedekind com* $\mathrm{ff}(A) = K$ *perfeito e* $f(X) \in A[X]$ *um polinômio de Eisenstein relativo a* $\mathfrak{p} \in \mathrm{Spec}(A)$. *Então* f *é irredutível em* $A[X]$ *e se* α *é uma raiz de* f *então* $\mathfrak{p}$ *é totalmente ramificado em* $K[\alpha]$. *De fato, tem-se* $\mathfrak{p}B = \mathfrak{P}^m$ *com* $\mathfrak{P} = (\mathfrak{p}, \alpha)$ *e* $m = \deg(f)$. *Tais extensões são denominadas extensões de Eisenstein.*

DEMONSTRAÇÃO. Seja $L = K[\alpha]$ então temos $[L : K] \leq m$. Seja $\mathfrak{P}$ um primo de A_L dividindo $\mathfrak{p}$ com índice de ramificação e. Temos a equação

$$\alpha^m + a_1\alpha^{m-1} + ... + a_m = 0.$$

Como f é de Eisenstein temos as relações

$$\begin{aligned} &v_{\mathfrak{P}}(\alpha^m) = mv_{\mathfrak{P}}(\alpha) \\ &v_{\mathfrak{P}}\left(a_i\alpha^{m-i}\right) \geq (m-i)v_{\mathfrak{P}}(\alpha) + e;\ 1 \leq i \leq m-1 \\ &v_{\mathfrak{P}}(a_m) = e \quad . \end{aligned}$$

Pelo lema devemos ter $v_{\mathfrak{P}}(\alpha) \neq 0$ donde $v_{\mathfrak{P}}(a_i\alpha^{m-i}) > v_{\mathfrak{P}}(a_m) = e,\ 1 \leq i \leq m-1$ e, novamente, pelo lema temos que $mv_{\mathfrak{P}}(\alpha) = e$. Logo,

$$mv_{\mathfrak{P}}(\alpha) = e \leq [L : K] \leq m$$

e devemos ter $[L : K] = m = e$. A primeira igualdade implica que $f = \mathrm{Irr}(\alpha, K)$ e a segunda com o teorema 2.6.2 nos diz que $f(\mathfrak{P}/\mathfrak{p}) = 1 = g$ donde $\mathfrak{p}B = \mathfrak{P}^m$ onde $\mathfrak{P} = (\mathfrak{p}, \alpha)$ pelo teorema 2.6.8 (note que α é inteiro donde $A_L = A[\alpha]$ e caímos na hipótese do teorema e neste caso $f(X) \equiv X^m \mod \mathfrak{p}$). □

OBSERVAÇÃO 2.7.4. Note que como A não é, em geral, domínio fatorial não podemos usar o famoso lema de Gauss para concluir que f é irredutível em $K[X]$ (como no caso do critério de Eisenstein clássico).

Parte 2

Os Teoremas de Finitude no Caso de Corpos Numéricos

Nesta segunda parte, estaremos considerando K sempre um corpo numérico, isto é, uma extensão (finita) de $\mathbb{Q}$. Vamos demonstrar para tais corpos dois resultados fundamentais: a finitude do número de classe e o teorema das unidades de Dirichlet. O primeiro afirma exatamente o que diz seu nome: o número de classe é finito. Sua demonstração é extremamente elegante e inusitada. Sua importância está no fato que ele torna o problema de fatorização (de ideais) nos anéis de inteiros destes corpos tratável e bem parecidos com o caso dos inteiros (racionais). O segundo teorema se parece muito com o primeiro em sua demonstração. Ele afirma que o grupo das unidades dos inteiros destes corpos é finitamente gerado.

CAPíTULO 3

A finitude do número de classe

Neste capítulo provaremos que no caso de um corpo numérico (uma extensão de $\mathbb{Q}$) o número de classe é finito. Nas primeiras três seções vamos introduzir o ferramental da demonstração: vamos generalizar o conceito de norma de elementos para ideais fracionários, introduzir o conceito de reticulados e demonstrar o famoso teorema de Minkowski da geometria dos números e demonstrar mais alguns lemas. Na última seção temos a demonstração da finitude do número de classe propriamente dita.

3.1. A norma de um ideal fracionário

Seja A um domínio de Dedekind com corpo de frações K, $L \geq K$ uma extensão finita separável e $B = A_L$. Vimos que $\mathrm{Nm}_{L/K} : L^\times \longrightarrow K^\times$ é um homomorfismo de grupo. Também vimos que $\mathrm{Id}\,(A)$ e $\mathrm{Id}(B)$ são grupos abelianos livres gerados pelos ideais primos de A e B respectivamente. Queremos definir um homomorfismo $\mathcal{N} : \mathrm{Id}(B) \longrightarrow \mathrm{Id}(A)$ que comute com Nm. Isto é tal que o diagrama abaixo comute:

$$\begin{array}{ccc} L^\times & \longrightarrow & \mathrm{Id}(B) \\ \Big\downarrow{\scriptstyle Nm} & & \Big\downarrow{\scriptstyle \mathcal{N}} \\ K^\times & \longrightarrow & \mathrm{Id}(A) \end{array} \tag{3.1.1}$$

onde os homomorfismos horizontais mapeiam elementos de K e L nos respectivos ideais principais. Como $\mathrm{Id}(B)$ é livre sobre os ideais primos, só precisamos definir $\mathcal{N}\,(\mathfrak{P})$ para $\mathfrak{P}$ primo de B.

Seja $\mathfrak{p}$ um primo de A e escreva $\mathfrak{p}B = \prod \mathfrak{P}_i^{e_i}$. Se $\mathfrak{p}$ é principal, digamos $\mathfrak{p} = (\pi)$, então de (3.1.1) devemos ter

$$\mathcal{N}\,(\mathfrak{p}B) = \mathcal{N}\,(\pi B) = (\mathrm{Nm}\,(\pi))\,A = (\pi^m) = \mathfrak{p}^m \tag{3.1.2}$$

onde $m = [L : K]$. Por outro lado, como $\mathcal{N}$ é pra ser homomorfismo devemos ter:

$$\mathcal{N}\,(\mathfrak{p}B) = \mathcal{N}\left(\prod \mathfrak{P}_i^{e_i}\right) = \prod \left(\mathcal{N}\,(\mathfrak{P}_i)\right)^{e_i}. \tag{3.1.3}$$

Comparando as equações (3.1.2) e (3.1.3) e lembrando de 2.6.2 que $m = \sum e_i f_i$ vemos que devemos definir $\mathcal{N}\,(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$.

DEFINIÇÃO 3.1.1. Definimos a norma de um ideal primo $\mathfrak{P}$ de B como sendo o ideal $\mathcal{N}(\mathfrak{P}) := \mathfrak{p}^f$ de A onde $\mathfrak{p} = \mathfrak{P} \cap A$ e $f = f(\mathfrak{P}/\mathfrak{p}) = [B/\mathfrak{P} : A/\mathfrak{p}]$. Estendendo livremente para o grupo $\mathrm{Id}(B)$ obtemos um homomorfismo $\mathcal{N} : \mathrm{Id}(B) \longrightarrow \mathrm{Id}(A)$.

Vimos que Nm é transitiva sobre uma torre de corpos. Da nossa definição, $\mathcal{N}$ também é pois isso remonta ao fato que os índices de inércia o são. Isto é $f(\mathfrak{Q}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{p})$ se $\mathfrak{Q}$ é um primo que divide $\mathfrak{P}$ em uma extensão M de L. Vamos agora demonstrar que nossa definição é, de fato, correta, ou seja, que (3.1.1) comuta.

PROPOSIÇÃO 3.1.2. *Sejam $A \leq B$ e $K \leq L$ como acima.*

(1) *Para todo ideal fracionário $\mathfrak{a}$ de A, $\mathcal{N}_{L/K}(\mathfrak{a}B) = \mathfrak{a}^m$ onde $m = [L : K]$.*

(2) *Suponha que L é Galoisiano sobre K. Seja $\mathfrak{P}$ um primo, não-nulo, de B e $\mathfrak{p} = \mathfrak{P} \cap A$. Escreva*[1] *$\mathfrak{p}B = (\mathfrak{P}_1...\mathfrak{P}_g)^e$ Então*

$$\left(\mathcal{N}_{L/K}(\mathfrak{P})\right) B = \left(\mathfrak{p}^f\right) B = (\mathfrak{P}_1...\mathfrak{P}_g)^{ef} = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\mathfrak{P}$$

(3) *Para todo elemento $\zeta \in L$, $\left(\mathrm{Nm}_{L/K}(\zeta)\right) A = \mathcal{N}_{L/K}(\zeta B)$, isto é, (3.1.1) comuta.*

DEMONSTRAÇÃO. (1) É suficiente demonstrarmos o afirmado para um ideal primo $\mathfrak{p}$ de A. Neste caso,

$$\mathcal{N}(\mathfrak{p}B) = \mathcal{N}\left(\prod \mathfrak{P}_i^{e_i}\right) = \prod \mathcal{N}(\mathfrak{P}_i)^{e_i} = \prod \mathfrak{p}^{e_i f_i} = \mathfrak{p}^{\sum e_i f_i} = \mathfrak{p}^m$$

onde usamos o teorema 2.6.2. Como $\mathcal{N}(\mathfrak{P}_i) = \mathfrak{p}^f$ para todo i, em particular para $\mathfrak{P}$, temos

$$\left(\mathcal{N}(\mathfrak{p})\right) B = \left(\mathfrak{p}^f\right) B = (\mathfrak{p}B)^f = (\mathfrak{P}_1...\mathfrak{P}_g)^{ef}.$$

(2) Agora, vimos no teorema 2.6.2 que $\mathrm{Gal}(L/K)$ age transitivamente no conjunto $\{\mathfrak{P}_1...\mathfrak{P}_g\}$. É um exercício fácil de teoria de grupos ver que cada $\mathfrak{P}_i$ aparece $m/g = ef$ (novamente usando 2.6.2) vezes na família $\{\sigma\mathfrak{P} : \sigma \in \mathrm{Gal}(L/K)\}$. O resultado segue imediatamente.

(3) Suponha, inicialmente, que L é Galois sobre K. A aplicação $\iota : \mathrm{Id}(A) \longrightarrow \mathrm{Id}(B)$ dada por $\mathfrak{a} \longmapsto \mathfrak{a}B$ é injetora pois ela o é nos geradores de $\mathrm{Id}(A)$. Assim, para mostrarmos que $\mathrm{Nm}(\zeta) A = \mathcal{N}(\zeta B)$ é suficiente mostrarmos que $(\mathrm{Nm}(\zeta)) B = \iota(\mathrm{Nm}(\zeta) A) = \iota(\mathcal{N}(\zeta B)) = (\mathcal{N}(\zeta B)) B$. Sabemos que $B = \sum A\beta_i$ para um conjunto finito de β_i. Então $\sigma(\zeta B) = \sigma(\zeta \sum A\beta_i) = \sigma(\zeta) \sum A\sigma(\beta_i) = \sigma(\zeta) B$ onde na última igualdade usamos o lema 1.3.13. Assim,

$$(\mathcal{N}(\zeta B)) B = \prod \sigma(\zeta B) = \prod (\sigma(\zeta) B) = \left(\prod \sigma(\zeta)\right) B = (\mathrm{Nm}(\zeta)) B.$$

Para o caso geral, seja E uma extensão Galoisiana finita de K contendo L e $d := [E : L]$. Sendo $C = \overline{B}$ em E, pelo item 1., do caso anterior e como a norma é transitiva temos:

$$\left(\mathcal{N}_{L/K}(\zeta B)\right)^d = \mathcal{N}_{E/K}(\zeta C) = \left(\mathrm{Nm}_{E/K}(\zeta)\right) A = \left(\mathrm{Nm}_{L/K}(\zeta)\right)^d A.$$

[1] Lembremos do teorema 2.6.2

Como $\mathrm{Id}(A)$ é livre segue que $\mathcal{N}_{L/K}(\zeta B) = \left(\mathrm{Nm}_{L/K}(\zeta)\right) A$ como queríamos. □

DEFINIÇÃO 3.1.3. Seja $\mathfrak{a}$ um ideal e não-nulo em um anel de inteiros $\mathbb{Z}_K$ de um corpo numérico K. Então pela observação 1.3.5, $\mathfrak{a}$ tem índice finito em $\mathbb{Z}_K$. Definimos a norma numérica de $\mathfrak{a}$, que denotamos por $\mathbb{N}(\mathfrak{a})$, como sendo este índice. Isto é, $\mathbb{N}(\mathfrak{a}) := (\mathbb{Z}_K : \mathfrak{a})$.

PROPOSIÇÃO 3.1.4. *Seja $\mathbb{Z}_K$ o anel de inteiros de um corpo numérico K.*

(1) *Para todo ideal $\mathfrak{a}$ em $\mathbb{Z}_K$, $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) = (\mathbb{N}(\mathfrak{a}))$ e, portanto, $\mathbb{N}(\mathfrak{ab}) = \mathbb{N}(\mathfrak{a})\mathbb{N}(\mathfrak{b})$.*

(2) *Sejam $\mathfrak{b} \subseteq \mathfrak{a}$ ideais fracionários em K então $(\mathfrak{a} : \mathfrak{b}) = \mathbb{N}\left(\mathfrak{a}^{-1}\mathfrak{b}\right)$.*

DEMONSTRAÇÃO. (1) Escreva $\mathfrak{a} = \prod \mathfrak{P}_i^{r_i}$ e sejam $f_i = f(\mathfrak{P}_i/(p_i))$ onde $(p_i) = \mathbb{Z} \cap \mathfrak{P}_i$. Então $\mathcal{N}(\mathfrak{P}_i) = (p_i)^{f_i}$. Pelo teorema chinês do resto, $\mathbb{Z}_K/\mathfrak{a} \cong \prod \mathbb{Z}_K/\mathfrak{P}_i^{r_i}$ donde $(\mathbb{Z}_K : \mathfrak{a}) = \prod (\mathbb{Z}_K : \mathfrak{P}_i^{r_i})$. No decorrer da prova do teorema 2.6.2 mostramos que $[\mathbb{Z}_K/\mathfrak{P}_i^{r_i} : \mathbb{Z}/(p_i)] = f_i r_i$. Assim,

$$\prod (\mathbb{Z}_K : \mathfrak{P}_i^{r_i}) = \prod (\mathbb{Z} : p_i\mathbb{Z})^{f_i r_i} = \prod p_i^{f_i r_i} \implies (\mathbb{N}(\mathfrak{a})) = \left(\prod p_i^{f_i r_i}\right) = \prod (p_i)^{f_i r_i} = \mathcal{N}(\mathfrak{a}).$$

A multiplicatividade de $\mathbb{N}$ segue agora da de $\mathcal{N}$.

(2) Suponha, inicialmente, que $\mathfrak{a}$ e $\mathfrak{b}$ são inteiros. Então $\mathfrak{a}^{-1}\mathfrak{b}$ é inteiro e, por 1., $\mathbb{N}(\mathfrak{a})\mathbb{N}\left(\mathfrak{a}^{-1}\mathfrak{b}\right) = \mathbb{N}(\mathfrak{b})$ donde

$$\mathbb{N}\left(\mathfrak{a}^{-1}\mathfrak{b}\right) = \frac{\mathbb{N}(\mathfrak{b})}{\mathbb{N}(\mathfrak{a})} = (\mathfrak{a} : \mathfrak{b}).$$

Para $\mathfrak{a}$ e $\mathfrak{b}$ arbitrários, note que existem d_1 e $d_2 \in \mathbb{Z}_K$ tais que $d_1\mathfrak{a}, d_2\mathfrak{b} \subseteq \mathbb{Z}_K$, isto é, $d_1\mathfrak{a}$ e $d_2\mathfrak{b}$ são ideais inteiros. Tomando $d = d_1 d_2$ temos $d\mathfrak{a}, d\mathfrak{b} \subseteq \mathbb{Z}_K$. Agora, $x \longmapsto dx$ é um isomorfismo de $\mathbb{Z}_K$-módulos donde $(d\mathfrak{a} : d\mathfrak{b}) = (\mathfrak{a} : \mathfrak{b})$. Assim, pelo caso anterior, temos $(\mathfrak{a} : \mathfrak{b}) = (d\mathfrak{a} : d\mathfrak{b}) = \mathbb{N}\left((d\mathfrak{a})^{-1}(d\mathfrak{b})\right) = \mathbb{N}\left(\mathfrak{a}^{-1}\mathfrak{b}\right)$. □

3.2. Reticulados

DEFINIÇÃO 3.2.1. Seja V um espaço vetorial de dimensão n sobre $\mathbb{R}$. Um reticulado em V é um subgrupo da forma $\Lambda = \mathbb{Z}e_1 \oplus ... \oplus \mathbb{Z}e_r$ com $\{e_1, ..., e_r\}$ linearmente independentes em V. Ou seja, um reticulado é um grupo abeliano livre gerado por elementos linearmente independentes de V. Quando $r = n$ dizemos que o reticulado é saturado.

Em termos do produto tensorial podemos dizer que um reticulado é saturado quando ao estendermos os escalares para $\mathbb{R}$ obtemos um isomorfismo, isto é $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \cong V$ pela aplicação $\sum \zeta_i \otimes \lambda_i \longmapsto \sum \zeta_i \lambda_i$.

EXEMPLO 3.2.2. O subgrupo $\mathbb{Z} + \mathbb{Z}\sqrt{2} \leq \mathbb{R}$ é grupo abeliano livre de posto 2 pois $\sqrt{2}$ é irracional, no entanto, ele não é um reticulado em $\mathbb{R}$ pois 1 e $\sqrt{2}$ são linearmente dependentes em $\mathbb{R}$.

A escolha de uma base para V determina um isomorfismo de V com $\mathbb{R}^n$ e, portanto, uma topologia em V que o torna um espaço vetorial topológico (as operações de soma e produto por escalar são contínuas). Tal topologia independe da base pois todo $\mathbb{R}$-automorfismo de

$\mathbb{R}^n$ é homeomorfismo. Um subgrupo Λ de V é dito discreto se ele é discreto na topologia induzida por V. Lembrando que um espaço topológico é discreto se e somente se todos os seus pontos (e, portanto, todos seus subconjuntos) são abertos, temos que Λ é discreto se e somente se todo ponto λ de Λ possui uma vizinhança U em V tal que $U \cap \Lambda = \{\lambda\}$.

Vamos demonstrar agora uma proposição que nos dá outro critério para decidir se um subgrupo Λ de V é um reticulado. Antes, um lema:

LEMA 3.2.3. *As seguintes condições em um subgrupo Λ de um espaço vetorial real V são equivalentes:*

(1) *Λ é um subgrupo discreto.*
(2) *Existe um aberto U de V tal que $U \cap \Lambda = \{0\}$*
(3) *Todo compacto de V intersecta Λ em um conjunto finito.*
(4) *Todo conjunto limitado de V intersecta Λ em um conjunto finito.*

DEMONSTRAÇÃO. (1. $\iff$ 2.) É claro que 1. $\implies$ 2.. Para a recíproca note que $x \longmapsto \lambda + x$ é um homeomorfismo para todo $\lambda \in V$. Assim, se U é como em 2. então $\lambda + U$ é vizinhança de λ tal que $(\lambda + U) \cap \Lambda = \{\lambda\}$.

(1. $\implies$ 3.) Se $K \subseteq V$ é compacto então como $K \cap \Lambda$ é fechado em um compacto ele é compacto. Por outro lado, $K \cap \Lambda$ é discreto donde $K \cap \Lambda$ é finito.

(3. $\implies$ 4.) É evidente visto que todo conjunto limitado de V é pré-compacto, isto é, possui fecho compacto.

(4. $\implies$ 2.) Seja V uma vizinhança limitada de 0. Então $S := (U \cap \Lambda) \backslash \{0\}$ é finito por 4. e, portanto, fechado. Assim, $U \backslash S$ é uma vizinhança aberta de 0 tal que $(U \backslash S) \cap \Lambda = \{0\}$ □

PROPOSIÇÃO 3.2.4. *Um subgrupo Λ de V é um reticulado se e somente se ele é discreto.*

DEMONSTRAÇÃO. É claro que um reticulado é discreto. Reciprocamente, seja Λ um subgrupo discreto de V e $\{e_1, ..., e_r\}$ um subconjunto linearmente independente maximal (em relação a quantidade de elementos) de Λ. Procedemos por indução sobre r.

Se $r = 0$ então $\Lambda = \{0\}$ e não há nada à provar.

Se $r = 1$ então todo $\lambda \in \Lambda$ se escreve como $\lambda = \zeta e_1$, $\zeta \in \mathbb{R}$. Como Λ é discreto, pelo lema anterior, $\{\zeta e_1 : |\zeta| < M\} \cap \Lambda$ é finito donde existe $f_1 \in \Lambda$ tal que $f_1 = \zeta_1 e_1$ com $\zeta_1 > 0$ mínimo. Afirmamos que $\Lambda = \mathbb{Z} f_1$. Suponha que $\lambda \in \Lambda$ mas $\lambda \notin \mathbb{Z} f_1$. Então existe $m \in \mathbb{Z}$ tal que $\lambda - m f_1 = b f_1$ com $0 < b < 1$. Mas então $\Lambda \ni \lambda - m f_1 = b f_1 = b \zeta_1 e_1$ com $0 < b\zeta_1 < \zeta_1$ contrariando a escolha de f_1.

Provemos para r. Seja $\Lambda' = \Lambda \cap (\mathbb{R} e_1 + ... + \mathbb{R} e_{r-1})$ que é um subgrupo discreto de $V' := \mathbb{R} e_1 + ... + \mathbb{R} e_{r-1}$. Pela hipótese de indução, $\Lambda' = \mathbb{Z} f_1 + ... + \mathbb{Z} f_{r-1}$ para alguns f_i linearmente independentes sobre $\mathbb{R}$ que, portanto, também formam uma base para V'. Todo elemento $\lambda \in \Lambda$ se escreve de forma única como $\lambda = \zeta_1 f_1 + ... + \zeta_{r-1} f_{r-1} + \zeta e_r$, $\zeta_i, \zeta \in \mathbb{R}$. Seja $\varphi : \Lambda \longrightarrow \mathbb{R}$ dada por $\lambda \longmapsto \zeta$ e seja $\Lambda'' := \mathrm{Im}\,(\varphi)$. Note que ζ também é imagem de $\Lambda \ni (\zeta_1 - [\zeta_1]) f_1 + ... + (\zeta_{r-1} - [\zeta_{r-1}]) f_{r-1} + \zeta e_r$ onde $[x]$ denota o maior inteiro menor

ou igual à x (função parte inteira). Assim, todo elemento $\zeta \in \{\zeta \in \Lambda'' : 0 \leq |\zeta| < M\}$ é imagem de um elemento de Λ no conjunto limitado $\{\lambda \in \Lambda : 0 \leq \zeta_i < 1, |\zeta| < M\}$. Pelo lema anterior, existem finitos λ´s neste último conjunto e, portanto, finitos ζ´s no primeiro. Pelo caso $r = 1$ segue que Λ'' é um reticulado em $\mathbb{R}$, digamos $\Lambda'' = \mathbb{Z}\varphi(f_r),\ f_r \in \Lambda$.

Seja agora $\lambda \in \Lambda$ fixo. Então $\varphi(\lambda) = m\varphi(f_r),\ m \in \mathbb{Z}$ logo $\varphi(\lambda - mf_r) = 0$ donde $\lambda - mf_r \in \Lambda'$ e este pode ser escrito como $\lambda - mf_r = m_1 f_1 + ... + m_{r-1} f_{r-1},\ m_i \in \mathbb{Z}$ donde segue o desejado. □

DEFINIÇÃO 3.2.5. Seja Λ um reticulado saturado em V, digamos, $\Lambda = \sum_{i=1}^{n} \mathbb{Z}e_i$. Para cada $\lambda \in \Lambda$ seja $D_\lambda := \{\lambda + \sum \zeta_i e_i : 0 \leq \zeta_i < 1\}$. Um conjunto desta forma é dito ser um paralelepípedo fundamental para Λ. Está claro que a forma de um paralelepípedo fundamental depende da escolha de uma base para Λ. No entanto, fixado uma base, os paralelepípedos fundamentais cobrem V sem sobreposição.

Sabemos do cálculo que dados elementos $v_1, ..., v_n \in \mathbb{R}^n$ o volume do paralelepípedo determinado por eles tem volume dado por $\mu(P) := |\det(v_1, ..., v_n)|$. Assim, para um reticulado saturado $\Lambda = \sum \mathbb{Z}e_i$ o volume do paralelepípedo fundamental é $\mu(D) = |\det(e_1, ..., e_n)|$ e se também tivermos $\Lambda = \sum \mathbb{Z}f_i$ então a matriz relacionando $\{e_i\}$ com $\{f_i\}$ é inversível em $M_n(\mathbb{Z})$ e, portanto, tem determinante ± 1. Conseqüentemente, o volume de um paralelepípedo fundamental independe da base escolhida para Λ.

Se $\Lambda \supseteq \Lambda'$ são dois reticulados saturados em $\mathbb{R}^n$, podemos escolher geradores $\{e_i\}$ e $\{f_j\}$ para Λ e Λ' tal que $f_i = m_i e_i,\ m_i \in \mathbb{N}^*$ (este é o teorema dos fatores invariantes para módulos livres finitamente gerados sobre um domínio principal e é uma especialização do teorema A.2.11). Com tal escolha, o paralelepípedo fundamental D' de Λ' é união disjunta de $\prod m_i = (\Lambda : \Lambda')$ paralelepípedos fundamentais D de Λ. Temos, portanto, a fórmula:

$$\frac{\mu(D')}{\mu(D)} = (\Lambda : \Lambda'). \tag{3.2.1}$$

Dada uma base para V obtemos um isomorfismo $V \cong \mathbb{R}^n$ e, portanto, uma medida μ invariante por translação. Um outra escolha de base para V nos dá outra medida ν, mas tal que $\nu = \zeta\mu$, $\zeta \in \mathbb{R}^\times$. Portanto, a razão entre as medidas de dois conjuntos está bem definida e, em particular, a fórmula (3.2.1) vale para reticulados em V.

THEOREM 3.2.6. *Seja D_0 um paralelepípedo fundamental para um reticulado saturado Λ em um espaço vetorial real V. Se S é um subconjunto mensurável de V e $\mu(S) > \mu(D_0)$ então S contém pontos $\alpha \neq \beta$ tal que $\alpha - \beta \in \Lambda$.*

DEMONSTRAÇÃO. O conjunto $S \cap D_\lambda$ é mensurável para todo paralelepípedo fundamental D_λ e

$$\mu(S) = \sum_{\lambda \in \Lambda} \mu(S \cap D_\lambda)$$

pois $\{D_\lambda\}$ cobre V sem sobreposição. Para cada D_λ existe um único $\lambda' \in \Lambda$ tal que o transladado de $S \cap D_\lambda$ por λ' é subconjunto de D_0. Como $\mu(S) > \mu(D_0)$, pelo menos

dois desses conjuntos tem intersecção não-vazia (caso contrário teríamos uma cobertura de um subconjunto de D_0 por conjuntos disjuntos da forma $S \cap D_\lambda + \lambda'$ e então $\mu(D_0) \geq \sum \mu(S \cap D_\lambda) = \mu(S)$). Isto é, existem $\alpha, \beta \in S$ tal que $\alpha - \lambda_0 = \beta - \lambda_1$, $\lambda_0 \neq \lambda_1 \in \Lambda$ donde $0 \neq \beta - \alpha \in \Lambda$ como queríamos. □

LEMA 3.2.7. *Seja $T \subseteq V$ mensurável tal que $(\alpha - \beta)/2 \in T$ para todo $\alpha, \beta \in T$ e Λ um reticulado saturado em V. Então T possuirá um ponto do reticulado, distinto da origem, sempre que $\mu(T) > 2^n \mu(D)$ onde $n = \dim V$ e D é um paralelepípedo fundamental de Λ.*

DEMONSTRAÇÃO. Seja $S = (1/2)T$. Então se $\alpha, \beta \in S$ temos $\alpha - \beta = (1/2)(\alpha' - \beta')$, $\alpha', \beta' \in T$ donde $\alpha - \beta \in T$. Pelo teorema anterior, S contém pontos distintos $\alpha \neq \beta \in \Lambda$ sempre que $\mu(S) > \mu(D)$, isto é, $\mu((1/2)T) > \mu(D) \implies (1/2^n)\mu(T) > \mu(D) \implies \mu(T) > 2^n \mu(D)$. Neste caso, $T \ni \alpha - \beta \neq 0$ com $\alpha - \beta \in \Lambda$ como queríamos. □

THEOREM 3.2.8. *(Teorema de Minkowski) Seja T um subconjunto de um espaço vetorial real V tal que T é compacto, convexo e simétrico em relação a origem e Λ um reticulado saturado em V. Se $\mu(T) \geq 2^n \mu(D)$ onde $n = \dim V$ e D é um paralelepípedo fundamental de Λ então T possui um ponto da reticulado outro que não a origem.*

DEMONSTRAÇÃO. Seja $\epsilon_0 > 0$. O conjunto $(1 + \epsilon_0)T$ é mensurável e satisfaz a hipótese do lema anterior. Como $\mu((1+\epsilon)T) = (1+\epsilon_0)^n \mu(T) > 2^n \mu(D)$, pelo mesmo lema, $((1+\epsilon_0)T \cap \Lambda) \setminus \{0\} \neq \varnothing$ e é finito pois $(1+\epsilon_0)T$ é compacto. Como T é fechado, temos $T = \cap_{\epsilon > 0}(1+\epsilon)T$. Se nenhum dos finitos pontos de $((1+\epsilon_0)T \cap \Lambda) \setminus \{0\}$ está em T podemos tomar ϵ'suficientemente pequeno tal que $((1+\epsilon')T \cap \Lambda) \setminus \{0\} = \varnothing$ o que é absurdo. □

OBSERVAÇÃO 3.2.9. O teorema anterior foi descoberto por Minkowski em 1896 e foi o ponto de partida de um ramo na teoria de números, hoje já praticamente inativa, denominada geometria dos números. Vamos demonstrar o uso deste teorema provando que todo número natural se escreve como soma de quatro quadrados.

Da identidade

$$\begin{aligned}&\left(a^2+b^2+c^2+d^2\right)\left(A^2+B^2+C^2+D^2\right) = \\ &(aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2+ \\ &(aC-bD+cA+dB)^2+(aD+bC+-cB+dA)^2\end{aligned}$$

vemos que é suficiente mostrarmos que todo primo p se escreve como soma de quatro quadrados. Como $2 = 1^2 + 1^2 + 0^2 + 0^2$ podemos supor p ímpar.

Afirmamos que $m^2 + n^2 + 1 \equiv 0 \mod p$ tem solução em $\mathbb{Z}$. Vamos mostrar que

$$\#\left\{\overline{m}^2 : 0 \leq m \leq p-1\right\} = (p+1)/2$$

pois sendo assim o mesmo vale para $\left\{\overline{n}^2 + \overline{1} : 0 \leq n \leq p-1\right\}$ e então para que a congruência acima não tenha solução deveríamos ter $\overline{m}^2 \neq \overline{n}^2 + \overline{1}$ para todos os $p+1$ valores

que eles assumem o que é impossível. Sejam $a \neq b$ tal que $0 \leq a, b \leq p-1$. Agora, $a^2 \equiv b^2 \mod p \iff (a+b)(a-b) \equiv 0 \mod p \iff a+b \equiv 0 \mod p$ (estamos supondo $a \neq b$). Como $0 \leq a, b \leq p-1$ este último acontece se e somente se $a+b=p$. Assim, sendo $R := \{(a,b) : 0 \leq a, b \leq p-1,\ a \neq b,\ a+b=p\}$ temos $\#R = p-1$ pois $a+b=p$ tem exatamente uma solução se $a>0$ e não tem solução se $a=0$. Agora, se $(a,b) \in R$ então $(b,a) \in R$ sem termos determinado nenhum novo elemento de $S := \left\{\overline{m}^2 : 0 \leq m \leq p-1\right\}$. Logo, $\#S = \#\mathbb{F}_p - \#R/2 = p - (p-1)/2 = (p+1)/2$ como queríamos.

Fixe uma solução m, n para a congruência e considere o reticulado

$$\Lambda := \left\{(a,b,c,d) \in \mathbb{Z}^4 : c \equiv ma+nb \mod p,\ \ d \equiv mb-na \mod p\right\} \subseteq \mathbb{Z}^4$$

(que Λ é um reticulado segue do fato que ele é subgrupo de $\mathbb{Z}^4$ que é discreto donde Λ é discreto). Note que $p\mathbb{Z}^4 \subseteq \Lambda$ donde $\Lambda/p\mathbb{Z}^4 \subseteq \mathbb{Z}^4/p\mathbb{Z}^4 = \mathbb{F}_p^4$ e este é, em realidade, um subespaço vetorial bidimensional de $\mathbb{F}_p^4$ (a e b são arbitrários mas então c e d estarão determinados). Logo, $\left(\mathbb{Z}^4 : \Lambda\right) = p^2$ e pela fórmula (3.2.1), $\mu(D_\Lambda) = \left(\mathbb{Z}^4 : \Lambda\right)\mu(D_{\mathbb{Z}^4}) = p^2$. Seja $T := \overline{B(0,r)}$ o fecho da bola de centro 0 e raio $r>0$ então $\mu(T) = \pi^2 r^4/2$ (do cálculo ou de resultados da próxima seção) de maneira que escolhendo $r^2 > 1.9p$ temos $\mu(T) > 16\mu(D_\Lambda)$. Pelo teorema de Minkowski, existe $(a,b,c,d) \in (\Lambda \backslash \{0\}) \cap T$. Como $(a,b,c,d) \in \Lambda$ temos

$$a^2+b^2+c^2+d^2 \equiv a^2\left(1+m^2+n^2\right) + b^2\left(1+m^2+n^2\right) \mod p$$

e como $(a,b,c,d) \in T$ temos $a^2+b^2+c^2+d^2 < 2p$. Seque que $a^2+b^2+c^2+d^2 = p$ como queríamos.

3.3. Três lemas de cálculo

LEMA 3.3.1. *Sejam $a_1, ..., a_n \in \mathbb{R}_+^\times$. Então $\left(\prod a_i\right)^{1/n} \leq \left(\sum a_i\right)/n$.*

DEMONSTRAÇÃO. Podemos supor $a_1 \leq a_2 \leq ... \leq a_n$. Supondo também que $a_n \leq 1$ mostremos que $n\left(\prod a_i\right)^{1/n} \leq \sum a_i$. Para $n=1$ o resultado é óbvio. Provemos para n:

$$n\left(\prod^n a_i\right)^{1/n} = (n-1)\left(\prod^n a_i\right)^{1/n} + \left(\prod^n a_i\right)^{1/n} \leq$$

$$\leq (n-1)\left(\prod^{n-1} a_i\right)^{1/(n-1)} + a_n \leq \sum^n a_i$$

onde usamos que $a_i \leq a_n \forall i \implies \prod^n a_i \leq a_n^n \implies \left(\prod^n a_i\right)^{1/n} \leq a_n$. Agora para o caso geral (se $a_n > 1$) seja $\lambda > a_n$ donde $\lambda^{-1}a_1 \leq ... \leq \lambda^{-1}a_n \leq 1$ e do demonstrado acima temos

$$n\left(\prod^n \lambda^{-1}a_i\right)^{1/n} \leq \sum^n \lambda^{-1}a_i \implies n\left(\prod^n a_i\right)^{1/n} \leq \sum^n a_i$$

como queríamos. □

LEMA 3.3.2. *Sejam* $m \in \mathbb{N}^*, a_1, ..., a_m \in \mathbb{R}_+^\times$. *Defina*

$$I(a_1, ..., a_m; t) := \int_{Z(t)} x_1^{a_1} ... x_m^{a_m} dx_1 ... dx_m$$

onde $Z(t) := \{x \in \mathbb{R}^m : x_i \geq 0, \sum x_i \leq t\}$. *Então*

$$I(a_1, ..., a_m; t) = t^{\sum a_i + m} \frac{\Gamma(a_1 + 1) ... (a_m + 1)}{\Gamma(a_1 + ... + a_m + m + 1)}$$

onde Γ *denota a função gama de Euler.*

DEMONSTRAÇÃO. Lembremos que a função $\Gamma(x) := \int_0^\infty e^{-t} t^{x-1} dt$ é tal que

$$\Gamma(x) = (x-1)\Gamma(x-1) \quad . \tag{3.3.1}$$

Fazendo $x_i' = x_i/t$ em I obtemos

$$I(a_1, ..., a_m; t) = \int_{Z(1)} x_1'^{a_1} ... x_m'^{a_m} t^{\sum a_i + m} dx_1' ... dx_m' = t^{\sum a_i + m} I(a_1, ..., a_m; 1)$$

e é suficiente mostrarmos o lema para $t = 1$. Procedemos por indução:

$$I(a_1; 1) = \int_0^1 x_1^{a_1} dx_1 = \frac{1}{a_1 + 1} = \frac{\Gamma(a_1 + 1)}{\Gamma(a_1 + 2)}$$

pela fórmula (3.3.1). Seja $Z(x_m') := \left\{x \in \mathbb{R}^{m-1} : x_i \geq 0, \sum x_i \leq 1 - x_m\right\}$ então

$$\begin{aligned} I(a_1, ..., a_m; 1) &= \int_0^1 x_m^{a_m} \left(\int_{Z(x_m)'} x_1^{a_1} ... x_{m-1}^{a_{m-1}} dx_1 ... dx_{m-1} \right) dx_m = \\ &= \int_0^1 x_m^{a_m} I(a_1, ..., a_{m-1}; 1 - x_m) dx_m = \\ &= I(a_1, ..., a_{m-1}; 1) \int_0^1 x_m^{a_m} (1 - x_m)^{\sum^{m-1} a_i + (m-1)} dx_m = \\ &= I(a_1, ..., a_{m-1}; 1) \frac{\Gamma(a_m + 1)\Gamma(a_1 + ... + a_{m-1} + m)}{\Gamma(a_1 + ... a_m + m + 1)} \end{aligned}$$

onde na última igualdade usamos a conhecida identidade $\int_0^1 x^{p-1}(1-x)^{q-1} = \Gamma(p)\Gamma(q)/\Gamma(p+q)$. Pela hipótese de indução obtemos finalmente

$$I(a_1, ..., a_m; 1) = \frac{\Gamma(a_1 + 1) ... \Gamma(a_{m-1} + 1)}{\Gamma(a_1 + ... + a_{m-1} + m)} \frac{\Gamma(a_m + 1)\Gamma(a_1 + ... + a_{m-1} + m)}{\Gamma(a_1 + ... + a_m + m + 1)}$$

como queríamos. □

Seja $V = \mathbb{R}^r \times \mathbb{C}^s$, espaço vetorial real de dimensão $n = r + 2s$. Defina a norma em V dada por $||x|| := \sum_{i=1}^r |x_i| + 2\sum_{i=r+1}^s |z_i|$ onde $x = (x_1, ..., x_r, z_{r+1}, ..., z_{r+s})$.

LEMA 3.3.3. *Seja* $t \in \mathbb{R}_+^\times$ *e* $X(t) := \{x \in V : ||x|| \leq t\}$ *então* $\mu(X(t)) = 2^r (\pi/2)^s t^n/n!$.

DEMONSTRAÇÃO. Como $X(t)$ é simétrico em relação aos eixos reais temos $\mu(X(t)) = 2^r \mu(Y(t))$ onde $Y(t) := \{x \in V : ||x|| \leq t,\ x_1, ..., x_r \geq 0\}$. Fazendo a mudança de coordenadas Φ_j em $z_j := x_j + iy_j$ dada por $x_j := (1/2)\rho_j \cos\theta_j,\ y_j := (1/2)_j \sin\theta_j$ vemos que

$$J(\Phi_j) := \begin{pmatrix} \frac{1}{2}\cos\theta_j & -\frac{1}{2}{}_j \sin\theta_j \\ \frac{1}{2}\sin\theta_j & \frac{1}{2}\rho_j \cos\theta_j \end{pmatrix}$$

donde $|\det J(\Phi_j)| = \rho_j/4$. Logo,

$$\mu(Y(t)) = \int_{Y(t)} dx_1...dx_r dx_{r+1} dy_{r+1}...dx_{r+s} dy_{r+s} =$$
$$= 4^{-s} \int \rho_{r+1}...\rho_{r+s} dx_1...dx_r d\rho_{r+1} d\theta_{r+1}...d\rho_{r+s} d\theta_{r+s}$$

onde $Y'(t) := \left\{(x, \rho, \theta) \in \mathbb{R}^{r+2s} : x_i, \rho_i \geq 0,\ 0 \leq \theta_i \leq 2\pi,\ \sum x_i + \sum \rho_i \leq t\right\}$. Continuando:

$$\mu(Y(t)) = \left(\frac{2\pi}{4}\right)^s \int_{Y''(t)} \rho_{r+1}...\rho_{r+s} dx_1...dx_r d\rho_{r+1}...d\rho_{r+s}$$

com $Y''(t) := \{(x, \rho) \in \mathbb{R}^{r+s} : x_i, \rho_i \geq 0, \sum x_i + \sum \rho_i \leq t\}$. Pelo lema anterior tomando $m = r + s$, $a_i = 0$, $1 \leq i \leq r$ e $a_i = 1,\ r + 1 \leq i \leq m$ temos

$$\mu(Y(t)) = \left(\frac{\pi}{2}\right)^s t^{s+m} \frac{\Gamma(1)...\Gamma(1)\Gamma(2)...\Gamma(2)}{\Gamma(n+1)} = \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$$

donde $\mu(X(t)) = 2^r (\pi/2)^s t^n/n!$.

(1) Caso $r = 2$, $s = 0$ então $\mu(X(t)) = 2t^2$ o que corresponde ao quadrado de lado $\sqrt{2}t$ definido por $|x| + |y| \leq t$.
(2) Caso $r = 0,\ s = 1$ então $X(t)$ corresponde ao círculo de raio $t/2$ cuja área é $\mu(X(t)) = \pi t^2/4$.

□

3.4. A finitude do número de classe

Seja K um corpo numérico de grau n. Temos então n imersões $K \hookrightarrow \overline{\mathbb{Q}}$. Denote $\{\sigma_1, ..., \sigma_r\}$ as imersões reais (isto é, tal que $\sigma_i(K) \subseteq \mathbb{R}$) e $\{\sigma_{r+1}, \overline{\sigma_{r+1}}..., \sigma_{r+s}, \overline{\sigma_{r+s}}\}$ as imersões tal que $\mathbb{R} \supsetneq \sigma_{r+i}(K)$, $\overline{\sigma_{r+i}(K)} \subseteq \mathbb{C}$. Então $n = r + 2s$ e temos o monomorfismo de anéis: $\sigma : K \hookrightarrow V : \mathbb{R}^r \times \mathbb{C}^s$ dado por

$$\sigma(\zeta) \longmapsto (\sigma_1(\zeta), ..., \sigma_r(\zeta), \Re(\sigma_{r+1}(\zeta)), \Im(\sigma_{r+1}(\zeta)), ..., \Im(\sigma_{r+s}(\zeta))).$$

Identificamos V com $\mathbb{R}^n$ usando a base $\{1, i\}$ para $\mathbb{C}$.

Aqui Δ_K denota o discriminante da extensão e $B_K := (4/\pi)^s (n!/n^n) |\Delta_K|^{1/2}$ é denominado o limitante de Minkowski para K.

PROPOSIÇÃO 3.4.1. *Seja $\mathfrak{a}$ um ideal, não-nulo, de $\mathbb{Z}_K$. Então $\sigma(\mathfrak{a})$ é um reticulado saturado em V e o volume do paralelepípedo fundamental de $\sigma(\mathfrak{a})$ é $2^{-s}\mathbb{N}(\mathfrak{a}) |\Delta_K|^{1/2}$.*

DEMONSTRAÇÃO. Como $\mathfrak{a}$ é $\mathbb{Z}$-módulo finitamente gerado sem torção (pois $\mathfrak{a}$ é $\mathbb{Z}_K$-módulo finitamente gerado sem torção e $\mathbb{Z}_K$ é $\mathbb{Z}$-módulo livre) temos que $\mathfrak{a}$ é $\mathbb{Z}$-módulo livre. Como $\mathfrak{a} \subseteq \mathbb{Z}_K$ e $\mathbb{Z}_K \cong (\alpha) \subseteq \mathfrak{a}$ para $\alpha \in \mathfrak{a} \backslash \{0\}$ temos de um resultado conhecido da teoria de módulos sobre domínios que $n = \dim_{\mathbb{Z}} (\alpha) \leq \dim_{\mathbb{Z}} \mathfrak{a} \leq \dim_{\mathbb{Z}} \mathbb{Z}_K = n$. Seja então $\alpha_1, ..., \alpha_n$ uma base para $\mathfrak{a}$ como $\mathbb{Z}$-módulo. Então $\sigma(\mathfrak{a}) = \sigma\left(\sum \mathbb{Z}\alpha_i\right) = \sum \mathbb{Z}\sigma(\alpha_i)$ e para vermos que $\sigma(\mathfrak{a})$ é reticulado saturado basta mostrarmos que $\{\sigma(\alpha_i)\}$ é conjunto linearmente independente em $\mathbb{R}^n$ o que pela definição de σ equivale a mostrar que o determinante da matriz $A \in M_n(\mathbb{R})$ cuja i-ésima linha é

$$(\sigma_1(\alpha_i), ..., \sigma_r(\alpha_i), \Re(\sigma_{r+1}(\alpha_i)), \Im(\sigma_{r+1}(\alpha_i)), ...)$$

é não-nulo. Seja $B \in M_n(\mathbb{C})$ a matriz cuja i-ésima linha é

$$\left(\sigma_1(\alpha_i), ..., \sigma_r(\alpha_i), \sigma_{r+1}(\alpha_i), \overline{\sigma_{r+1}(\alpha_i)}, ...\right)$$

e observe que se em B somamos a coluna $r+2$ à coluna $r+1$ e subtraímos metade da coluna $r+1$ da coluna $r+2$ obtemos $2\Re(\sigma_{r+1}(\alpha_i))$ na coluna $r+1$ e $-i\Im(\sigma_{r+1}(\alpha_i))$ na coluna $r+2$. Repita a operação para os demais pares de colunas. Tais operações não mudam o determinante de B de forma que obtemos:

$$\begin{aligned}\det B &= \det\left((\sigma_1(\alpha_i), ..., \sigma_r(\alpha_i), 2\Re(\sigma_{r+1}(\alpha_i)), -i\Im(\sigma_{r+1}(\alpha_i)), ...)_i\right) = \\ &= (-2i)^s \det A \quad .\end{aligned}$$

Mas vimos na proposição 1.3.7 que $(\det B)^2 = \mathrm{D}(\alpha_1, ..., \alpha_n) \neq 0$ donde $\det A = (-2i)^{-s} \mathrm{D}(\alpha_1, ..., \alpha_n)^{1/2} \neq 0$ donde segue o desejado.

Agora como $\sigma(\mathfrak{a}) = \sum \mathbb{Z}\sigma(\alpha_i)$ o volume do paralelepípedo fundamental D de $\sigma(\mathfrak{a})$ é $|\det A|$. Pela observação 1.3.5 sabemos que $|\mathrm{D}(\alpha_1, ..., \alpha_n)| = (\mathbb{Z}_K : \mathfrak{a})^2 |\Delta_K|$ donde $\mu(D) = 2^{-s}(\mathbb{Z}_K : \mathfrak{a}) |\Delta_K|^{1/2}$ como queríamos. □

PROPOSIÇÃO 3.4.2. *Seja $\mathfrak{a}$ um ideal não-nulo em $\mathbb{Z}_K$. Então $\mathfrak{a}$ contém um elemento não-nulo $\alpha \in \mathbb{Z}_K$ tal que $|\mathrm{Nm}(\alpha)| \leq B_K \mathbb{N}(\mathfrak{a})$.*

DEMONSTRAÇÃO. Considere em V a norma discutida anteriormente, dada por, $\|x\| = \sum_{i=1}^{r} |x_i| + 2\sum_{i=r+1}^{r+s} |z_i|$ onde $x = (x_1, ..., x_r, z_{r+1}, ..., z_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$. Seja $X(t)$ como no lema 3.3.3 e D o paralelepípedo fundamental do (pela proposição anterior) reticulado saturado $\sigma(\mathfrak{a})$. O conjunto $X(t)$ é compacto, convexo e simétrico em relação à origem, portanto, tomando t grande o suficiente tal que $\mu(X(t)) \geq 2^n \mu(D)$ o teorema de Minkowski 3.2.8 mostra que $X(t)$ contém um ponto $\sigma(\alpha) \neq 0$. Para este $\alpha \in \mathfrak{a}$ temos

$$\begin{aligned}|\mathrm{Nm}(\alpha)| &= |\sigma_1(\alpha)| ... |\sigma_r(\alpha)| |\sigma_{r+1}(\alpha)| \left|\overline{\sigma_{r+1}(\alpha)}\right| ... |\sigma_{r+s}(\alpha)| \left|\overline{\sigma_{r+s}(\alpha)}\right| = \\ &= |\sigma_1(\alpha)| ... |\sigma_r(\alpha)| |\sigma_{r+1}(\alpha)|^2 ... |\sigma_{r+s}(\alpha)|^2 \leq \\ &\leq \left(\sum_{i=1}^{r} |\sigma_i(\alpha)| + 2\sum_{i=r+1}^{r+s} |\sigma_i(\alpha)|\right)^n n^{-n} \leq \frac{\|\sigma(\alpha)\|^n}{n^n} \leq \frac{t^n}{n^n}\end{aligned}$$

onde usamos o lema 3.3.1 na primeira desigualdade. Agora, para termos $\mu(X(t)) \geq 2^n \mu(D)$, usando o lema 3.3.3 que nos dá o volume de $X(t)$ e a proposição anterior que nos dá o volume de D, precisamos que

$$2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} \geq 2^n 2^{-s} \mathbb{N}(\mathfrak{a}) |\Delta_K|^{1/2}$$

ou seja

$$t^n \geq n! 2^{n-r} \pi^{-s} \mathbb{N}(\mathfrak{a}) |\Delta_K|^{1/2} = n! 2^{2s} \pi^{-s} \mathbb{N}(\mathfrak{a}) |\Delta_K|^{1/2}.$$

Para esta escolha de t temos então:

$$|\mathrm{Nm}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \mathbb{N}(\mathfrak{a}) |\Delta_K|^{1/2} = B_K \mathbb{N}(\mathfrak{a})$$

como queríamos. □

Vamos então aos dois teoremas principais desta seção:

THEOREM 3.4.3. *Seja K uma extensão de grau n de $\mathbb{Q}$ e seja Δ_K seu discriminante. Seja $2s$ o número de imersões de K em $\overline{\mathbb{Q}}$ (fecho algébrico) que não estão contidas nos reais, isto é, quando estendida para $\mathbb{C}$ sua imagem não está contida nos reais. Então existe um conjunto de representantes para $\mathrm{Cl}(K)$ consistindo de ideais inteiros $\mathfrak{a}$ tal que $\mathbb{N}(\mathfrak{a}) \leq B_K$ onde $B_K = (4/\pi)^s (n!/n^n) |\Delta_K|^{1/2}$ é o limitante de Minkowski para K.*

DEMONSTRAÇÃO. Seja $\mathfrak{c}$ um ideal fracionário arbitrário de $\mathbb{Z}_K$. Precisamos mostrar que a classe de $\mathfrak{c}$ em $\mathrm{Cl}(K)$ é representada por um ideal inteiro $\mathfrak{a}$ tal que $\mathbb{N}(\mathfrak{a}) \leq B_K$. Seja $d \in K^\times$ tal que $(d)\mathfrak{c}^{-1} = d\mathfrak{c}^{-1} =: \mathfrak{b}$ seja um ideal inteiro (por exemplo, qualquer elemento de $\mathfrak{c}$). De acordo com a proposição anterior, existe $\beta \in \mathfrak{b}$, $\beta \neq 0$, tal que $|\mathrm{Nm}(\beta)| \leq B_K \mathbb{N}(\mathfrak{b})$. Agora, $(\beta) \subseteq \mathfrak{b}$ donde $(\beta) = \mathfrak{a}\mathfrak{b}$ para algum ideal inteiro $\mathfrak{a}$ (exatamente $\beta\mathfrak{b}^{-1}$). Note que $\mathfrak{a} \sim \mathfrak{b}^{-1} \sim \mathfrak{c}$ e que

$$(\mathbb{N}(\mathfrak{a})\mathbb{N}(\mathfrak{b})) = (\mathbb{N}(\mathfrak{a}\mathfrak{b})) = (\mathbb{N}((\beta))) = \mathcal{N}((\beta)) = (\mathrm{Nm}(\beta))$$

onde usamos as proposições 3.1.2-1 e 3.1.4-3 nas últimas duas igualdades respectivamente. Como $\mathbb{N}(\mathfrak{a})\mathbb{N}(\mathfrak{b}) \in \mathbb{N}$ e $\mathrm{Nm}(\beta) \in \mathbb{Z}$ (pois $\beta \in \mathbb{Z}_K$) temos

$$\mathbb{N}(\mathfrak{a})\mathbb{N}(\mathfrak{b}) = |\mathrm{Nm}(\beta)| \leq B_K \mathbb{N}(\mathfrak{b}) \implies \mathbb{N}(\mathfrak{a}) \leq B_K$$

como queríamos. □

THEOREM 3.4.4. *Seja $K \geq \mathbb{Q}$ uma extensão finita. Então o número de classe de K é finito.*

DEMONSTRAÇÃO. Pelo teorema anterior, é suficiente mostrarmos que existem apenas uma quantidade finita de ideais inteiros $\mathfrak{a}$ de $\mathbb{Z}_K$ tal que $\mathbb{N}(\mathfrak{a}) \leq B_K$. Vamos mostrar mais; que para qualquer natural $M > 0$, existem apenas uma quantidade finita de ideais inteiros $\mathfrak{a}$ de $\mathbb{Z}_K$ com $\mathbb{N}(\mathfrak{a}) \leq M$. Ora, se $\mathfrak{a} = \prod \mathfrak{p}_i^{r_i}$ então $\mathbb{N}(\mathfrak{a}) = \prod p_i^{r_i f_i}$ onde $(p_i) = \mathfrak{p}_i \cap \mathbb{Q}$ e $f_i = f(\mathfrak{p}_i/(p_i))$. Como $\mathbb{N}(\mathfrak{a}) \leq M$ isto permite apenas uma quantidade finita de possibilidades

para p_i (e, portanto, para $\mathfrak{p}_i$ visto que existem apenas uma quantidade finita de $\mathfrak{p}_i$´s que dividem (p_i)) e r_i. □

OBSERVAÇÃO 3.4.5. Seja S o conjunto dos ideais inteiros de K com norma menor ou igual à B_K. Vimos que S é finito e que $\mathrm{Cl}(K) = S/\sim$ onde $\mathfrak{a} \sim \mathfrak{b}$ se e somente se $\mathfrak{a} = (d)\,\mathfrak{b}$, $d \in K^\times$. Para acharmos S basta calcularmos as decomposições em $\mathbb{Z}_K$ de um número suficiente de primos $p_i \in \mathbb{Z}$ (os primos menores ou iguais à B_K). Para decidirmos quando $\mathfrak{a} \sim \mathfrak{b}$ temos que verificar se $\mathfrak{c} := \mathfrak{a}\mathfrak{b}^{-1}$ é principal. Agora, podemos supor sem perda de generalidade que $\mathfrak{c}$ é inteiro, caso contrário, $\mathfrak{c}^{-1}$ é inteiro e temos que $\mathfrak{c}^{-1}$ é principal se e somente se $\mathfrak{c}$ é principal. Assim, para $\gamma \in \mathfrak{c}$:

$$(\gamma) = \mathfrak{c} \iff \mathfrak{c}^{-1}(\gamma) = \mathbb{Z}_K \iff \left(\mathbb{Z}_K : \mathfrak{c}^{-1}(\gamma)\right) = 1 \iff$$
$$\iff \mathbb{N}\left(\mathfrak{c}^{-1}(\gamma)\right) = 1 \overset{*}{\iff} \mathcal{N}\left(\mathfrak{c}^{-1}(\gamma)\right) = \mathbb{Z} \overset{**}{\iff}$$
$$\iff \mathcal{N}(\mathfrak{c})^{-1}(\mathrm{Nm}(\gamma)) = \mathbb{Z} \overset{*}{\iff} (\mathbb{N}(\mathfrak{c})) = (\mathrm{Nm}(\gamma)) \iff \mathbb{N}(\mathfrak{c}) = |\mathrm{Nm}(\gamma)|$$

onde em $(*)$ usamos a proposição 3.4.2-2 e em $(**)$ usamos a proposição 3.4.1-3. Em suma, para decidirmos se $\mathfrak{a} \sim \mathfrak{b}$ precisamos resolver a equação $\mathrm{Nm}(\gamma) = m \in \mathbb{Z}$. Ela admite uma solução se e somente se $\mathfrak{a} \sim \mathfrak{b}$. Ao expressarmos γ em termos de uma base integral isto se torna uma equação diofantina bem especial que possui algoritmos eficientes para resolvê-la. Assim, é possível calcularmos $\mathrm{Cl}(K)$ efetivamente.

EXEMPLO 3.4.6. (1) Seja $K = \mathbb{Q}[i]$. Neste caso, a condição do teorema 3.4.3 é

$$\mathbb{N}(\mathfrak{a}) \leq (2/4)\,(4/\pi)\,2 < 1.27 < 2$$

donde $\mathbb{N}(\mathfrak{a}) = 1$ e temos $\mathfrak{a} = \mathbb{Z}_K$. Ou seja, $\mathbb{Z}_K$ é domínio principal.

(2) Seja $K = \mathbb{Q}\left[\sqrt{-5}\right]$. Neste caso pelo exemplo 1.3.21 temos $\Delta_K = -20$ donde

$$\mathbb{N}(\mathfrak{a}) \leq (2/4)\,(4/\pi)\,|-20|^{1/2} < 3.$$

Qualquer ideal fracionário próprio, não-nulo, satisfazendo a desigualdade deve dividir o ideal (2) de $\mathbb{Z}$. É fácil ver que $(2) = \mathfrak{p}^2$ onde $\mathfrak{p} = \left(2, 1+\sqrt{-5}\right)$ e este é o único ideal dividindo (2) visto que a extensão é Galoisiana e, portanto, vale o teorema 2.6.2. Assim, $\mathbb{Z}_K$ e $\mathfrak{p}$ formam um conjunto de representantes para $\mathrm{Cl}(\mathbb{Z}_K)$. Agora, $\mathfrak{p}$ não é principal pois não existe um elemento $\mathbb{Z}_K \ni \alpha = m + n\sqrt{-5}$ tal que $\mathrm{Nm}(\alpha) = m^2 + 5n^2 = 2$. Como conseqüência $h_K = 2$.

(3) Seja K um corpo cúbico com discriminante menor que zero. Como $\mathrm{sign}(\Delta_K) = (-1)^s$ e $[K:\mathbb{Q}] = r + 2s$ temos $s = 1$ e $r = 1$. Neste caso, $B_K < 0.283\,|\Delta_K|^{1/2}$. Para $|\Delta_K| \leq 49$ temos $\mathrm{B}_K < 2$ donde para $-49 \leq \Delta_K < 0$ o número de classe $h_K = 1$.

DEFINIÇÃO 3.4.7. Uma extensão $L \geq K$ finita de um corpo numérico é dita irramificada ou não-ramificada se e somente se nenhum primo inteiro de $\mathbb{Z}_K^K$ se ramifica em $\mathbb{Z}_K^L$.

THEOREM 3.4.8. *Não existem extensões irramificadas de* $\mathbb{Q}$.

DEMONSTRAÇÃO. Seja K uma extensão finita de $\mathbb{Q}$. Como o conjunto de representantes para p grupo de classes é sempre não-vazio e um elemento dele possui norma maior ou igual à 1, o teorema 3.4.3 nos diz que $1 \leq (n!/n^n)(4/\pi)^s |\Delta_K|^{1/2}$, ou seja,

$$|\Delta_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2} =: a_n;\ n \in \mathbb{N}^*.$$

Note que $a_2 > 1$ e que $a_{n+1}/a_n = (\pi/4)^{1/2}(1+1/n)^n > 1$. De fato, sendo

$$f(x) := (\pi/4)^{1/2}(1+1/x)^x;\ x \geq 1$$

temos

$$f'(x) = (\pi/4)^{1/2}\ln(1+1/x)(1+1/x)^x\left(-1/x^2\right) \leq 0.$$

Logo, $f(x)$ é não-crescente e como $\lim_{x\to+\infty} f(x) = \left(\pi^{1/2}/2\right)e > 1$ temos que $f(x) > 1\,\forall x \geq 1$ como afirmado. Assim, a seqüência $\{a_n\}_{n\in\mathbb{N}^*}$ é monotonicamente crescente. Segue que $|\Delta_K|^{1/2} > 1$. Portanto, existe $p \in \mathbb{Z}$ primo tal que $p \mid \Delta_K$ e sabemos de 2.6.7 que (p) ramifica-se em K. □

COROLÁRIO 3.4.9. *Não existe polinômio irredutível mônico $f(X) \in \mathbb{Z}[X]$ com $\partial f > 1$ (grau) e* $\operatorname{disc}(f(X)) = \pm 1$.

DEMONSTRAÇÃO. Seja f um tal polinômio. Sabemos da observação 1.3.5 que $\operatorname{disc}(f(X)) = (\mathbb{Z}_K : M)\operatorname{disc}(\mathbb{Z}_K/\mathbb{Z})$ onde M é o $\mathbb{Z}$-módulo gerado pelas raízes de f. Se $\operatorname{disc}(f(X)) = \pm 1$ então $\operatorname{disc}(\mathbb{Z}_K/\mathbb{Z}) = \pm 1$ o que vimos acarreta que $\mathbb{Q}[\alpha] \geq \mathbb{Q}$ (α raiz de f) é irramificada contrariando o teorema anterior. □

OBSERVAÇÃO 3.4.10. Podem existir extensões irramificadas de outros corpos numéricos que não $\mathbb{Q}$. Em realidade, um dos teoremas principais da teoria de corpos de classe diz que a máxima extensão abeliana irramificada de K possui grupo de Galois canonicamente isomorfo à $\operatorname{Cl}(K)$. Indicamos **[Mil97]** como uma boa referência para a teoria dos corpos de classe. Em particular, de acordo com o exemplo 2. acima $\operatorname{Cl}\left(\mathbb{Q}\left[\sqrt{-5}\right]\right) \cong \mathbb{F}_2$ donde $\mathbb{Q}\left[\sqrt{-5}\right]$ deve possuir uma extensão irramificada de grau 2.

EXEMPLO 3.4.11. Seja α raiz de $f(X) = X^5 - X + 1$, que é irredutível. Vimos em um exemplo anterior (ou usando a fórmula (1.3.3)) que f possui discriminante 19×151. Em particular, $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. Pelo teorema 3.4.3 todo elemento de $\operatorname{Cl}(\mathbb{Z}_K)$ contém um ideal com $\mathbb{N}(\mathfrak{a}) < 0.062 \times \sqrt{19 \times 151} = 3.3 < 4$. Se $\mathfrak{p}$ é um primo de $\mathbb{Z}_K$ com $\mathbb{N}(\mathfrak{p}) = 2$ então $f(\mathfrak{p}/(2)) = 1$. Pelo teorema 2.6.8, $f(X) \equiv g(X) \mod(2)$ com $\partial g = 1$, ou seja, f possui uma raiz $\mod(2)$. Mas $f\left(\overline{0}\right) = \overline{1}$ e $f\left(\overline{1}\right) = \overline{1}$ donde não existe tal $\mathfrak{p}$! Similarmente para $\mathbb{N}(\mathfrak{p}) = 3$. Logo, $\mathbb{Z}_K$ é domínio principal.

CAPíTULO 4

O teorema da unidade

Neste capítulo veremos um segundo importante resultado da teoria para as extensões finitas de $\mathbb{Q}$: o teorema da unidade de Dirichlet. Ele determina a estrutura do grupo multiplicativo das unidades de $\mathbb{Z}_{\mathbb{K}}$ em uma extensão $K \geq \mathbb{Q}$ finita.

4.1. Considerações preliminares

Lembremos que um grupo abeliano finitamente gerado G é isomorfo à $T \oplus \mathbb{Z}^k$ onde T é o subgrupo de torção de G (que é finito) e $k \in \mathbb{N}$ depende apenas de G e é denominado posto. O teorema da unidade diz que o grupo das unidades de $\mathbb{Z}_{\mathbb{K}}$ é finitamente gerado de posto $r+s-1$, onde r e s são os números de imersões reais e complexas como no capítulo anterior. Denotaremos $U_K := \mathbb{Z}_{\mathbb{K}}{}^{\times}$ e $\mu_K \leq U_K$ o subgrupo de torção. Note que μ_Ké o conjunto das raízes da unidade que estão em K. De fato, se $u \in \mu_K$ então existe $n \in \mathbb{N}$ tal que $u^n = 1$ e então u é raiz da unidade. Por outro lado, se $u^n = 1$ para algum n então u é raiz de $X^n - 1 = 0$ donde $u \in \mathbb{Z}_{\mathbb{K}}$. Da mesma forma $\left(u^{-1}\right)^n - 1 = (u^n)^{-1} - 1 = 0$, donde $u^{-1} \in \mathbb{Z}_K$. Assim, $u \in U_K$ e como u é de torção temos $u \in \mu_K$. Note também que se $r > 0$ (K pode ser identificado com um subcorpo de $\mathbb{R}$) então $\mu_K = \{\pm 1\}$.

DEFINIÇÃO 4.1.1. Um conjunto $\{u_1, ..., u_{r+s-1}\} \subseteq U_K$ é dito ser um sistema fundamental de unidades se seus elementos formam uma base para a parte livre de U_K. Isto é, se todo $u \in U_K$ pode ser escrito de forma única como $u = \xi u_1^{m_1} ... u_{r+s-1}^{m_{r+s-1}}, \xi \in \mu_K, m_i \in \mathbb{Z}$.

Vejamos um lema importante que nos dá uma caracterização alternativa para as unidades.

LEMA 4.1.2. *Seja $\alpha \in K$. Então $\alpha \in U_K$ se e somente se $\alpha \in \mathbb{Z}_K$ e $\mathrm{Nm}_{K/\mathbb{Q}} = \pm 1$.*

DEMONSTRAÇÃO. Se $\alpha \in U_K$ então $\alpha, \alpha^{-1} \in \mathbb{Z}_K$ e das propriedades demonstradas da norma temos

$$\pm 1 = \mathrm{Nm}_{K/\mathbb{Q}}(\pm 1) = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\,\mathrm{Nm}_{K/\mathbb{Q}}(\alpha^{-1})$$

e além disso $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha), \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^{-1}) \in \mathbb{Z}$ donde $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Para a volta, pelo corolário 1.2.4 e identificando K com um subcorpo de $\mathbb{C}$, ou seja, fixando uma imersão σ_0 de K em $\mathbb{C}$ temos $\pm 1 = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \prod_\sigma \sigma(\alpha) = \sigma_0(\alpha) \prod_{\sigma \neq \sigma_0} \sigma(\alpha)$ onde $\sigma : K \hookrightarrow \mathbb{C}$ são todas as imersões de K em $\mathbb{C}$ (incluindo as reais). Se $\alpha \in \mathbb{Z}_K$ então $\pm\sigma_0(\alpha)^{-1} = \prod_{\sigma \neq \sigma_0} \sigma(\alpha) \in \mathbb{C}$ é inteiro algébrico pois os $\sigma(\alpha)$ são raízes de uma mesma equação integral. Assim, como também $\pm\sigma_0(\alpha)^{-1} \in K$ temos $\pm\sigma_0(\alpha)^{-1} \in \mathbb{Z}_K$. Segue que α tem inverso em $\mathbb{Z}_K$ e é, portanto, uma unidade. □

EXEMPLO 4.1.3. Seja $K = \mathbb{Q}[\sqrt{d}]$. Vimos que $\mathbb{Z}_K = \left\{m + n\sqrt{d} : m, n \in \mathbb{Z}\right\}$ ou $\mathbb{Z}_K = \left\{m + n\frac{(1+\sqrt{d})}{2} : m, n \in \mathbb{Z}\right\}$. Pelo lema acima as unidades de K satisfazem

$$\mathrm{Nm}(m + n\sqrt{d}) = m^2 - n^2 d = \pm 1$$

ou

$$\mathrm{Nm}\left(m + n\frac{(1+\sqrt{d})}{2}\right) = \left(m + n\frac{(1+\sqrt{d})}{2}\right)\left(m + n\frac{(1-\sqrt{d})}{2}\right) =$$

$$= m^2 + mn + \frac{n^2}{4} - \frac{n^2 d}{4} = \pm 1.$$

Isto é,

$$m^2 - n^2 d = \pm 1$$

ou

$$(2m + n)^2 - n^2 d = \pm 4.$$

Fica então claro que se $d < 0$ estas equações tem apenas um número finito de soluções e, portanto, $U_K = \mu_K$. Isto concorda com o teorema da unidade pois como $d < 0$ devemos ter uma imersão complexa não-real. Da condição $r + 2s = 2$ para as imersões deduzimos $r = 0$, $s = 1$ e que $r + s - 1 = 0$, assim, U_K tem posto 0. Por outro lado se $d > 0$ então temos duas imersões reais, isto é, $r = 2\,, s = 0$ e o teorema da unidade afirma que U_K tem posto 1.

EXEMPLO 4.1.4. Considere $K = \mathbb{Q}[\alpha]$ onde α é raiz de $X^3 + 10X + 1$. Temos pela fórmula (1.3.3), que $\mathrm{disc}(K/\mathbb{Q}) = -4027$. Como $\mathrm{sign}(\mathrm{disc}(K/\mathbb{Q})) = (-1)^s$ e $r + 2s = 3$ devemos ter $r = 1 = s$. Agora, $\mathrm{Nm}(\alpha) = \prod \alpha_i = (-1)^3 = -1$ onde os α_i são os conjugados de α e estamos usando o observado em 1.1.3. Segue que α é unidade. Veremos adiante que α é unidade fundamental e, portanto, o teorema da unidade dos diz que $U_K = \{\pm\alpha^m : m \in \mathbb{Z}\}$.

4.2. Demonstração do teorema da unidade

Lembremos do capítulo anterior onde tínhamos $\mathbb{Q} \subseteq K$ de grau $n \in \mathbb{N}$ e definimos o monomorfismo de anéis $\sigma : K \hookrightarrow V := \mathbb{R}^r \times \mathbb{C}^s$ dado por

$$\sigma(\xi) = (\sigma_1(\xi), ..., \sigma_r(\xi), \sigma_{r+1}(\xi), ..., \sigma_{r+s}(\xi))\,.$$

Queremos utilizar a teoria dos reticulados para a demonstração do teorema. Precisamos de um "análogo" para σ onde temos como domínio o grupo multiplicativo $K^\times$. Isto nos leva a considerar a aplicação $L : K^\times \hookrightarrow \mathbb{R}^{r+s}$ dado por

$$L(\xi) = (\ln|\sigma_1(\alpha)|\,, ..., \ln|\sigma_r(\xi)|\,, 2\ln|\sigma_{r+1}(\xi)|\,, ..., 2\ln|\sigma_{r+s}(\xi)|)\,.$$

Isto é em "essência" compor σ com o logaritmo natural que sabemos ser um homomorfismo do grupo multiplicativo $\mathbb{R}_+^\times$ no grupo aditivo $\mathbb{R}_+$. Como $|\alpha| = |\overline{\alpha}|$, para garantirmos a

independência linear, abandonamos as coordenadas complexo-conjugadas e multiplicamos por 2 as restantes.

A aplicação L é claramente um homomorfismo. Pelo lema anterior, se $\xi \in U_K$ então $\mathrm{Nm}(\xi) = \pm 1$, isto é,

$$|\sigma_1(\xi)| ... |\sigma_r(\xi)| |\sigma_{r+1}(\xi)|^2 ... |\sigma_{r+s}(\xi)|^2 = 1$$

e tomando o logaritmo obtemos

$$|\sigma_1(\xi)| + ... + |\sigma_r(\xi)| + 2|\sigma_{r+1}(\xi)| + 2|\sigma_{r+s}(\xi)| = 0.$$

Portanto, $L(\xi) \in H := \{x \in \mathbb{R}^{r+s} : x_1 + ... + x_r + 2x_{r+1} + ... + 2x_{r+s} = 0\}$ que é um hiperplano. Reparametrizando H em termos da última coordenada obtemos um isomorfismo $H \cong \mathbb{R}^{r+s-1}$.

No restante desta seção vamos demonstrar que $L(U_K)$ é um reticulado saturado em H e que $\ker L = \mu_K$. Isto demonstra que U_K é finitamente gerado e que $\mathrm{rank}(U_K) = \mathrm{rank}(L(U_K)) = \dim H = r + s - 1$ que é o teorema da unidade:

THEOREM 4.2.1. *(Teorema da Unidade Dirichlet) Seja $\mathbb{Q} \subseteq K$ uma extensão finita. Então U_K é finitamente gerado e tem posto igual a $r + s - 1$ onde r e s são o número de imersões reais e complexas de K respectivamente.* ■

LEMA 4.2.2. *Para quaisquer $m, M \in \mathbb{N}$ o conjunto de inteiros algébricos α com grau (grau do polinômio mínimo) menor que m e tais que $|\alpha'| < M$ (valor absoluto com respeito a qualquer imersão em $\mathbb{C}$) é finito.*

DEMONSTRAÇÃO. A primeira condição limita o grau dos polinômios mínimos a considerar. A segunda condição limita, em módulo, as raízes destes polinômios e, tendo em vista a observação 1.1.3, indiretamente limita, em módulo, os coeficientes destes polinômios. Como tais coeficientes devem ser inteiros, existem apenas uma quantidade finita deles e, portanto, uma quantidade finita de raízes. □

PROPOSIÇÃO 4.2.3. *Na notação desenvolvida acima, temos que $L(U_K)$ é um reticulado em H e $\ker L$ é um grupo finito (e, portanto, igual a μ_K).*

DEMONSTRAÇÃO. Seja $0 \in C \subseteq H$ um conjunto limitado. Digamos que

$$C \subseteq \{x \in H : |x_i| \leq M\}.$$

Se $L(\xi) \in C$ então $\ln|\sigma_i(\xi)| \leq M$, $\forall i$, ou seja, $|\sigma_i(\xi)| \leq e^M$, $\forall i$. Como $[\mathbb{Q}[\xi] : \mathbb{Q}] \leq [K : \mathbb{Q}]$, pelo lema anterior o conjunto de tais ξ é finito. Ou seja, $L(U_K) \cap C$ é finito. Pelo lema 3.2.3 e proposição 3.2.4 segue que $L(U_K)$ é reticulado em H. Como $L(\ker L) = 0 \in C$ temos, em particular, que $\ker L$ é finito. Como o kernel é subgrupo segue que $\ker L \subseteq \mu_K$. Reciprocamente, se $\xi \in \mu_K$ então $\sigma(\xi) \in \{z \in \mathbb{C} : |z| = 1\}$ donde vemos que $\xi \in \ker L$. Logo, $\ker L = \mu_K$ completando a prova. □

LEMA 4.2.4. *Seja $A = (a_{ij}) \in M_m(\mathbb{R})$ tal que $a_{ij} < 0$, $\forall i \neq j$ e $\sum_j a_{ij} > 0$, $\forall i$. Então A é inversível.*

DEMONSTRAÇÃO. Suponha que não e fixe $(x_1, ..., x_m) \in \ker A$ não-nulo. Considere i tal que $|x_i| = \max |x_j|$. Dividindo por $|x_i|$ podemos supor $|x_i| = 1$ e então $|x_j| \leq 1$, $\forall j$. Neste caso, a i-ésima equação fica:

$$0 = \sum a_{ij}x_j = a_{ii} + \sum_{j \neq i} a_{ij}x_j \geq a_{ii} + \sum_{j \neq i} a_{ij} > 0$$

onde usamos as hipóteses na primeira e segunda desigualdades. Temos um absurdo e, portanto, $\ker A = (0)$. Segue que A é inversível. □

PROPOSIÇÃO 4.2.5. *O conjunto $L(U_K)$ é um reticulado saturado em H.*

DEMONSTRAÇÃO. Considere novamente o monomorfismo $\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s}$ do capítulo anterior. Para $x = (x_1, ..., x_r, x_{r+1}, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s$ defina

$$\mathrm{Nm}(x) := x_1 ... x_r x_{r+1}\overline{x_{r+1}} ... x_{r+s}\overline{x_{r+s}}.$$

Então do corolário 1.2.4 temos $\mathrm{Nm}(\sigma(\alpha)) = \mathrm{Nm}(\alpha)$. Note também que $|\mathrm{Nm}(x)| = |x_1| ... |x_r| |x_{r+1}|^2 ... |x_{r+s}|^2$. Lembremos da proposição 3.4.1 onde mostramos que $\sigma(\mathbb{Z}_K)$ é um reticulado saturado em $\mathbb{R}^r \times \mathbb{C}^s$ e o volume de seu paralelepípedo fundamental é $2^{-s} |\Delta_K|^{1/2}$. Mais precisamente, se $\alpha_1, ..., \alpha_n$ é uma $\mathbb{Z}$-base para $\mathbb{Z}_K$ mostramos que o valor absoluto do determinante da matriz cujas linhas são

$$\sigma(\alpha_i) = (\sigma_1(\alpha_i), ..., \sigma_r(\alpha_i), \Re(\sigma_{r+1}(\alpha_i)), \Im(\sigma_{r+1}(\alpha_i)), ...)$$

é $2^{-s} |\Delta_K|^{1/2}$. Fizemos isso mostrando que tal matriz pode ser obtida da matriz cujas linhas são

$$(\sigma_1(\alpha_i), ..., \sigma_r(\alpha_i), \sigma_{r+1}(\alpha_i), \overline{\sigma_{r+1}}(\alpha_i), ...)$$

através de operações elementares nas colunas que multiplicam o módulo do determinante da matriz por 2^{-s} e sabemos que o determinante da última matriz é $\pm |\Delta_K|^{1/2}$.

Agora vamos proceder analogamente: seja $x \in \mathbb{R}^r \times \mathbb{C}^s$ tal que $\frac{1}{2} \leq |\mathrm{Nm}(x)| \leq 1$ e defina $x\sigma(\mathbb{Z}_K) := \{x\sigma(\alpha) : \alpha \in \mathbb{Z}_K\}$ que como $\mathbb{R}^r \times \mathbb{C}^s$ é anel está bem definido. É imediato que $x\sigma(\mathbb{Z}_K)$ é novamente um reticulado. O volume de seu paralelepípedo fundamental é o módulo do determinante da matriz cuja i-ésima linha é:

$$(x_1\sigma_1(\alpha_i), ..., x_r\sigma_r(\alpha_i), \Re(x_{r+1}\sigma_{r+1}(\alpha_i)), \Im(x_{r+1}\sigma_{r+1}(\alpha_i)), ...)\,.$$

Como antes temos que o valor absoluto do determinante de tal matriz é 2^{-s} vezes o módulo do determinante da matriz cuja i-ésima linha é:

$$(x_1\sigma_1(\alpha_i), ..., x_r\sigma_r(\alpha_i), x_{r+1}\sigma_{r+1}(\alpha_i), \overline{x_{r+1}}\,\overline{\sigma_{r+1}}(\alpha_i), ...)$$

que é, pela multi-linearidade do determinante igual a:

$$|x_1| ... |x_r| |x_{r+1}|^2 ... |x_{r+r}|^2 |\Delta_K|^{1/2} = |\mathrm{Nm}(x)| |\Delta_K|^{1/2}\,.$$

Portanto, $x\sigma(\mathbb{Z}_K)$ é um reticulado cujo paralelepípedo fundamental tem volume

$$2^{-s}\left|\Delta_K\right|^{1/2}\left|\mathrm{Nm}(x)\right|.$$

Note que enquanto x varia sobre $\frac{1}{2} \leq |\mathrm{Nm}(x)| \leq 1$ o volume permanece limitado.

Podemos então considerar um conjunto compacto, convexo e simétrico em relação à origem $T \subseteq \mathbb{R}^r \times \mathbb{C}^s$ tal que, de acordo com o teorema de Minkowski 3.2.8, para todo x com $\frac{1}{2} \leq |\mathrm{Nm}(x)| \leq 1$ existe $\gamma \in \mathbb{Z}_K$, $\gamma \neq 0$ tal que $x\sigma(\gamma) \in T$. Os pontos de T tem coordenadas limitadas e, portanto, $|\mathrm{Nm}(y)| \leq M$, $\forall y \in T$ e algum $M > 0$. Segue que $x\sigma(\gamma) \in T \implies |\mathrm{Nm}(x\sigma(\gamma))| \leq M$, ou ainda,

$$|\mathrm{Nm}(\gamma)| = |\mathrm{Nm}(\sigma(\gamma))| \leq \frac{M}{|\mathrm{Nm}(x)|} \leq 2M.$$

Considere o conjunto $\{(\gamma)\}_{\gamma\in\Lambda}$ de ideais de $\mathbb{Z}_K$ onde γ varia no conjunto Λ dos $\gamma \in \mathbb{Z}_K$ para os quais existe x satisfazendo $\frac{1}{2} \leq |\mathrm{Nm}(x)| \leq 1$ e $x\sigma(\gamma) \in T$. Vimos que para um tal γ tem-se $|\mathrm{Nm}(\gamma)| \leq 2M$ onde M depende apenas de T. As proposições 3.1.2-3 e 3.1.3-1 combinadas afirmam que

$$(\mathrm{Nm}(\gamma)) = \mathcal{N}((\gamma)) = (\mathbb{N}((\gamma))) \implies |\mathrm{Nm}(\gamma)| = \mathbb{N}(\gamma)$$

ou seja, para $\gamma \in \Lambda$ temos $\mathbb{N}((\gamma)) \leq 2M$. O teorema 3.4.4 afirma que, neste caso, existem apenas uma quantidade finita de tais ideais; digamos $(\gamma_1), ..., (\gamma_t)$. Assim, se $\gamma \in \Lambda$ então $(\gamma) = (\gamma_i)$ para algum i. Segue que existe $\varepsilon \in U_K$ tal que $\gamma = \gamma_i\varepsilon$. Como $\gamma \in \Lambda$ temos $x\sigma(\gamma) \in T$ para algum x satisfazendo $\frac{1}{2} \leq |\mathrm{Nm}(x)| \leq 1$. Ou seja, $x\sigma(\gamma_i\varepsilon) \in T$ que é equivalente à $x\sigma(\varepsilon) \in \sigma(\gamma_i^{-1})T$. Seja $T' = \sigma(\gamma_1^{-1}) \cup ... \cup \sigma(\gamma_t^{-1})T$

Estamos prontos para terminar a demonstração. Afirmamos que (assumindo $r+s-1 \geq 1$ caso contrário não há nada a ser feito) $\forall i \in \{1, ..., r+s\}$, $\exists \varepsilon_i \in U_K$ tal que $\forall j \neq i$, $|\sigma_j(\varepsilon_i)| < 1$. De fato, supondo que não, $\exists i \in \{1, ..., r+s\}$ tal que $\forall \varepsilon \in U_K$, $\exists j \neq i$ tal que $|\sigma_j(\varepsilon)| \geq 1$. Seja $d = \sup\{|x_k| : x = (x_1, ..., x_{r+s}) \in T'\}$ e tome

$$x_0 = \left(d+1, d+1, ..., \frac{1}{(d+1)^{r+s-1}}, d+1, ..., d+1\right)$$

onde o fator $1/(d+1)^{r+s-1}$ aparece na i-ésima coordenada. Note que $|\mathrm{Nm}(x_0)| = 1$. Da hipótese de absurdo, $\forall \varepsilon \in U_K$, $\exists j \neq i$ tal que $|(x_0\sigma(\varepsilon))_j| = (d+1)\left|\sigma_j(\varepsilon)\right| > d$ donde provamos que $\forall \varepsilon \in U_K$, $x_0\sigma(\varepsilon) \notin T'$. Ou seja, $\forall \varepsilon \in U_K$, $\forall k = 1, ..., t$, $x_0\sigma(\varepsilon) \notin \sigma(\gamma_k^{-1})T$, ou ainda,

$$\forall \varepsilon \in U_K,\ \forall k = 1, ..., t,\ x_0\sigma(\varepsilon\gamma_k) \notin T.$$

Mas note que $\{(\varepsilon\gamma_k)\}_{\varepsilon\in U_K,\, k\in\{1,...,t\}} = \{(\gamma)\}_{\gamma\in\Lambda}$ donde para este x_o,vale que $\forall \gamma \in \Lambda$, $x_0\sigma(\gamma) \notin T$ o que, como vimos, contraria o teorema de Minkowski. Isto demonstra o afirmado.

Seja então $\{\varepsilon_1, ..., \varepsilon_{r+s}\} \subseteq U_K$ com tais propriedades. Segue que $\ln|\sigma_j(\varepsilon_i)| < 0$, $\forall j \neq i$. Afirmamos que $\{L(\varepsilon_1), ..., L(\varepsilon_{r+s-1})\}$ é conjunto linearmente independente no reticulado

$L(U_K)$. Para isto precisamos mostrar que a matriz cuja i-ésima linha é

$$(\ln|\sigma_1(\varepsilon_i)|, ..., 2\ln|\sigma_{r+s-1}(\varepsilon_i)|)$$

é inversível. Os elementos fora da diagonal são negativos mas a soma

$$\ln|\sigma_1(\varepsilon_i)| + ... + 2\ln|\sigma_{r+s}(\varepsilon_i)| = 0$$

pois $L(\varepsilon_i) \in H$. Assim,

$$\ln|\sigma_1(\varepsilon_i)| + ... + 2\ln|\sigma_{r+s-1}(\varepsilon_i)| = -2\ln|\sigma_{r+s}(\varepsilon_i)| > 0.$$

Finalmente, pelo lema anterior tal matriz é inversível o que demonstra a proposição. □

4.3. Unidades em corpos cúbicos de discriminante negativo

Vamos agora estabelecer uma relação importante para o caso dos corpos cúbicos de discriminante negativo. Lembremos que pela proposição 1.3.20, $\text{sign}(\text{disc}(K/\mathbb{Q})) = (-1)^s$ e, portanto, no caso em questão devemos ter $r = s = 1$. Identifiquemos no que segue K como um subcorpo de $\mathbb{R}$ através de sua única imersão real. O teorema da unidade demonstrado na última seção afirma então que $U_K = \{\pm\varepsilon^m : m \in \mathbb{Z}\}$ para alguma unidade ε. Note que como $-\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$ também são unidades fundamentais podemos supor $\varepsilon > 1$.

LEMA 4.3.1. *Nas condições acima descritas tem-se* $|\Delta_K| < 4\varepsilon^3 + 24$.

DEMONSTRAÇÃO. Como $\varepsilon \notin \mathbb{Q}$ e $[K : \mathbb{Q}] = 3$ devemos ter $\mathbb{Q}[\varepsilon] = K$. Também como $s = 1$ devemos ter que os dois conjugados de ε devem ser complexo-conjugados. Denote $\delta e^{i\theta}, \delta e^{-i\theta}$, $0 \leq \theta \leq \pi$ tais conjugados. Devemos ter

$$\pm 1 = \text{Nm}(\varepsilon) = \varepsilon(\delta e^{i\theta})(\delta e^{-i\theta}) = \varepsilon\delta^2 > 0$$

logo $\varepsilon\delta^2 = 1$ e $\delta = \varepsilon^{-1/2}$. Escrevendo $\varepsilon = u^2$, $u \in \mathbb{R}$, $u > 1$ temos $u^{-1}\delta^{i\theta}, u^{-1}\delta^{-i\theta}$ como os conjugados de ε.

Seja $\Delta' = \text{D}(1, \varepsilon, \varepsilon^2)$. Sabemos que $\Delta_K | \Delta'$ pelo observado em 1.3.5 e, portanto, é suficiente mostrarmos que $|\Delta'| < 4\varepsilon^3 + 24$.

Pela proposição 1.3.16 temos

$$\left(\Delta'\right)^{1/2} = \left(u^2 - u^{-1}e^{i\theta}\right)\left(u^2 - u^{-1}e^{-i\theta}\right)\left(u^{-1}e^{i\theta} - u^{-1}e^{-i\theta}\right) =$$

$$= 2i\left(\left(u^3 + u^{-3}\right)\sin\theta - 2\cos\theta\right)\sin\theta.$$

Fazendo $2\xi = u^3 + u^{-3}$ temos $|\Delta'|^{1/2} = 4(\xi - \cos\theta)\sin\theta$ que para u fixado atinge o máximo quando $\xi\cos\theta - \cos^2\theta + \sin^2\theta = 0$, ou seja,

$$\xi\cos\theta - 2\cos^2\theta + 1 = 0$$

Defina $-g(x) = \xi x - 2x^2 + 1$, $|x| \leq 1$. Da fórmula de Bháskara e como $\xi > 1$ (pois $u > 1$ implica $u^3 + u^{-3} > 2$) vemos que uma raíz de $g(x)$ é maior que 1. Sejam x_0, x_1 as raízes com $x_1 > 1$ então como $x_1 x_0 = -1$ temos $-1 < x_0 < 0$. Podemos melhorar nossas estimativas

para x_0 observando que $g(0) = -1$ e

$$g\left(\frac{-1}{2u^3}\right) = 2\left(\frac{-1}{2u^3}\right)^2 - \xi\left(\frac{-1}{2u^3}\right) - 1 = \frac{3}{4}\left(u^{-6} - 1\right) < 0$$

e temos que $-1 < x_0 < -1/2u^3$. Então, $x_0^2 > 1/4u^6$ isto é, $u^{-6} - 4x_0^2 < 0$ donde

$$u^{-6} - 4x_0^{-2} - 4x_0^4 < 0$$

pois $4x_0^2 < x_0^{-2} + x_0^4$ para $|x_0| \leq 1$. Usaremos a expressão acima a seguir.

Substituindo x_0 na expressão para Δ' temos (fazendo $\cos\theta = x_0$)

$$\left|\Delta'\right| \leq 16\left(\xi^2 - 2\xi x_0 + x_0^2\right)\left(1 - x_0^2\right).$$

Usando que $\xi x_0 = 2x_0^2 - 1$ e $\xi^2 x_0^2 = 4x_0^4 - 4x_0^2 + 1$ (pois $g(x_0) = 0$) temos

$$\begin{aligned}\left|\Delta'\right| &\leq 16\left(\xi^2 + 2 - 4x_0^2 + x_0^2 - 4x_0^4 + 4x_0^2 - 1 + 4x_0^4 - 2x_0^2 - x_0^4\right) = \\ &= 16\left(\xi^2 + 1 - x_0^2 - x_0^4\right) = 16\left(\frac{u^6 + 2 + u^{-6}}{4} + 1 - x_0^2 - x_0^4\right) = \\ &= 4u^6 + 24 + 4\left(u^{-6} - 4x_0^2 - 4x_0^4\right) < 4u^6 + 24.\end{aligned}$$

Ou seja, $|\Delta'| < 4\varepsilon^3 + 24$ como queríamos. □

EXEMPLO 4.3.2. Voltando ao exemplo do início do capítulo seja α raiz real de $X^3 + 10X + 1$ e $K = \mathbb{Q}[\alpha]$. Vimos que $\alpha \in U_K$e que $\Delta_K = -4027$ donde pelo lema acima $\varepsilon > \sqrt[3]{\frac{4027-24}{4}} > 10$. Como $\alpha \approx -0,099903$ temos $-\alpha^{-1} \approx 10,00998$ e como $\alpha = \pm\varepsilon^m$, $m \in \mathbb{Z}$ devemos ter $-\alpha^{-1} = \varepsilon$ donde α também é unidade fundamental como tínhamos afirmado no início do capítulo.

4.4. Cálculo de μ_K

Como o título da seção sugere, aqui vamos estabelecer um procedimento (algoritmo) para o cálculo de μ_K.

Vimos que μ_K é composto das raízes da unidade que estão em K. No próximo capítulo vamos mostrar que se ζ_m é uma raíz m-ésima primitiva da unidade, isto é, $(\zeta_m)^m = 1$ e m é o menor valor positivo do expoente para que isso aconteça, então $\mathbb{Q}[\zeta_m]$ é uma extensão Galoisiana de $\mathbb{Q}$ com grupo de Galois isomorfo a $\mathbb{Z}_m^\times$. Disso segue que se $\zeta_m \in K$, como $\mathbb{Q}[\zeta_m] \subseteq K$, então $\varphi(m) = [\mathbb{Q}[\zeta]{:}\mathbb{Q}] \,|\, [K : \mathbb{Q}]$ onde $\varphi(m) := \text{card}(\mathbb{Z}_m^\times)$ é a função totiente de Euler.

Em particular dado K existe apenas uma quantidade finita de possibilidades para m. Para cada m precisamos testar se $\text{Irr}(\zeta_m, \mathbb{Q}) \in \mathbb{Q}[X]$ tem raíz em K. Uma tal raiz tem módulo limitado pelos coeficientes de $\text{Irr}(\zeta_m, \mathbb{Q})$ e, portanto, há um limitante para os coeficientes dos fatores de uma possível decomposição de $\text{Irr}(\zeta_m, \mathbb{Q})$ em $\mathbb{Z}_K[X]$. Tomando uma base integral para $\mathbb{Z}_K$ temos uma quantidade finita de possíveis coordenadas para tais coeficientes. O problema então se reduz a uma busca por tentativa e erro.

4.5. Cálculo de um sistema de unidades fundamentais

Agora, vejamos um algoritmo para o cálculo da parte livre do grupo de unidades.

O cálculo de unidades no caso geral se concentra em achar muitas soluções para equações do tipo $\mathrm{Nm}(\alpha) = m$, onde m é fixo e então tomar o quociente de tais soluções. Tais equações são um tipo especial de equação diofantina denominadas equações de Pell. Felizmente para tais equações possuímos algoritmos eficientes para o cálculo de soluções.

Como existem apenas uma quantidade finita de ideais $\mathfrak{a}$ com $\mathbb{N}(\mathfrak{a}) = m$, se tivermos mais soluções para a equação acima do que o número destes ideais então freqüentemente teremos $\alpha_i\mathbb{Z}_K = \alpha_j\mathbb{Z}_K$ donde α_i/α_j é uma unidade. Fica então apenas restando achar um número $r + s - 1$ de tais unidades que sejam linearmente (integralmente) independentes, para o qual também possuímos algoritmos eficientes.

Para uma exposição detalhada de tais algoritmos recomendamos [**Coh96**, Cap.1]. Note que o método descrito aqui é em essência o mesmo que o usado na demonstração do teorema da unidade.

4.6. Reguladores

Nesta última seção definiremos apenas por completeza, já que nada daqui será usado adiante, outro importante invariante de K. Seja $t = r + s - 1$ e $u_1, ..., u_t$ um sistema de unidades fundamentais. Então $L(u_i)$ (definido anteriormente no capítulo) geram o reticulado $L(U_K)$ em $\mathbb{R}^t$.

DEFINIÇÃO 4.6.1. O regulador de K, denotado por $\mathrm{Reg}(K)$, é definido como o determinante da matriz cuja i-ésima linha é $L(u_i)$. A menos de sinal, este é o volume do paralelepípedo fundamental de $L(U_K)$.

O regulador atua para U_K/μ_K (unidades módulo torção) da mesma forma que o discriminante atua para $\mathbb{Z}_K$. Pode-se definir o regulador para um conjunto qualquer $\{\varepsilon_1, ..., \varepsilon_t\}$ de unidades (na realidade já o usamos na demonstração do lema 4.3.1) e então

$$(U_K : \mathrm{span}\,(\{\varepsilon_1, ..., \varepsilon_t\} \cup \mu_K))^2 = \frac{|\mathrm{Reg}(\varepsilon_1, ..., \varepsilon_t)|}{|\mathrm{Reg}(K)|}$$

como com o discriminante.

Parte 3

A Teoria para as Extensões Ciclotômicas e o Último Teorema de Fermat

CAPíTULO 5

Extensões Ciclotômicas

Neste curto capítulo identificaremos as construções da teoria algébrica de números desenvolvida anteriormente no caso das extensões ciclotômicas de $\mathbb{Q}$ que, por definição, são as geradas por raízes da unidade. Elas proporcionam exemplos importantes da teoria[1] além de possuírem aplicações em outros problemas como o Último Teorema de Fermat que veremos no próximo capítulo.

DEFINIÇÃO 5.0.2. Um elemento ζ de um corpo L é uma raíz n-ésima primitiva da unidade se e somente se $\zeta^n = 1$ e $n \in \mathbb{N}$ é mínimo com tal propriedade. Em outras palavras, ζ é elemento de ordem n do grupo multiplicativo $L^\times$.

EXEMPLO 5.0.3. Em $\mathbb{C}$ as raízes n-ésimas da unidade tem a forma $e^{2\pi i(m/n)}$, $m, n \in \mathbb{Z}$. O lema a seguir afirma, em particular, que uma tal raíz é primitiva se e somente se m é primo com n.

LEMA 5.0.4. *Seja $\zeta \in L$ uma raiz n-ésima primitiva da unidade. Então ζ^m é uma raiz n-ésima primitiva da unidade se e somente se m é primo com n.*

DEMONSTRAÇÃO. Suponha que ζ^m tem ordem n em $L^\times$ e seja d um divisor comum de m e n. Então

$$(\zeta^m)^{\frac{n}{d}} = (\zeta^n)^{\frac{m}{d}} = 1$$

donde necessariamente $d = 1$ e segue o desejado. Reciprocamente, se m e n são primos entre si existem $a, b \in \mathbb{Z}$ tal que $am + bn = 1$ e então $\zeta = \zeta^{am+bn} = \zeta^{am}$. Assim, se $(\zeta^m)^d = 1$ teremos

$$\zeta^d = (\zeta^{am})^d = (\zeta^{md})^a = 1$$

donde $n|d$ pois ζ tem ordem n. Logo, ζ^m tem ordem maior ou igual a n. Como $(\zeta^m)^n = (\zeta^n)^m = 1$ ele tem, de fato, ordem n. □

Em tudo que segue neste capítulo fixamos $K := \mathbb{Q}[\zeta]$ onde ζ é uma raiz n-ésima primitiva da unidade. Note que $\zeta^i \neq \zeta^j$ para $i \neq j \bmod n$. Segue que K possui todas as raízes de $X^n - 1$ (as raízes n-ésimas da unidade). Como K é gerado por tais raízes

[1] As extensões ciclotômicas foram, historicamente, os primeiros e mais importantes exemplos para a teoria algébrica de números. Tal foi seu uso que por alguns anos as suas propriedades aritméticas particulares foram erroneamente tomadas como propriedades compartilhadas por todas as extensões numéricas (isto é, sobre $\mathbb{Q}$). Por exemplo para extensões ciclotômicas tem-se $\mathbb{Z}_{\mathbb{Q}[\zeta]} = \mathbb{Z}[\zeta]$ (veremos adiante) e acreditou-se que isso seria válido em geral, coisa que vimos ser falso no exemplo 1.3.21.

ele é o corpo de decomposição de $X^n - 1$ [**Mil98b**, pg.23], em particular, $\mathbb{Q} \subseteq K$ é uma extensão Galoisiana. Seja $G := \mathrm{Gal}(K/\mathbb{Q})$. É fácil ver que os elementos de ordem n de K são estáveis pela ação de G, isto é, o subgrupo gerado pelos elementos de ordem n de K é preservado por G. Portanto, pelo lema acima, dado $\tau \in G$ tem-se $\tau(\zeta) = \zeta^m$, onde m é primo com n e único módulo n. Temos então um monomorfismo (lembrando que os elementos regulares de $\mathbb{Z}_n$ são justamente as imagens do números primos com n) $G \longrightarrow \mathbb{Z}_n^\times$.

Vamos mostrar a seguir que esta aplicação é um isomorfismo o que, por resultados clássicos da teoria de Galois, equivale à igualdade

$$[K : \mathbb{Q}] = \varphi(n) := \mathrm{card}\left(\mathbb{Z}_n^\times\right)$$

onde φ é a aplicação totiente de Euler.

Definição 5.0.5. O n-ésimo polinômio ciclotômico é definido como

$$\Phi_n(X) := \prod (X - \zeta')$$

onde ζ' percorre o conjunto das raízes n-ésimas primitivas da unidade.

Pelo discutido acima, G fixa Φ_n, donde $\Phi_n \in \mathbb{Q}[X]$. Como $\Phi_n(\zeta) = 0$ temos que $\Phi_n = \mathrm{Irr}(\zeta, \mathbb{Q})$ se e somente se Φ_n é irredutível. Neste caso teremos $[K : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$. Em suma, temos as seguintes equivalências:

(1) $G \cong \mathbb{Z}_n^\times$
(2) $[K : \mathbb{Q}] = \varphi(n)$
(3) G age transitivamente nas raízes n-ésimas primitivas da unidade.
(4) Φ_n é irredutível.

Note que cada raíz n-ésima da unidade é uma raiz d-ésima primitiva da unidade para exatamente um d divisor de n, pois se $\zeta^n - 1 = 0$, então ζ tem ordem, no máximo, n e sua ordem divide n. Segue que

$$X^n - 1 = \prod_{d|n} \Phi_n(X). \tag{5.0.1}$$

Examinemos primeiro o caso $n = p^r$, p primo.

Proposição 5.0.6. *Nas condições acima descritas para K e com $n = p^r$, p primo tem-se:*

(1) *$K \supseteq \mathbb{Q}$ tem grau igual a $\varphi(p^r) = p^{r-1}(p-1)$.*
(2) *O anel de inteiros de K é $\mathbb{Z}[\zeta]$.*
(3) *O elemento $\pi := \zeta - 1$ é primo em $\mathbb{Z}_K$ e $p\mathbb{Z}_K = (\pi)^e$ com $e = \varphi(p^r)$.*
(4) *Tem-se $\mathrm{disc}(\mathbb{Z}_K/\mathbb{Z}) = \pm p^c$ para algum $c \in \mathbb{N}$. Em particular, p é o único primo que se ramifica em $\mathbb{Q}$.*

Demonstração. Primeiro note que, obviamente, $\mathbb{Z}[\zeta] \subseteq \mathbb{Z}_K$ e que se ζ' é outra raiz p^r-ésima primitiva da unidade então $\zeta' = \zeta^s$ e $\zeta = (\zeta')^t$, para $s, t \in \mathbb{N}$. Logo, $\mathbb{Q}[\zeta'] = K$ e

$\mathbb{Z}[\zeta'] = \mathbb{Z}[\zeta]$. Agora,

$$1-\zeta' = 1-\zeta^s = (1-\zeta)\left(1+\zeta+...+\zeta^{s-1}\right) \implies \frac{1-\zeta'}{1-\zeta} = 1+\zeta+...+\zeta^{s-1} \in \mathbb{Z}[\zeta]$$

e similarmente $1-\zeta/1-\zeta' \in \mathbb{Z}[\zeta]$ donde $1-\zeta/1-\zeta'$ é uma unidade de $\mathbb{Z}[\zeta]$ bem como de $\mathbb{Z}_K$.

A equação (5.0.1) nos dá:

$$X^{p^r}-1 = \prod_{d|p^r} \Phi_d(X) = \Phi_p(X)\Phi_{p^2}(X)...\Phi_{p^r}(X) =$$

$$= \left(\prod_{d|p^{r-1}} \Phi_d(X)\right)\Phi_{p^r}(X) = \left(X^{p^{r-1}}-1\right)\Phi_{p^r}(X) \implies$$

$$\implies \Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \frac{t^p-1}{t-1} = 1+t+...+t^{p-1};\ t = X^{p^{r-1}}. \tag{5.0.2}$$

Segue que $\Phi_{p^r}(1) = p$. Usando a definição de Φ_{p^r} temos que

$$p = \Phi_{p^r}(1) = \prod\left(1-\zeta'\right) = \prod \frac{1-\zeta'}{1-\zeta}(1-\zeta) = u\prod(1-\zeta) = u\,(1-\zeta)^{\varphi(p^r)}$$

onde $u \in \mathbb{Z}[\zeta]^\times$. Portanto, temos a seguinte igualdade de ideais em $\mathbb{Z}_K$:

$$(p) = (\pi)^e;\ \pi := 1-\zeta,\ e = \varphi\left(p^r\right).$$

Como $\varphi(p^r) \geq [K:\mathbb{Q}]$, do fato do homomorfismo $G \longrightarrow \mathbb{Z}_{p^r}^\times$ discutido anteriormente ser injetor e do teorema 2.6.2 devemos ter $f = g = 1$, ou seja, (π) é ideal primo em $\mathbb{Z}_K$ tal que $f\left((\pi)/(p)\right) = 1$ e $(p) = (\pi)^{\varphi(p^r)}$. Com isto provamos (1) e (3).

Agora vamos provar que $\mathrm{disc}(\mathbb{Z}[\zeta]/\mathbb{Z})$ é potência de p. Da observação 1.3.5 isto implicará que $\mathrm{disc}(\mathbb{Z}_K/\mathbb{Z})$ é potência de p (provando (4)) e que $(\mathbb{Z}_K : \mathbb{Z}[\zeta])$ é potência de p. Neste caso, $p^M(\mathbb{Z}_K/\mathbb{Z}[\zeta]) = 0$ para algum $M \in \mathbb{N}$, ou seja, $p^M\mathbb{Z}_K \subseteq \mathbb{Z}[\zeta]$.

Já sabemos que $\Phi_{p^r} = \mathrm{Irr}(\zeta, \mathbb{Q})$ podemos então usar a proposição 1.3.16 para calcular $\mathrm{disc}(\mathbb{Z}[\zeta]/\mathbb{Z})$. Assim,

$$\mathrm{disc}\left(\mathbb{Z}[\zeta]/\mathbb{Z}\right) = \mathrm{disc}\left(\Phi_{p^r}(X)\right) = \pm\,\mathrm{Nm}_{K/\mathbb{Q}}\left(\Phi'_{p^r}(\zeta)\right)$$

Diferenciando a primeira equação da expressão (5.0.2) e substituindo X por ζ obtemos

$$\Phi'_{p^r}(\zeta) = \frac{p^r\zeta^{p^r-1}}{\zeta^{p^{r-1}}-1}.$$

Como ζ é unidade (pois $\zeta^n = 1 \implies \zeta^{-1} = \zeta^{n-1}$) temos $\mathrm{Nm}_{K/\mathbb{Q}}\,\zeta = \pm 1$ e é claro que $\mathrm{Nm}_{K/\mathbb{Q}}(p^r) = (p^r)^{\varphi(p^r)} = p^{r\varphi(p^r)}$. Calculemos $\mathrm{Nm}_{K/\mathbb{Q}}(\zeta^{p^s}-1)$. Primeiro, para $s = 0$: o polinômio mínimo de $1-\zeta$ é $f(X) := \Phi_{p^r}(1-X)$ já que ele é mônico e irredutível pois se $\Phi_{p^r}(1-X) = P(X)Q(X)$ com P e Q não constantes então $\Phi_{p^r}(X) = P(1-X)Q(1-X)$ contrariando a minimalidade de $\Phi_{p^r}(X)$. Agora, f tem termo constante $f(0) = \Phi_{p^r}(1) = p$.

Vimos que, a menos de sinal, a norma de um elemento é exatamente o termo constante do seu polinômio mínimo. Logo, $\mathrm{Nm}_{K/\mathbb{Q}}(1-\zeta) = \pm p$. Usando isso, calculemos agora para $s < r$: é claro que ζ^{p^s} é uma raiz p^{r-s}-ésima primitiva da unidade e o cálculo acima (com $r-s$ no lugar de r) mostra que

$$\mathrm{Nm}_{\mathbb{Q}[\zeta^{p^s}]/\mathbb{Q}}\left(1-\zeta^{p^s}\right) = \pm p.$$

Pela transitividade da norma em torres de extensões e do fato que $\mathrm{Nm}_{M/L}\,\alpha = \alpha^{[M:L]}$ para $\alpha \in L$ temos que $\mathrm{Nm}_{K/\mathbb{Q}}(1-\zeta^{p^s}) = p^a$, $a < r$. Portanto,

$$\mathrm{Nm}_{K/\mathbb{Q}}\left(\Phi'_{p^r}(\zeta)\right) = \pm\frac{p^r\varphi\left(p^r\right)}{p^a} = p^c,\ c \in \mathbb{N}$$

pois $a < r$.

Resta-nos mostrar (2). Como $f((\pi)/(p)) = 1$ temos que a inclusão $\mathbb{Z} \hookrightarrow \mathbb{Z}_K$ induz um isomorfismo $\mathbb{Z}_p \cong \mathbb{Z}_K/(\pi)$. Em particular $\mathbb{Z} + \pi\mathbb{Z}_K = \mathbb{Z}_K$ e, é claro, $\mathbb{Z}[\zeta] + \pi\mathbb{Z}_K = \mathbb{Z}_K$. Multiplicando por π temos também $\pi\mathbb{Z}[\zeta] + \pi^2\mathbb{Z}_K = \pi\mathbb{Z}_K$. Dado $\alpha \in \mathbb{Z}_K$ usando estas duas equações podemos escrever

$$\alpha = \alpha' + \gamma;\ \alpha' \in \pi\mathbb{Z}_K, \gamma \in \mathbb{Z}[\zeta]$$

$$\alpha' = \alpha'' + \gamma';\ \alpha'' \in \pi^2\mathbb{Z}_K, \gamma' \in \mathbb{Z}[\zeta].$$

Logo, $\alpha = (\gamma + \gamma') + \alpha'$, ou seja, temos que $\mathbb{Z}_K \subseteq \mathbb{Z}[\zeta] + \pi^2\mathbb{Z}_K$ provando que $\mathbb{Z}_K = \mathbb{Z}[\zeta] + \pi^2\mathbb{Z}_K$. De maneira geral temos $\mathbb{Z}_K = \mathbb{Z}[\zeta] + \pi^m\mathbb{Z}_K$, $\forall m \in \mathbb{N}$. Mas vimos que para $m \geq M$ tem-se $p^m\mathbb{Z}_K \subseteq \mathbb{Z}[\zeta]$ donde

$$\forall m \geq M,\ \mathbb{Z}[\zeta] + \pi^m\mathbb{Z}_K = \mathbb{Z}[\zeta].$$

Isto mostra que devemos ter $\mathbb{Z}_K = \mathbb{Z}[\zeta]$ como queríamos. □

Observação 5.0.7. O sinal de $\mathrm{disc}(K/\mathbb{Q})$ pode ser facilmente calculado a partir do critério de Stickelberger. Como K não possui imersões reais a menos que $\zeta = \pm 1$ (neste caso $K = \mathbb{Q}$) temos $\mathrm{sign}(\mathrm{disc}(K/\mathbb{Q})) = (-1)^s$, onde $s = [K:\mathbb{Q}]/2 = \varphi(p^r)/2 = (p-1)p^{r-1}/2$. Se $p = 2$ temos s ímpar se e somente se $r = 2$. Se $p \neq 2$ temos $p \equiv 1 \bmod 4$ ou $p \equiv 3 \bmod 4$ e é imediato que s é ímpar se e somente se tem-se o último.

Observação 5.0.8. Sejam ζ e ζ', respectivamente, raízes p^r-ésima e q^s-ésima primitivas da unidade com $p \neq q$. Então $\mathbb{Q}[\zeta] \cap \mathbb{Q}[\zeta'] = \mathbb{Q}$, pois da proposição acima resulta que $L \subseteq \mathbb{Q}[\zeta]$ implica que p é o único possível primo que ramifica-se em L e o análogo vale para $\mathbb{Q}[\zeta']$. Como a intersecção dos dois está contida em ambos devemos ter $\mathbb{Q}[\zeta] \cap \mathbb{Q}[\zeta'] = \mathbb{Q}$.

A seguir vamos ao caso n arbitrário.

LEMA 5.0.9. *Sejam L e M extensões finitas de $\mathbb{Q}$ tais que $[LM:\mathbb{Q}] = [L:\mathbb{Q}][M:\mathbb{Q}]$ onde LM denota o compósito*[2] *de L e M e seja $d = \gcd(\mathrm{disc}(\mathbb{Z}_L), \mathrm{disc}(\mathbb{Z}_M))$. Então $\mathbb{Z}_{LM} \subseteq d^{-1}\mathbb{Z}_L\mathbb{Z}_M$.*

DEMONSTRAÇÃO. Sejam $\{\alpha_1, ..., \alpha_l\}$ e $\{\beta_1, ..., \beta_m\}$ bases integrais de L e M respectivamente. Então $\{\alpha_i\beta_j\}_{i,j}$ gera LM e da hipótese da dimensão, forma uma base para LM sobre $\mathbb{Q}$. Assim, qualquer $\gamma \in \mathbb{Z}_{LM}$ pode ser escrito como

$$\gamma = \sum_{i,j} \frac{a'_{ij}}{r_{ij}}\alpha_i\beta_j;\ a'_{ij}, r_{ij} \in \mathbb{Z}$$

que fazendo $r := \gcd(r_{ij})$ podemos reescrever como

$$\gamma = \sum_{i,j} \frac{a_{ij}}{r}\alpha_i\beta_j;\ a_{ij}, r \in \mathbb{Z} \tag{5.0.3}$$

e de maneira que nenhum fator primo de r divide todos os a_{ij}. Precisamos mostrar então que $r|d$ pois, neste caso, se $s = d/r$ então $d^{-1} = (rs)^{-1}$ e

$$\gamma = \sum_{i,j} \frac{a_{ij}s}{d}\alpha_i\beta_j \in d^{-1}\mathbb{Z}_L\mathbb{Z}_M.$$

Identifiquemos M com um subcorpo de $\mathbb{C}$ (através de uma imersão qualquer) e seja σ uma imersão de L em $\mathbb{C}$. Afirmamos que σ estende-se de maneira única para uma imersão de LM em $\mathbb{C}$. Para isso, escreva $L = \mathbb{Q}[\alpha]$ (aqui, usamos o teorema do elemento primitivo) e segue então que $LM = M[\alpha]$. Da hipótese de dimensão deduzimos que $\mathrm{Irr}(\alpha, \mathbb{Q}) = \mathrm{Irr}(\alpha, M)$ (caso contrário teríamos $[LM:\mathbb{Q}] < [L:\mathbb{Q}][M:\mathbb{Q}]$). Assim, existe um (único) L-homomorfismo τ mapeando α em $\sigma(\alpha)$, isto é, tal que $\tau|_L = \sigma$. Podemos, então, abusar e denotar τ por σ também. Aplicando σ na fórmula (5.0.3) acima obtemos

$$\sigma(\gamma) = \sum_{i,j} \frac{a_{ij}}{r}\sigma(\alpha_i)\beta_j.$$

Escreva $x_i := \sum_j (a_{ij}/r)\beta_j$, de forma que se $\sigma_1, ..., \sigma_m$ são as imersões de L em $\mathbb{C}$ tenhamos o seguinte sistema de equações lineares:

$$\sum_i \sigma_k(\alpha_i)\, x_i = \sigma_k(\gamma)\,;\ 1 \leq k \leq m.$$

Pela regra de Cramer temos $Dx_i = D_i$, onde $D = \det(\sigma_k(\alpha_i))$ e $D_i \in \mathbb{Z}_{LM}$ pois D_i é um determinante de uma matriz com coeficientes em $\mathbb{Z}_{LM}$. Sabemos da proposição 1.3.7 que $D^2 = \mathrm{disc}(\mathbb{Z}_L/\mathbb{Z}) = \Delta_L$, de onde $\Delta_L x_i = DD_i \in \mathbb{Z}_{LM}$ e, por outro lado, $\Delta_L x_i \in M$. Assim, como $\Delta_L x_i \in M \cap \mathbb{Z}_{LM}$ devemos ter $\Delta_L x_i \in \mathbb{Z}_M$. Agora, $\Delta_L x_i = \sum_j \Delta_L(a_{ij}/r)\beta_j$ e $\{\beta_j\}$ é base integral, portanto, $(\Delta_L a_{ij})/r \in \mathbb{Z}$, ou seja, $r|\Delta_L a_{ij}$, $\forall i, j$. Segue que $r|\Delta_L$.

Similarmente deduzimos que $r|\Delta_M$ donde $r|d$ como queríamos. □

[2] O menor corpo contendo os corpos dados.

THEOREM 5.0.10. *Seja ζ uma raiz n-ésima primitiva da unidade, $n \in \mathbb{N}$ e $K = \mathbb{Q}[\zeta]$ como antes. Então:*

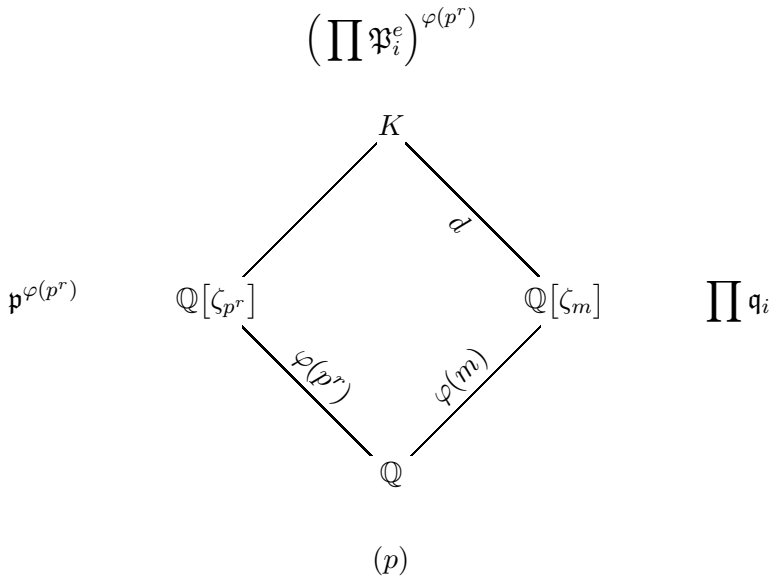
(1) *K tem grau $\varphi(n)$ sobre $\mathbb{Q}$.*
(2) *O anel de inteiros de K é $\mathbb{Z}[\zeta]$*
(3) *Se p ramifica-se em K então $p|n$. Mais precisamente, se $n = p^r m$ com $p \nmid m$ então*

$$(p) = (\mathfrak{p}_1 ... \mathfrak{p}_s)^{\varphi(p^r)}$$

em K com $\mathfrak{p}_i$ primos distintos de $\mathbb{Z}_K$.

DEMONSTRAÇÃO. Procederemos por indução no número de primos dividindo n. No caso deste número ser 1 temos $n = p^r$ que é a proposição 5.0.6. No caso de ele possuir mais de um primo em sua fatoração, selecione um e escreva $n = p^r m$ com $p \nmid m$. Como m possui menos primos em sua fatoração podemos assumir, pela hipótese de indução, o teorema válido para ele. Defina $\zeta_{p^r} := \zeta^m$ e $\zeta_m := \zeta^{p^r}$ notando que ζ_{p^r} e ζ_m são raízes p^r-ésima e m-ésima primitivas da unidade, respectivamente. Note também que $K = \mathbb{Q}[\zeta] = \mathbb{Q}[\zeta_{p^r}]\mathbb{Q}[\zeta_m]$.

Sabemos que $[\mathbb{Q}[\zeta_{p^r}] : \mathbb{Q}] = \varphi(p^r)$ e $[\mathbb{Q}[\zeta_m] : \mathbb{Q}] = \varphi(m)$ pela hipótese de indução. Considere o seguinte diagrama que mostra a fatorização de $(p)\mathbb{Z}_K$ e onde os números no interior do losango são as respectivas dimensões das extensões:



Os $\mathfrak{q}_i$ são distintos, pois pela hipótese de indução p não ramifica-se em $\mathbb{Q}[\zeta_m]$. Além disso, os índices de ramificação dos $\mathfrak{P}_i$ são os mesmos, pois $\mathbb{Q}[\zeta_{p^r}] \subseteq K$ é Galoisiana. Sabemos do discutido no início deste capítulo que $[K : \mathbb{Q}] \leq \varphi(n)$. Em particular, temos $d \leq \varphi(n)/\varphi(m) = \varphi(p^r)$ (a função totiente de Euler é multiplicativa). Mas observe que $\mathfrak{P}_i | \mathfrak{q}_k$ para algum k. Neste caso, $(\mathfrak{P}_i^e)^{\varphi(p^r)} | \mathfrak{q}_k$, pois um primo não pode estar acima de

dois primos distintos. Portanto, do teorema 2.6.2 devemos ter $e\varphi(p^r) \leq d \leq \varphi(p^r)$ donde $d = \varphi(p^r)$ e $e = 1$. Isto demonstra (1) e (3).

Para (2) observe que $p \nmid \text{disc}(\mathbb{Z}_{\mathbb{Q}[\zeta_m]}/\mathbb{Z})$ donde como $\text{disc}(\mathbb{Z}_{\mathbb{Q}[\zeta_{p^r}]}/\mathbb{Z}) = \pm p^c$ temos que tais discriminantes são primos entre si. Do lema anterior segue que

$$\mathbb{Z}_K \subseteq \mathbb{Z}_{\mathbb{Q}[\zeta_{p^r}]}\mathbb{Z}_{\mathbb{Q}[\zeta_m]} = \mathbb{Z}[\zeta_{p^r}]\mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta]$$

onde, novamente, usamos a hipótese de indução e a proposição anterior. Segue que $\mathbb{Z}_K = \mathbb{Z}[\zeta]$. □

Com isso encerramos este capítulo onde conseguimos resultados importantes sobre a aritmética das extensões ciclotômicas.

CAPíTULO 6

O Último Teorema de Fermat Para Primos Regulares

Neste último capítulo usaremos a teoria desenvolvida até aqui para dar uma solução parcial para um problema famosíssimo: o último teorema de Fermat. Até a solução completa dada por A. Wiles em 1995 o que apresentaremos aqui era o melhor resultado na direção de resolver este problema. Esta solução parcial é atribuída a E. Kummer, matemático alemão a quem boa parte da teoria dos domínios de Dedekind (não na linguagem e generalidade aqui desenvolvidas, é claro) é atribuída. Em realidade, Kummer não buscava diretamente resolver o problema de Fermat quando desenvolvia sua teoria, mas, com o tempo ficou evidente a abrangência e utilidade desta.

O problema de Fermat consiste em provar a seguinte afirmação: dado $n \geq 3$, $n \in \mathbb{N}$ não existe solução inteira para a equação

$$X^n + Y^n = Z^n. \tag{6.0.4}$$

Este é um exemplo de um problema diofantino particularmente difícil, visto que as técnicas usuais, como a utilizada para resolver as equações de Pell discutidas brevemente no capítulo sobre o teorema da unidade, falham.

Hoje em dia este problema também pode ser descrito como um problema de Geometria Aritmética. Se dividirmos a equação acima por Z^n obtemos a seguinte equação:

$$\alpha^n + \beta^n = 1;\ \alpha, \beta \in \mathbb{Q}.$$

Enquanto que a Geometria Algébrica preocupa-se em descrever as propriedades geométricas e, em última instância, encontrar as soluções para um sistema algébrico[1] sobre um corpo algebricamente fechado, a geometria aritmética propõe-se em estudar o comportamento destes mesmos problemas sobre a mudança do corpo subjacente. Em geral estuda-se estes problemas sobre uma extensão finita de $\mathbb{Q}$. Uma ótima referência para este campo moderno e muito abrangente é [**Lor95**]. A solução apresentada por A. Wiles para o problema pertence a este campo e é uma abordagem muitíssimo diferente da utilizada aqui.

Em primeiro lugar observe que podemos reduzir o problema para expoentes primos. De fato, se provarmos a inexistência de soluções para os primos e se $x, y, z \in \mathbb{Z}$ é uma solução para o expoente n sendo $p|n$, p primo, então $x^{n/p}, y^{n/p}, z^{n/p}$ seria uma solução para o expoente p e teríamos um absurdo. Por fim prova-se facilmente em [**Edw77**, Seção 1.5, pg. 9] que não existe solução para o caso $n = 4$ de maneira a excluir os números da

[1] Conjunto finito de polinômios com coeficientes em um corpo.

forma 2^k, $k > 1$ que são os únicos naturais maiores que 2 não divisíveis por um primo $p > 2$.

Aqui usaremos o que conhecemos da aritmética das extensões ciclotômicas para mostrar que nela conseguimos uma fatoração conveniente para a equação de Fermat e que, com algumas hipóteses adicionais sobre o expoente primo p [2], de fato, é impossível uma tal solução.

Para mais informações históricas indicamos o livro [**Edw77**]. Na próxima seção vamos expor a idéia principal da demonstração que consiste na fatoração "inteligente" da equação (6.0.4) dada por Lamé e implicitamente presente nas soluções dadas por Euler para o caso $p = 3$ e Dirichlet para o caso $p = 5$.

6.1. A idéia de Lamè e o caso (I) do teorema de Fermat

Suponha que (x, y, z) é uma solução inteira da equação de Fermat (6.0.4) onde $n = p$ com p primo ímpar. Primeiramente, note que podemos supor x, y, z dois-a-dois primos entre si, pois se dois deles tem um fator em comum o terceiro necessariamente também terá este fator de forma que podemos eliminá-lo da equação.

Nesta seção vamos expor a idéia principal e demonstrar o último teorema de Fermat no caso particular onde supomos que $p \nmid xyz$, isto é, que p não divide nenhum dos números da hipotética solução. Este é o denominado caso (I) do teorema de Fermat.

Considere o polinômio $t^p + 1$ cujas raízes são $-1, -\zeta, ..., -\zeta^{p-1}$ onde ζ é uma raíz p-ésima primitiva da unidade. Assim, $t^p + 1 = \prod_{i=0}^{p-1}(t + \zeta^i)$. Substituindo t por x/y obtemos:

$$\left(\frac{x}{y}\right)^p + 1 = \prod_{i=0}^{p-1}\left(\frac{x}{y} + \zeta^i\right) \implies \frac{x^p}{y^p} + 1 = \frac{1}{y^p}\prod_{i=0}^{p-1}\left(x + y\zeta^i\right) \implies x^p + y^p = \prod_{i=0}^{p-1}\left(x + y\zeta^i\right)$$

isto é,

$$z^p = \prod_{i=0}^{p-1}\left(x + y\zeta^i\right). \tag{6.1.1}$$

A equação acima é o ponto chave da demonstração e foi primeiramente considerada por Lamè. Este, sem o suporte da teoria dos inteiros ciclotômicos, achava que os números da forma $a + b\zeta^i$; $a, b \in \mathbb{Z}$ seriam os inteiros da extensão $K := \mathbb{Q}[\zeta]$. Assim, como pelo lema abaixo os fatores da equação são primos entre si, cada fator deveria ser uma p-ésima potência. Vimos que, realmente, $\mathbb{Z}_K = \mathbb{Z}[\zeta]$ mas a conclusão que os fatores são p-ésimas potências é falsa em geral. Isto foi apontado por Liouville, já era sabido por Kummer e se deve ao fato que $\mathbb{Z}[\zeta]$ não necessariamente é domínio fatorial, como vimos. A teoria do grupo de classes de ideais responde justamente esta pergunta.

[2] Explicitamente a hipótese que $p \nmid h_{\mathbb{Q}[\zeta]}$ onde ζ é uma raíz p-ésima primitiva da unidade.

LEMA 6.1.1. *Nas hipóteses da seção, os elementos $x+\zeta^i y \in \mathbb{Z}[\zeta]$ são dois-a-dois primos entre si.*

DEMONSTRAÇÃO. Vamos mostrar que não existe um ideal primo $\mathfrak{q}$ dividindo $(x+\zeta^i y)$ e $(x+\zeta^j y)$, simultaneamente, se $i \neq j$. Supondo o contrário temos

$$\mathfrak{q} \mid \left(x+\zeta^i y - x - \zeta^j y\right) = \left(\zeta^i - \zeta^j\right) y = \left(1-\zeta^{j-i}\right) y = \mathfrak{p} y \tag{6.1.2}$$

pois $\zeta^{j-i} = \zeta^k$ para $k \equiv j-i \bmod p$ e $1 \leq k \leq p-1$ ($k \neq 0$ pois $i \neq j$) e $\mathfrak{p} = (1-\zeta)$ como no capítulo anterior. Similarmente $\mathfrak{q} | \mathfrak{p} x$. Como x e y são primos entre si temos $\mathfrak{p} = \mathfrak{q}$. Agora $(x+y) = (x+\zeta^i y)$ como ideais pois $\zeta \in U_K$. Logo, $x+y \equiv x+\zeta^i y \equiv 0 \bmod \mathfrak{p}$. Mas então $x+y \in \mathfrak{p} \cap \mathbb{Z} = (p)$ e $z^p = x^p + y^p \equiv x+y \equiv 0 \bmod p$ donde $p|z$ o que é absurdo. □

A idéia genial de Kummer é observar que como $\mathbb{Z}[\zeta]$ tem fatoração única de ideais podemos olhar para a equação (6.1.1) como expressando uma igualdade de ideais. Como pelo lema acima os fatores são primos entre si, cada fator é uma p-ésima potência de um ideal fracionário. Isto é, podemos escrever

$$\left(x+\zeta^i y\right) = \mathfrak{a}_i^p. \tag{6.1.3}$$

A seguir, Kummer fez a hipótese adicional que $p \nmid h_K$ onde, como antes, h_K denota o número de classe de K. Com esta hipótese temos que $\mathrm{Cl}(K)$ não tem elementos de ordem p de forma que na equação acima devemos ter $\mathfrak{a}_i \in \mathrm{P}(\mathbb{Z}[\zeta])$ (na notação do capítulo 3, $P(\mathbb{Z}_K)$ é o subgrupo dos ideais principais), isto é, $\mathfrak{a}_i = (\alpha_i)$; $\alpha_i \in \mathbb{Z}[\zeta]$ e assim conseguimos "consertar" a demonstração de Lamè que vamos expor.

LEMA 6.1.2. *Para todo $\alpha \in \mathbb{Z}[\zeta]$, $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\zeta]$.*

DEMONSTRAÇÃO. Escreva $\alpha = a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2}$; $a_i \in \mathbb{Z}$. Então

$$\alpha^p = \left(a_0 + ... + a_{p-2}\zeta^{p-2}\right)^p \equiv a_0^p + a_1^p\left(\zeta\right)^p + ... + a_{p-2}^p\left(\zeta^{p-2}\right)^p \bmod p\mathbb{Z}[\zeta]$$

pois os coeficientes binomiais são múltiplos de p. Agora $\zeta^p = 1$ donde

$$\alpha^p \equiv a_0^p + ... + a_{p-2}^p \bmod p\mathbb{Z}[\zeta]$$

o que mostra o desejado. □

O lema acima mostra que em $\mathbb{Z}[\zeta]$ toda p-ésima potência é congruente, módulo p, a um inteiro.

LEMA 6.1.3. *Suponha $\alpha = a_0 + a_1\zeta + ... + a_{p-1}\zeta^{p-1}$, com $a_i \in \mathbb{Z}$ e pelo menos um $a_j = 0$. Então se α é divisível por um inteiro n, isto é, $\alpha \in n\mathbb{Z}[\zeta]$ então cada a_i é divisível por n.*

DEMONSTRAÇÃO. Sabemos que $\Phi_p(X) = 1+X+...+X^{p-1}$ pois $X^p-1 = (X-1)\Phi_p(X)$ assim $0 = 1+\zeta+...+\zeta^{p-1}$. Segue daí que qualquer subconjunto de $\{1, \zeta, ..., \zeta^{p-1}\}$ com $p-1$ elementos é uma base de $\mathbb{Z}[\zeta]$. Suponha que $a_{i_0} = 0$ então escrevendo $\alpha = n\beta$; $\beta \in \mathbb{Z}[\zeta]$ e

como $\{1, \zeta, ..., \zeta^{p-1}\} - \{\zeta_{i_0}\}$ é base temos $\beta = b_0 + ... + b_{p-1}\zeta^{p-1}$ de maneira única e com $b_{i_0} = 0$. Segue que $\alpha = n\beta = nb_0 + ... + nb_{p-1}\zeta^{p-1}$ donde $a_0 = nb_0, ..., a_{p-1} = nb_{p-1}$. □

LEMA 6.1.4. *Se α é um inteiro algébrico cujos conjugados possuem, todos, valor absoluto 1 (com respeito a alguma imersão em $\mathbb{C}$) então α é uma raiz da unidade.*

DEMONSTRAÇÃO. Seja $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ os conjugados de α. Por hipótese $|\alpha_i| = 1$, $\forall i$. Fixe $m \in \mathbb{N}$, $m \neq 0$ e seja $\beta_1 = \alpha_1^m$. Sejam também $f(X) = \text{Irr}(\beta, \mathbb{Q}) = X^k + a_1X^{k-1} + ... + a_k$; $a_i \in \mathbb{Z}$ e $\beta_2, ..., \beta_k$ os conjugados de β. Então $\beta_i = \alpha_j^m$ para algum j. De fato, denotando $L = \text{Spl}(f)$ o corpo de decomposição de f e G o grupo de Galois de L, sabemos que G permuta os α_i. Temos então a torre $\mathbb{Q} \subseteq \mathbb{Q}[\beta_1] \subseteq \mathbb{Q}[\alpha_1] \subseteq L$ com $\mathbb{Q} \subseteq L$ galoisiana. Segue que $\mathbb{Q}[\beta_1] \subseteq L$ e $\mathbb{Q}[\alpha_1] \subseteq L$ também são galoisianas. Portanto, $\beta_i = \sigma(\beta_1)$ para algum $\sigma \in G$. Ou seja, $\beta_i = \sigma(\beta_1) = \sigma(\alpha_1^m) = \sigma(\alpha_1)^m = \alpha_j^m$, para algum j como queríamos.

Agora, em particular, temos $|\beta_i| = |\alpha_j|^m = 1$ da hipótese. Vimos na observação 1.1.3 que $a_l = \pm S_l(\beta_1, ..., \beta_k)$ onde S_l denota o l-ésimo polinômio simétrico elementar. Portanto,

$$|a_l| = \left| \sum_{i_1 < ... < i_l} \beta_{i_1} ... \beta_{i_l} \right| \leq \sum_{i_1 < ... < i_l} |\beta_{i_1} ... \beta_{i_l}| = \sum_{i_1 < ... < i_l} 1 = \binom{k}{l} \leq k$$

e como $\mathbb{Q}[\alpha^m] \subseteq \mathbb{Q}[\alpha]$ temos que k divide $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$. Em suma, mostramos que para qualquer $m \in \mathbb{N}$, $m \neq 0$, o valor absoluto dos coeficientes do polinômio mínimo de α^m é limitado pelo grau de α sobre $\mathbb{Q}$. Portanto, só existe uma quantidade finita de polinômios mínimos que possuem uma potência de α como raiz e, em particular, só existe uma quantidade finita de potências de α. Segue que α tem ordem finita em $\mathbb{C}^\times$, isto é, α é raiz da unidade. □

PROPOSIÇÃO 6.1.5. *Seja u uma unidade de K. Então $u = \zeta^r v$ onde $v \in K$ é tal que $\bar{v} = v$.*[3]

DEMONSTRAÇÃO. Seja $\sigma_1 : K \hookrightarrow \mathbb{C}$ uma imersão e a utilize para identificar K com um subcorpo de $\mathbb{C}$. Defina $\alpha = u/\bar{u} \in \mathbb{Z}_K$ pois $\bar{u} \in U_K$. Se α' é um conjugado de α então

$$|\alpha'| = |\sigma(\alpha)| = \left| \frac{\sigma(u)}{\sigma(\bar{u})} \right| = \left| \frac{\sigma(u)}{\overline{\sigma(u)}} \right| = 1$$

onde σ é o automorfismo determinado por $\sigma(\alpha) = \alpha'$. Pelo lema anterior, $\alpha \in \mu_K$, ou seja, $u/\bar{u} = \pm\zeta^a$.

Suponha que $u/\bar{u} = -\zeta^a$ e escreva $u = a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2}$ então $u \equiv a_0 + ... + a_{p-2} \bmod(\pi)$ onde $\pi = 1 - \zeta$ como no capítulo anterior. Também, $\bar{u} \equiv a_0 + ... + a_{p-2} \bmod(\pi)$ donde $u \equiv \bar{u} \bmod(\pi)$. Por outro lado, como $u = -\zeta^a\bar{u}$ temos $u \equiv -\bar{u} \bmod(\pi)$. Segue que $\bar{u} \equiv -\bar{u} \bmod(\pi)$, ou seja, $2\bar{u} \equiv 0 \bmod(\pi)$. Como $2 \notin (\pi)$ e (π) é primo temos $\bar{u} \equiv 0 \bmod(\pi)$

[3]Um elemento como este é denominado real. Ele pertence ao corpo $\mathbb{Q}[\zeta + \zeta^{-1}] \subseteq K$ que é o subcorpo real maximal.

o que é absurdo pois $\bar{u} \in U_K$. Portanto, $u/\bar{u} = +\zeta^a$. Seja r tal que $2r \equiv a \bmod p$ e defina $v := \zeta^{-2}u$. Então $u = \zeta^r v$ e note que $\bar{v} = \zeta^r \bar{u} = \zeta^r \zeta^{-r} v = v$ como queríamos mostrar. □

Armados destes resultados voltamos ao teorema de Fermat. Tínhamos $\left(x + \zeta^i y\right) = (\alpha_i)^p$. Tome $i = 1$ e omita os índices. Então temos $x + \zeta y = u\alpha^p$ para $u \in U_K$. Identificando K com um subcorpo de $\mathbb{C}$ através de alguma imersão pré-fixada, podemos pela, proposição anterior, escrever $u = \zeta^r v$, com v satisfazendo $\bar{v} = v$. Pelo lema 6.1.2 existe $a \in \mathbb{Z}$ tal que $\alpha^p \equiv a \bmod p\mathbb{Z}[\zeta]$. Portanto,

$$x + \zeta y = \zeta^r v \alpha^p \equiv \zeta^r v a \bmod p\mathbb{Z}[\zeta]$$

$$x + \bar{\zeta} y = \zeta^{-r} v \bar{\alpha}^p \equiv \zeta^{-r} v a \bmod p\mathbb{Z}[\zeta].$$

Tomando o produto obtemos

$$\begin{aligned} (x + \zeta y)\,\zeta^{-r} v a \equiv \left(x + \zeta^{-1} y\right)\zeta^r v a \bmod p\mathbb{Z}[\zeta] \implies \\ \implies (x + \zeta y)\,\zeta^r \equiv \left(x + \zeta^{-1} y\right)\zeta^r \bmod p\mathbb{Z}[\zeta] \implies \\ \implies x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \bmod p\mathbb{Z}[\zeta]. \end{aligned} \tag{6.1.4}$$

Agora, se $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ são todos distintos e supondo $p \geq 5$, pelo lema 6.1.3, p divide x e y contrariando nossas hipóteses. Portanto, restam as seguintes possibilidades:

(1) $1 = \zeta^{2r}$: Então a equação (6.1.4) reduz-se a $\zeta y - \zeta^{2r-1} y \equiv 0 \bmod p\mathbb{Z}[\zeta]$ e o lema 6.1.3 implica que p divide y. Absurdo.
(2) $\zeta = \zeta^{2r-1}$: Então a equação (6.1.4) implica $x - \zeta^2 x \equiv 0 \bmod p\mathbb{Z}[\zeta]$ e, novamente, o lema 6.1.3 implica que p divide x. Absurdo.
(3) $1 = \zeta^{2r-1}$: Então $\zeta = \zeta^{2r}$ e 6.1.4 implica $(x - y) - (x - y)\zeta \equiv 0 \bmod p\mathbb{Z}[\zeta]$ e o lema 6.1.3 implica que p divide $x - y$.

Para terminarmos vamos mostrar que o caso (I) do teorema de Fermat é verdadeiro para $p = 3$ e concluir um absurdo do item (3) acima.

Se $p = 3$ note que os únicos cubos módulo 9 são $-1, 0, 1$ e, portanto, como $x^3, y^3, z^3 \neq 0 \bmod p$, por hipótese, temos $x^3 + y^3 \equiv -2, 0, 2 \bmod 9$ e $z^3 \equiv -1, 1 \bmod 9$ o que é absurdo.

Por fim, note que se $p \geq 5$ não podemos ter $x \equiv y \equiv -z \bmod p$, caso contrário, teríamos $z^p \equiv x^p + y^p \equiv -2z^p \bmod p$, ou seja, $p|z$ contrariando as hipóteses. Portanto, uma das congruências acima é falsa e reescrevendo a solução da equação de Fermat como $x^p + (-z)^p = (-y)^p$, se necessário, podemos supor $x \neq y \bmod p$, isto é, $p \nmid x - y$ de maneira que temos um absurdo no caso (3) acima. Isto conclui a demonstração do caso (I) do teorema Fermat para primos p tais que $p \nmid h_K$.

Na próxima seção nos concentraremos no chamado caso (II) do último teorema de Fermat, muito mais difícil e onde será necessário mais uma hipótese sobre p.

6.2. As unidades de $\mathbb{Q}[\zeta]$ e o caso (II) do teorema de Fermat

Agora vamos analisar a equação de Fermat no caso em que a suposta solução (x, y, z) é tal que, sem perda de generalidade, os números são dois-a-dois primos entre si e $p|xyz$. Neste caso, p divide apenas um dos números pois senão ele dividiria todos o que contraria a hipótese deles não terem fatores em comum. Reescrevendo a solução, se necessário, podemos supor que $p|z$. Este é o famoso caso (II) do teorema de Fermat e é bem mais difícil.

No caso (I) usamos o grupo de classes de ideais, ao fazermos a hipótese de que $p \nmid h_K$, para resgatarmos a idéia de Lamè. Esta idéia que funcionou tão bem, aqui, será ainda mais importante. No presente caso, como vamos ver, os fatores da decomposição da equação (6.1.1) não são mais primos entre si e então as unidades de K entram em jogo. Vamos definir um grupo de classes de unidades quocientando as unidades por um subgrupo de unidades "boas" e então fazer a hipótese de que p não divide o número de tais classes.

Seja então $p > 2$ um primo e, como antes, $K := \mathbb{Q}[\zeta]$ onde ζ é uma raíz p-ésima primitiva da unidade. O teorema da unidade nos diz que $U_K \cong \mu_K \oplus \mathbb{Z}^{s-1}$ onde $s = (p-1)/2$.[4]

Se $(x_1, ..., x_s) \in \mathbb{Z}^s$ é tal que $x_1 + ... + x_s = 0$, o inteiro ciclotômico

$$\pm\zeta^k (1 - \sigma_1(\zeta))^{x_1} ... (1 - \sigma_s(\zeta))^{x_s} \in U_K \tag{6.2.1}$$

onde $\sigma_1, ..., \sigma_s : K \hookrightarrow \mathbb{C}$ é um conjunto completo de imersões duas-a-duas não conjugadas. Isto segue do fato que se ζ' é um conjugado de ζ então $(1-\zeta')/(1-\zeta) \in U_K$, que foi visto na proposição 5.0.6. Assim,

$$\pm\zeta^k (1 - \sigma_1(\zeta))^{x_1} ... (1 - \sigma_s\zeta)^{x_s} = \pm\zeta^k \left(\frac{1-\sigma_1(\zeta)}{1-\zeta}\right)^{x_1} ... \left(\frac{1-\sigma_s(\zeta)}{1-\zeta}\right)^{x_s} \in U_K$$

pois $(1-\zeta)^{x_1+...+x_s} = (1-\zeta)^0 = 1$.

NOTAÇÃO 6.2.1. Seja V_K o subgrupo de U_K gerado por unidades do tipo (6.2.1) e seja $k_K := (U_K : V_K)$ o número de classes de unidades de K que é finito pois V_K tem o mesmo posto que U_K e $\mathbb{Z}$ é domínio.

A partir de agora vamos supor também que $p \nmid k_K$. Ou seja, temos $p > 2$ e $p \nmid h_K k_K$. Primos desta forma são os que Kummer denominou de primos regulares. Posteriormente, ele mesmo concluiu, que sempre $k_K | h_K$ de forma que podemos definir a regularidade de um primo apenas em termos da divisibilidade de h_K por p.

DEFINIÇÃO 6.2.2. Um primo p é dito regular quando $p \nmid h_K$ onde h_K é o número de classe de ideais do corpo $\mathbb{Q}[\zeta]$.

[4] Lembremos que neste caso $r = 0$ e $[K : \mathbb{Q}] = p - 1$.

OBSERVAÇÃO 6.2.3. Se $v_1, ..., v_k$ é um conjunto de representantes para U_K/V_K podemos supor pela proposição 6.1.5 que $v_1, ..., v_k$ são reais, isto é, $v_i = \bar{v}_i$ (conjugado complexo em alguma imersão em $\mathbb{C}$ pré-fixada).

Vamos a demonstração reproduzindo aqui a equação (6.1.1):

$$z^p = \prod_{i=0}^{p-1} \left(x + y\zeta^i\right).$$

Olhando a prova do lema 6.1.1 vemos que ele não mais se aplica e, de fato, olhando a equação (6.1.2) observamos que o único possível fator comum entre $x + y\zeta^i$ e $x + y\zeta^j$ é $\pi = 1 - \zeta$. Como no caso (II) do teorema de Fermat temos $p|z$ deduzimos que $\pi|z$ e, portanto, necessariamente, $\pi|(x + y\zeta^i)$, $\forall i$. Mais que isso, como x e y são primos entre si da mesma equação temos que $(x + y\zeta^i)\pi^{-1}$ são dois-a-dois primos entre si.

Da mesma forma que no caso (I) teremos

$$\frac{x + y\zeta^i}{\pi} = u_i \alpha_i^p$$

com $u_i \in U_K$ e α_i dois-a-dois primos entre si. Em particular, π divide, no máximo, um α_i e, de fato, ele divide α_0 pois como $p|z$ temos $0 \equiv z^p \equiv x^p + y^p \equiv x + y \bmod p$ pelo pequeno teorema de Fermat. Assim,

$$p|x + y \implies \pi^{p-1}|x + y \implies \pi^{p-2}|u_0\alpha_0^p.$$

Escreva $\alpha_0 = \pi^m w$ onde $\pi \nmid w$, $m \geq 1$. Entre as p equações acima temos em particular[5]

$$x + y\zeta^{-1} = \pi u_{-1}\alpha_{-1}^p$$

$$x + y = \pi u_0 \pi^{mp} w^p$$

$$x + y\zeta = \pi u_1 \alpha_1^p.$$

Subtraindo a 2º equação da 3º e a 1º da 2º obtemos

$$(\zeta - 1)\, y = \pi y = \pi \left(u_1\alpha_1^p - u_0\pi^{mp}w^p\right)$$

$$\left(1 - \zeta^{-1}\right) y = \zeta^{-1}\left(\zeta - 1\right) y = \zeta^{-1}\pi y = \pi\left(u_0\pi^{mp}w^p - u_{-1}\alpha_{-1}^p\right).$$

Ou seja,

$$\left(u_1\alpha_1^p - u_0\pi^{mp}w^p\right) = \zeta\left(u_0\pi^{mp}w^p - u_{-1}\alpha_{-1}^p\right)$$

que equivale a

$$0 = u_1\alpha_1^p - (\zeta + 1)\, u_0\pi^{mp}w^p + u_{-1}\alpha_{-1}^p.$$

Como $\zeta + 1 = (\zeta^2 - 1)/(\zeta - 1) \in U_K$, podemos colocar a equação acima na forma:

$$U_0\pi^{mp}w^p = \alpha_1^p + U'_{-1}\alpha_{-1}^p;\ U_0, U'_{-1} \in U_K.$$

[5]Lembremos que os índices i estão definidos módulo p de forma que podemos substituir o índice $i = p - 1$ por $i = -1$.

Agora, olhando esta equação módulo $(p) = (\pi)^{p-1}$ temos pelo lema 6.1.2 a equação

$$0 \equiv a + U'_{-1}b \bmod(p);\ a, b \in \mathbb{Z}.$$

Segue que $U'_{-1} \equiv c \bmod(p)$; $c \in \mathbb{Z}$ pois $b \neq 0 \bmod(p)$, caso contrário, $p|\alpha^p_{-1}$, isto é, $p|\alpha_{-1}$ que vimos não acontecer.

Agora usamos o famoso lema de Kummer demonstrado no final deste capítulo. Ele é o ponto chave do caso (II) e o cerne da dificuldade. Ele garante que sob a condição $p \nmid k_K$ então $U'_{-1} \equiv c \bmod(p)$ com $c \in \mathbb{Z}$ implica $U'_{-1} = U^p_{-1}$ para $U_{-1} \in U_K$. Assim temos

$$U_0\pi^{mp}w^p = \alpha_1^p + (U_{-1}\alpha_{-1})^p\,;\, U_0, U_{-1} \in U_K.$$

Note que esta é uma equação parecida com a equação de Fermat $z^p = x^p + y^p$, e o mesmo argumento com alguma modificações nos dá uma terceira equação. De fato, suponha que temos uma equação do tipo

$$x^p + y^p = u\pi^{mp}w^p;\ u \in U_K,\ x, y, w \in \mathbb{Z}_K \tag{6.2.2}$$

com $m \geq 1$, x, y, w dois-a-dois primos entre si e $\pi \nmid xyw$. Como antes fatoramos o lado esquerdo como $x^p + y^p = (x + y\zeta^0)...(x + y\zeta^{p-1})$. Segue que π divide um dos fatores e, da mesma forma que antes, que π divide, na verdade, todos os fatores. Também, tem-se que os quocientes $(x + y\zeta^i)\pi^{-1}$ são todos dois-a-dois primos entre si.

Como $x+y$ não é mais, necessariamente, um inteiro (racional) não podemos argumentar como antes para deduzir que $\pi^2|x+y$. Mas ainda é verdade que π^2 divide um (e, portanto, somente um) dos fatores de $x^p + y^p$. Para vermos isso precisamos do seguinte lema:

LEMA 6.2.4. *Seja* $\alpha = a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2} \in \mathbb{Z}_K$ *e* $m > 0$. *Então existem* $c_0, c_1, ..., c_{m-1} \in \mathbb{Z}$ *tal que*

$$\alpha \equiv c_0 + c_1\,(\zeta - 1) + ... + c_{m-1}\,(\zeta - 1)^{m-1} \bmod (\zeta - 1)^m\,.$$

DEMONSTRAÇÃO. Procedemos por indução: para $m = 1$ temos

$$\alpha = a_0 + ... + a_{p-2}\zeta^{p-2} \equiv a_0 + a_1 + ... + a_{p-2} \bmod (\zeta - 1)$$

e basta tomar $c_0 = a_0 + ... + a_{p-2}$.

Supondo o resultado válido para $m - 1$ provemos para m. Temos

$$\alpha \equiv c_0 + c_1\,(\zeta - 1) + ... + c_{m-2}\,(\zeta - 1)^{m-2} \bmod (\zeta - 1)^{m-1}\,.$$

Então,

$$\beta := \alpha - \left(c_0 + ... + c_{m-2}\,(\zeta - 1)^{m-2}\right) \equiv 0 \bmod (\zeta - 1)^{m-1}$$

donde $(\zeta - 1)^{m-1}\,|\beta$, isto é, $\beta/(\zeta - 1)^{m-1} \in \mathbb{Z}_K$ e do caso $m = 1$ temos

$$\beta/(\zeta - 1)^{m-1} \equiv c_{m-1} \bmod(\zeta - 1)$$

que equivale a

$$\beta \equiv c_{m-1}(\zeta - 1)^{m-1} \bmod(\zeta - 1)^m.$$

Assim,

$$\alpha \equiv c_0 + ... + c_{m-2}(\zeta - 1)^{m-2} + c_{m-1}(\zeta - 1)^{m-1} \bmod (\zeta - 1)^m .$$

□

Voltando à demonstração do caso (II), queremos mostrar que π^2 divide um dos fatores de $x^p + y^p$. Pelo lema acima temos existem $a_0, a_1, b_0, b_1 \in \mathbb{Z}$ tais que

$$x \equiv a_0 + a_1\pi \bmod \pi^2$$

$$y \equiv b_0 + b_1\pi \bmod \pi^2.$$

Logo,

$$x + y\zeta^i \equiv a_0 + a_1\pi + (1+\pi)^i (b_0 + b_1\pi) = a_0 + b_0 + (a_1 + b_1 + ib_0)\pi \bmod \pi^2$$

pois os demais termos de $(1+\pi)^i$ envolvem π^2. Note que $0 \equiv x + y\zeta^i \equiv a_0 + b_0 \bmod \pi$ donde como $a_0 + b_0 \in (\pi) \cap \mathbb{Z} = (p)$ temos $a_0 + b_0 \equiv 0 \bmod p$. Assim, $\pi^2 | x + y\zeta^i$ se e somente se $a_1 + b_1 + ib_0 \equiv 0 \bmod \pi$ o que ocorre se e somente se $a_1 + b_1 + ib_0 \equiv 0 \bmod p$ pela mesma razão. Tal equação possui solução (para i) desde que $b_0 \neq 0 \bmod p$ o que é verdade caso contrário $\pi | x$ contrariando o assumido. Isto conclui que π^2 divide um dos fatores como queríamos.

Olhando a equação (6.2.2), pelo deduzido acima, devemos ter $m > 1$. Escreva $m = M+1$ onde $M > 0$. Como podemos substituir y por $y\zeta^i$ sem alterar a forma desta equação podemos assumir que $x + y$ é o fator de $x^p + y^p$ que é divisível por π^2. Resumindo, os mp fatores π de $x^p + y^p$ consistem de um único fator para cada termo $x + y\zeta^i$, $1 \leq i \leq p-1$ e $1 - (m-1)p = 1 + Mp$ fatores no termo $x + y$. Assim, como antes deduzimos as equações:

$$x + y\zeta^{-1} = \pi u_{-1}\alpha_{-1}^p$$

$$x + y = \pi u_0 \pi^{Mp} W^p$$

$$x + y\zeta = \pi u_1 \alpha_1^p$$

onde $u_{-1}, u_0, u_1 \in U_K$, $\alpha_{-1}, \alpha_1, W \in \mathbb{Z}_K$ com $\pi \nmid \alpha_{-1}\alpha_1 W$. Os mesmos passos que antes nos dá uma equação da forma

$$X^p + Y^p = U\pi^{Mp} W^p;\ X, Y, W \in \mathbb{Z}_K, U \in U_K$$

onde X, Y, W são dois-a-dois primos entre si, $\pi \nmid XYW$ e $M = m - 1$. Repetindo o processo sucessivamente obtemos uma equação com $M = 1$ o que vimos ser impossível. Isto completa a prova do caso (II) do teorema de Fermat salvo pela demonstração do lema de Kummer o qual agora iremos demonstrar.

6.3. O lema de Kummer

Para terminar precisamos mostrar o seguinte lema devido a Kummer:

LEMA 6.3.1. *(Kummer) Nas condições deste capítulo, (isto é, p primo regular, $K = \mathbb{Q}[\zeta]$ para ζ uma raíz p-ésima primitiva da unidade) a condição necessária $u \equiv a \bmod p$; $a \in \mathbb{Z}$ para que $u \in U_K$ seja uma p-ésima potência é também suficiente.*

DEMONSTRAÇÃO. A prova de que a condição é necessária é o lema 6.1.2. A suficiência é naturalmente mais difícil e sua demonstração é elucidativa com respeito a definição do grupo V_K e da regularidade de p.

Primeiro nos restringimos ao caso $u \in V_K$. Nesta condições escrevendo

$$u = \pm\zeta^l (1-\sigma_1(\zeta))^{x_1} ... (1-\sigma_s(\zeta))^{x_s}$$

afirmamos que $u = v^p$, $v \in U_K$ se e somente se $p|x_i \, \forall i$. De fato, se $p|x_i \, \forall i$ escreva

$$u = \pm\zeta^l (1-\sigma_1(\zeta))^{py_1} ... (1-\sigma_s(\zeta))^{py_s} \, ; \, 1 \leq l \leq p.$$

Do lema 6.1.2 temos $((1-\sigma_i(\zeta))^{y_i})^p \equiv c_i \bmod(p)$ com $c_i \in \mathbb{Z}$. Como, por hipótese, $u \equiv c \bmod(p)$ devemos ter $\zeta^l \equiv c' \bmod(p)$ para $c' \in \mathbb{Z}$. Agora, $\zeta = 1-(1-\zeta)$ donde

$$\zeta^l = 1 - \binom{l}{1}(1-\zeta) + \binom{l}{2}(1-\zeta)^2 - ... + (1-\zeta)^l$$

e vemos que $\zeta^l \equiv c' \bmod(p)$ com $c' \in \mathbb{Z}$ se e somente se $l = p$ pois módulo p temos $(1-\zeta)^i \neq (1-\zeta)^j$ para $i < j \leq p$. Assim,

$$u = \zeta^p (1-\sigma_1(\zeta))^{py_1} ... (1-\sigma_s(\zeta))^{py_s} = [(1-\sigma_1(\zeta))^{y_1} ... (1-\sigma_s(\zeta))^{y_s}]^p .$$

Reciprocamente, se $u = v^p$ devemos ter $v \in U_K$ caso contrário teríamos um elemento de $U_K - V_K$ de ordem p e do teorema de Lagrange para a ordem de um subgrupo de um grupo finito devemos ter $p|k_K$ contrariando a hipótese de p ser regular. Escreva então

$$v = \pm\zeta^m (1-\sigma_1(\zeta))^{y_1} ... (1-\sigma_s(\zeta))^{y_s} .$$

Então,

$$u = \pm\zeta^{mp} (1-\sigma_1(\zeta))^{py_1} ... (1-\sigma_s(\zeta))^{py_s} = \pm (1-\sigma_1(\zeta))^{py_1} ... (1-\sigma_s(\zeta))^{py_s}$$

ou seja,

$$\zeta^l (1-\sigma_1(\zeta))^{x_1-py_1} ... (1-\sigma_s(\zeta))^{x_s-py_s} = \pm 1.$$

Como antes, devemos ter $\zeta^l \equiv c' \bmod(p)$ com $c' \in \mathbb{Z}$ donde $l = p$ e temos

$$(1-\sigma_1(\zeta))^{x_1-py_1} ... (1-\sigma_s(\zeta))^{x_s-py_s} = \pm 1.$$

Segue daí que $x_i - y_i p = 0 \, \forall i$ donde $p|x_i \, \forall i$ concluindo a afirmação.

Suponha agora o caso geral onde $u \in U_K$ e $u \equiv c \bmod(p)$, $c \in \mathbb{Z}$. Então $u^{k_K} \equiv c^{k_K} \bmod(p)$. Como $u^{k_K} \in V_K$ temos

$$u^{k_K} = \pm\zeta^l (1-\sigma_1(\zeta))^{x_1} ... (1-\sigma_s(\zeta))^{x_s} .$$

Agora, mostra-se em [**Edw77**, Seção 6.17, pg.238], utilizando a transformada de Fourier discreta, que, sendo p regular, como $u^{k_K} \in U_K$, tem-se que $p|x_i \, \forall i$. Assim, $u^{k_K} = v^p$ pelo caso anterior. Como $p \nmid k_K$ existem inteiros a, b tais que $ak_K + bp = 1$ donde

$$u = u^{ak_K+bp} = v^{ap}u^{bp} = \left(v^a u^b\right)^p$$

e temos demonstrado o lema de Kummer. □

6.4. Caracterização dos primos regulares

Para encerrar é conveniente achar uma caracterização alternativa para os primos regulares visto que partir pela definição é algo intratavel. Quanto a isso, o próprio Kummer achou a resposta:

TEOREMA. *Um primo $p \in \mathbb{N}$ é regular se e somente se p não divide nenhum dos numeradores dos números de Bernoulli $B_2, B_3, ..., B_{p-3}$.*

Os números de Bernoulli podem ser definidos de duas maneiras:

- Como os coeficientes da expansão em série de potências da funcção $x/(e^x - 1)$. Isto é
$$\frac{x}{e^x - 1} = \sum B_n \frac{x^n}{n!}.$$
- Como o valor assumido pelos respectivos polinômios de Bernoulli (também denotados por $B_n(X)$) no ponto zero. Por sua vez o $n+1$-ésimo polinômio de Bernoulli é o único polinômio de grau $n+1$ que nos dá a soma das primeiras n-ésimas potências. Por exemplo,
$$B_2(X) = \frac{X(X+1)}{2} = \frac{X^2}{2} + \frac{X}{2}$$

A demonstração do teorema acima sai do escopo de nosso trabalho pois envolve um pedaço da teoria analítica dos números. Mais precisamente, a teoria analítica multiplicativa que trabalha com o grupo da funções multiplicativas (caracteres) e suas respectivas séries de Dirichlet. A demontração segue mais ou menos a linha da demonstração dada por Dirichlet para a densidade de primos em uma prograssão aritmética e depende fundamentalmente da famosa fórmula produto de Euler:

$$\sum_n \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}} \ \ (s > 1)$$

onde a soma varia sobre todos os naturais e o produto sobre todos os primos positivos. Aqui deixamos nos contentamos em deixar uma referência completa para demonstração: [**Edw77**, Cap.6, pg.181].

APÊNDICE A

Módulos Sobre Domínios de Dedekind

Neste apêndice vamos obter uma generalização do teorema dos fatores invariantes para módulos sobre domínios de Dedekind. Aqui A denotará um domínio de integridade e K seu corpo de frações. Nosso primeiro passo será mostrar que todo A-módulo M livre de torção pode ser imerso em um K-espaço vetorial.

A.1. O espaço vetorial envolvente

Em $M \times A\backslash\{0\}$ defina a relação $(m,\alpha) \sim (n,\beta) \iff \beta m = \alpha n$. É claro que esta relação é reflexiva e simétrica. Afirmamos que ela é transitiva. De fato, se $(m,\alpha) \sim (n,\beta)$ e $(n,\beta) \sim (p,\gamma)$ então $\beta m = \alpha n$ e $\beta p = \gamma n$ donde $\alpha\beta p = \gamma\beta m \implies \alpha p = \gamma m$ pois M é livre de torção. Assim, temos uma relação de equivalência. Denotaremos $KM := (M \times A\backslash\{0\}) \,/\, \sim$ e um elemento de KM por $[m,\alpha]$. Observe que fazemos de KM um grupo abeliano se definirmos $[m,\alpha] + [n,\beta] := [\beta m + \alpha n, \alpha\beta]$. Por fim, defina agora uma ação de K em KM fazendo $(s/t,[m,\alpha]) \longmapsto [sm,t\alpha]$ e teremos um K-espaço vetorial. Afirmamos que a aplicação $M \xrightarrow{i} KM$ dada por $i(m) := [m,1]$ é um A-monomorfismo. Ora, é claro que ela é homomorfismo. Agora se $i(m) = [0,1]$ então $[m,1] = [0,1]$ donde $m = 0$.

Se M é finitamente gerado, digamos por $m_1,...,m_k$ então $[m_1,1],...,[m_k,1]$ gera KM. De fato, dado $[m,\alpha] \in KM$ temos $[m,\alpha] = [\sum \lambda_i m_i, \alpha] = \sum \lambda_i \alpha^{-1} [m_i,1]$. Em particular, segue que se M é livre então uma base de M induz por i uma base em KM. Ou seja temos as implicações

$$M = \sum Am_i \implies KM = \sum Km_i$$
$$M = \oplus Am_i \implies KM = \oplus Km_i.$$

Podemos então generalizar a definição de posto de um módulo de maneira que também se aplique à módulos livres de torção.

DEFINIÇÃO A.1.1. O posto de um A-módulo livre de torção M, denotado por $(M:A)$ é o número (possivelmente infinito) $\dim_K KM$, isto é, $(M:A) = (KM:K)$.

Vejamos um resultado útil que usaremos freqüentemente do decorrer desta seção.

PROPOSIÇÃO A.1.2. *Seja A um domínio de integridade, K seu corpo de frações e M um A-módulo livre de torção. Então $KM \cong K \otimes_A M$ como espaços vetoriais.*

DEMONSTRAÇÃO. Defina a aplicação $\psi' : K \times M \longrightarrow KM$ dada por $(\alpha/\beta, m) \longmapsto [\alpha m, \beta]$ que é A-balanceada. De fato,

$$\psi'\left(\frac{\alpha}{\beta}+\frac{\gamma}{\delta}, m\right) = \psi'\left(\frac{\alpha\delta+\beta\gamma}{\beta\delta}, m\right) = [(\alpha\delta+\beta\gamma)m, \beta\delta] =$$

$$= [\alpha m, \beta] + [\gamma m, \delta] = \psi'\left(\frac{\alpha}{\beta}, m\right) + \psi'\left(\frac{\gamma}{\delta}, m\right)$$

e é evidente que

$$\psi'(\alpha/\beta, m+n) = \psi'(\alpha/\beta, m) + \psi'(\alpha/\beta, n)$$

e

$$\psi'((\alpha/\beta)\, r, m) = \psi'(\alpha/\beta, rm)\,;\, \forall a \in A.$$

Pela propriedade universal do produto tensorial temos o K-homomorfismo $\psi : K \otimes_A M \longrightarrow KM$ tal que $\psi(\alpha/\beta \otimes m) = [\alpha m, \beta]$. É claro que ψ é sobrejetora pois dado $[m, \beta] \in KM$ temos $\psi(1/\beta \otimes m) = [m, \beta]$. Resta-nos mostrar que ψ é injetora. A aplicação $\phi : KM \longrightarrow K \otimes_A M$ dada por $[m, \beta] \longmapsto 1/\beta \otimes m$ está bem definida pois se $[m, \beta] = [n, \delta]$ então $\beta n = \delta m$ e $1/\delta \otimes n = (1/\delta)(1/\beta) \otimes \beta n = (1/\delta)(1/\beta) \otimes \delta m = 1/\beta \otimes m$. Agora, $\phi(\psi(\alpha/\beta \otimes m)) = \phi([\alpha m, \beta]) = 1/\beta \otimes \alpha m = \alpha/\beta \otimes m$ e segue que ψ é injetora como queríamos. □

Combinando o que vimos temos que $M \hookrightarrow K \otimes_A M$ através do A-monomorfismo $m \longmapsto 1 \otimes m$ e que $(M : A) = (K \otimes_A M : K)$.

Se $\theta : M \longrightarrow N$ é um A-isomorfismo, sabemos que $1 \otimes \theta : K \otimes_A M \longrightarrow K \otimes_A N$ é K-isomorfismo. Em particular, $KM \cong KN$ através da aplicação $[m, \beta] \longmapsto [\theta(m), \beta]$.

A partir de agora A é um domínio de Dedekind e tendo em mente a imersão $M \hookrightarrow KM$ denotaremos o elemento $[\alpha m, \beta]$ por $(\alpha/\beta)\, m$ ou apenas ξm com $\xi \in K$. Assim, se $\theta' : KM \longrightarrow KN$ é um K-homomorfismo induzido pelo A-homomorfismo $\theta : M \longrightarrow N$ então

$$\theta'\left(\frac{\alpha}{\beta}m\right) = \theta'([\alpha m, \beta]) = \theta'\left(\frac{\alpha}{\beta}[m, 1]\right) = \frac{\alpha}{\beta}\theta'([m, 1]) = \frac{\alpha}{\beta}[\theta(m), 1] = [\alpha\theta(m), \beta] = \frac{\alpha}{\beta}\theta(m).$$

Em particular se $m \in M$ e $\xi \in K$ são tais que $\xi m \in M$ então

$$\theta(\xi m) = \theta'(\xi m) = \xi\theta(m). \tag{A.1.1}$$

A.2. Classificação dos módulo sobre um domínio de Dedekind

Aqui vamos obter resultados análogos aos de classificação de módulos sobre domínios principais. Antes, alguns lemas.

LEMA A.2.1. *Dois ideais fracionários M, N de A são A-isomorfos se e somente se eles estão na mesma classe de ideais.*

DEMONSTRAÇÃO. Suponha M e N na mesma classe então existe $\alpha \in K$ tal que $M = (\alpha)N = \alpha N$ donde $\theta : N \longrightarrow M$ dado por $n \longmapsto \alpha n$ é A-isomorfismo. Reciprocamente,

se $M \overset{\theta}{\cong} N$ estenda θ para o K-isomorfismo θ' como discutido acima. Supondo $M \neq (0)$, existe $m \in M,\ m \neq 0$. Como $1 = m^{-1}m \in m^{-1}M \cong M$ podemos supor sem perda de generalidade que $1 \in M$. Assim, dado $\alpha \in M \subseteq K$ temos pela equação (A.1.1), $\theta(\alpha) = \theta(\alpha 1) = \alpha\theta(1)$ donde $N = \theta(1)M$ e segue o desejado. □

LEMA A.2.2. *Todo A-módulo M, finitamente gerado, livre de torção e de posto 1 é A-isomorfo a um ideal fracionário de A. Mais que isso, existe um ideal fracionário $\mathfrak{a}$ de A tal que $M = \mathfrak{a}m$ onde $m \in M$ é uma base de KM.*

DEMONSTRAÇÃO. Por hipótese, $KM = Km$ onde podemos tomar $m \in M \setminus \{0\}$. Seja $\mathfrak{a} = \{\xi \in K : \xi m \in M\}$. É evidente que $\mathfrak{a}$ é um A-submódulo de K. O A-homomorfismo $\theta : \mathfrak{a} \longrightarrow M$ dado por $\theta(\xi) = \xi m$ é, uma vez que M é livre de torção, injetor. Como $M \hookrightarrow KM = Km$, θ é sobrejetora e, portanto, um isomorfismo. Como M é finitamente gerado, $\mathfrak{a}$ também o é, donde $\mathfrak{a}$ é ideal fracionário de A e segue o desejado. □

LEMA A.2.3. *Seja M um A-módulo finitamente gerado e livre de torção. Se $\zeta \in K$ é tal que $\zeta M \subseteq M$ então $\zeta \in A$.*

DEMONSTRAÇÃO. Supondo $M \neq (0)$ tome $m \in M,\ m \neq 0$ e seja $\mathfrak{a} = \{\xi \in K : \xi m \in M\}$ que, como vimos, é um ideal fracionário de A tal que $\mathfrak{a} \supseteq A$. Por hipótese $\zeta \in \mathfrak{a}$ donde $\mathfrak{a} \supseteq A[\zeta]$, pois $\mathfrak{a}$ é uma A-álgebra que contém A e o gerador ζ. Como $\mathfrak{a}$ é finitamente gerado e A é Noetheriano segue que $A[\zeta]$ é finitamente gerado. Por fim, como A é integralmente fechado segue que $\zeta \in A$. □

OBSERVAÇÃO A.2.4. Se $\mathfrak{a}$ é um ideal fracionário de A, não nulo, então $\mathfrak{a}$ tem posto 1 pois como K é A-módulo plano temos que $0 \longrightarrow \mathfrak{a} \longrightarrow K$ implica $0 \longrightarrow K\mathfrak{a} \longrightarrow KK = K$ e segue que $K\mathfrak{a}$ é K-subespaço vetorial, não nulo, de K donde $(K\mathfrak{a} : K) = 1$. Em geral, se $\mathfrak{a}_1, ..., \mathfrak{a}_n$ são ideais de A então $\oplus_{i=1}^n \mathfrak{a}_i$ é um A-módulo, livre de torção, finitamente gerado. Agora,

$$(\oplus_{i=1}^n \mathfrak{a}_i : A) = (K \otimes (\oplus_{i=1}^n \mathfrak{a}_i) : K) = (\oplus_{i=1}^n (K \otimes \mathfrak{a}_i) : K) = n.$$

Em seguida demonstraremos a recíproca deste resultado. Isto é, todo A-módulo livre de torção, finitamente gerado, de posto n, é isomorfo a soma direta externa de n ideais de A.

LEMA A.2.5. *Seja $\mathfrak{a}$ um ideal fracionário de A então $\mathfrak{a}$ é um A-módulo projetivo.*

DEMONSTRAÇÃO. Mostraremos que se $M \xrightarrow{\psi} \mathfrak{a} \longrightarrow 0$ é exata então $N := \ker\psi$ é somando direto de M o que, por resultados conhecidos, é equivalente ao desejado. Como $\mathfrak{a}\mathfrak{a}^{-1} = A$ existem elementos $\alpha_1, ..., \alpha_n \in \mathfrak{a}^{-1}$ e $\beta_1, ..., \beta_n \in \mathfrak{a}$ tais que $\sum \alpha_i\beta_i = 1$. Escolha elementos $m_1, ..., m_n \in M$ tais que $\psi(m_i) = \beta_i$. Seja $\gamma \in \mathfrak{a},\ \gamma \neq 0$ fixo porém arbitrário. Então $\gamma\alpha_i \in A,\ \forall i$ e $z := \sum(\gamma\alpha_i)m_i \in M$. Agora, $\psi(z) = \gamma\sum\alpha_i\psi(m_i) = \gamma$. Agora seja $T := Kz \cap M$. Vamos mostrar que $M = T \oplus N$. Em primeiro lugar, $T \cap N = (0)$ pois se $\xi z \in N$ onde $\xi \in K$ então pela equação (A.1.1) temos $0 = \psi(\xi z) = \xi\psi(z) = \xi\gamma \implies \xi = 0$.

Agora, dado $m \in M$ arbitrário, seja $\xi = \psi(m)$ então $\xi\alpha_i \in A$, $\forall i$ e $w := \sum (\xi\alpha_i)\, m_i \in M$. Mas $w = \xi\gamma^{-1}z \in Kz$ donde $w \in Kz \cap M = T$. Agora como $\psi(w) = \xi\gamma^{-1}\psi(z) = \xi$ temos que $m - w \in \ker\psi = N$ e $m = w + (m - w) \in T + N$. Logo $M = T \oplus N$ como queríamos. □

THEOREM A.2.6. *Seja A um domínio de Dedekind. Todo A-módulo finitamente gerado, livre de torção, de posto n é isomorfo a soma direta externa de n ideais fracionários de A.*

DEMONSTRAÇÃO. Procedemos por indução. No lema A.2.2 provamos para $n = 1$. Seja $n \geq 2$ e suponha o teorema válido para $n - 1$. Seja $m \in M,\ m \neq 0$ e $N := Km \cap M$. Como M e N são finitamente gerados temos que M/N também é. Afirmamos que M/N é livre de torção. Ora se $\alpha \in A\backslash\{0\}$ e $n \in M$ são tais que $\alpha n \in Km \cap M = N$ então existe $\xi \in K$ tal que $\alpha n = \xi m \implies n = \alpha^{-1}\xi m \in Km \implies n \in N$. Sendo assim, se $\alpha\overline{n} = 0$ em M/N então $\alpha n \in N$ e do argumento acima $n \in N$, isto é, $\overline{n} = 0$ em M/N como afirmado.

Nossa próxima afirmação é que M/N tem posto $n - 1$. De fato, da seqüência exata $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ e do fato que K é A-módulo plano segue que $0 \longrightarrow KN \longrightarrow KM \longrightarrow K(M/N) \longrightarrow 0$ é exata donde KN é subespaço vetorial de KM e $K(M/N) \cong KM/KN$. Agora, pelo que foi discutido sabemos que existe uma base de KM onde m figura. Da definição de N e por independência linear é fácil ver que qualquer outro elemento desta base não pertence a N. Sendo assim, tais elementos formam uma base para KM/KN. Disto segue que M/N tem posto $n - 1$ como afirmado e, em particular, que N tem posto 1.

Da hipótese de indução existem ideais $\mathfrak{a}_1, ..., \mathfrak{a}_{n-1}$ de A tais que $M/N \cong \mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_{n-1}$. Pelo lema A.2.5, cada parcela desta soma direta externa é um módulo projetivo e, portanto, M/N o é. Assim, $M \cong (M/N) \oplus N$ e N é livre de torção. Pelo lema A.2.2, $N \cong \mathfrak{a}_n$ um ideal fracionário de A. Concluindo, temos $M \cong \mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_{n-1} \oplus \mathfrak{a}_n$ como queríamos. □

Antes de continuarmos justifiquemos uma redução nas hipóteses sobre os ideais de A. Se $\mathfrak{a}$ é ideal fracionário de A sabemos que existe $\xi \in K$ tal que $\xi\mathfrak{a} \supseteq A$ (tome $\xi = m^{-1}$ onde m é um dos geradores de $\mathfrak{a}$). Note que $\mathfrak{a} \cong \xi\mathfrak{a}$ e, portanto, se $M \overset{\psi}{\cong} \mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_n$ então $M \cong \xi_1\mathfrak{a}_1 \oplus ... \oplus \xi_n\mathfrak{a}_n$ com $\xi_i\mathfrak{a}_i \supseteq A$. Assumiremos, portanto, a partir de agora que cada $\mathfrak{a}_i \supseteq A$.

Sejam $1_i := \iota_i(1) \in \mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_n$ onde $\iota_i : \mathfrak{a}_i \longrightarrow \mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_n$ é a inclusão canônica. Sejam também $m_i := \psi^{-1}(1_i)$. Pela equação (A.1.1) temos $M = \psi^{-1}(\mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_n) = \psi^{-1}(\oplus\mathfrak{a}_i 1_i) = \oplus\psi^{-1}(\mathfrak{a}_i 1_i) = \oplus\mathfrak{a}_i\psi^{-1}(1_i) = \oplus\mathfrak{a}_i m_i$. Ou seja, $m_1, ..., m_n$ formam uma "base" para M no sentido que todo elemento de M se escreve de maneira única como $\sum \lambda_i m_i$, $\lambda_i \in \mathfrak{a}_i$.

LEMA A.2.7. *Sejam $\mathfrak{a}_1, ..., \mathfrak{a}_n$ ideais fracionários de A. Então $\oplus\mathfrak{a}_i \cong A^{n-1} \oplus \mathfrak{a}_1...\mathfrak{a}_n$.*

DEMONSTRAÇÃO. Procedemos por indução. Mostremos para $n = 2$. Afirmamos que existem $\alpha, \beta \in K$ tais que $\alpha\mathfrak{a}_1 + \beta\mathfrak{a}_2 = A$. De fato, tome $\beta, \gamma \in K$ tais que $\beta\mathfrak{a}_2$ e $\gamma\mathfrak{a}_1^{-1}$ sejam

ideais inteiros de A. Pelo corolário 2.4.18 existe um ideal $\mathfrak{b}$ tal que $\mathfrak{b}\gamma\mathfrak{a}_1^{-1} = (\delta)$ e $\mathfrak{b}+\beta\mathfrak{a}_2 = A$ e como $\mathfrak{b} = \gamma\delta\mathfrak{a}_1$ tomando $\alpha = \gamma\delta$ segue o afirmado. Assim, substituindo os ideais por ideais isomorfos podemos supor que $\mathfrak{a}_1, \mathfrak{a}_2$ são inteiros e $\mathfrak{a}_1+\mathfrak{a}_2 = A$. Escolha $\alpha_1 \in \mathfrak{a}_1, \alpha_2 \in \mathfrak{a}_2$ tais que $\alpha_1 - \alpha_2 = 1$ e seja $\psi : \mathfrak{a}_1 \oplus \mathfrak{a}_2 \longrightarrow A \oplus \mathfrak{a}_1\mathfrak{a}_2$ dada por $\psi(\beta_1, \beta_2) = (\beta_1 + \beta_2, \alpha_1\beta_2 + \alpha_2\beta_1)$ que é um A-homomorfismo facilmente visto ser injetor. Quanto a sobrejetividade, dado $\alpha \in A$ e $\gamma \in \mathfrak{a}_1\mathfrak{a}_2$. basta tomar $\beta_1 := \alpha_1\alpha - \gamma$ e $\beta_2 = \gamma - \alpha_2\alpha$.

Supondo o resultado válido para $n-1$ provemos para n. Ora,

$$\mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_{n-1} \oplus \mathfrak{a}_n \cong A^{n-2} \oplus \mathfrak{a}_1...\mathfrak{a}_{n-1} \oplus \mathfrak{a}_n \cong A^{n-2} \oplus A \oplus (\mathfrak{a}_1...\mathfrak{a}_{n-1})\,\mathfrak{a}_n = A^{n-1} \oplus \mathfrak{a}_1...\mathfrak{a}_n$$

como queríamos. □

THEOREM A.2.8. *Sejam $M = \mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_m, N = \mathfrak{b}_1 \oplus ... \oplus \mathfrak{b}_n$ onde as parcelas são ideais fracionários de A. Então $M \cong N$ se e somente se $m = n$ e $\mathfrak{a}_1...\mathfrak{a}_m$ e $\mathfrak{b}_1...\mathfrak{b}_m$ estão na mesma classe (do grupo de classes).*

DEMONSTRAÇÃO. A volta segue diretamente dos lemas A.2.1 e A.2.7.

Agora suponha $M \overset{\theta}{\cong} N$. Então já vimos que $m = (M : A) = (N : A) = n$. Podemos assumir que cada $\mathfrak{a}_i, \mathfrak{b}_j$ contém A visto que ideais fracionários isomorfos estão na mesma classe pelo lema A.2.1. Sejam, para cada $1 \leq i \leq m$, $(a_{i1}, ..., a_{im}) := \theta(1_i)$ (1_i como acima) onde $a_{ij} \in \mathfrak{b}_j$. Pela equação (A.1.1) temos que

$$N = \theta(M) = \theta(\mathfrak{a}_1 1_i \oplus ... \oplus \mathfrak{a}_m 1_m) = \mathfrak{a}_1(a_{11}, a_{12}, ..., a_{1m}) + ... + \mathfrak{a}_m(a_{m1}, a_{m2}, ..., a_{mm}) =$$
$$= (\mathfrak{a}_1 a_{11} + \mathfrak{a}_2 a_{21} + ... + \mathfrak{a}_m a_{m1}, ..., \mathfrak{a}_1 a_{1m} + \mathfrak{a}_2 a_{2m} + ... + \mathfrak{a}_m a_{mm})$$

e vemos que $\mathfrak{b}_j = \sum \mathfrak{a}_k a_{kj}$. Assim, $\mathfrak{b}_1, ..., \mathfrak{b}_m$ contém todos os ideais da forma $a_{1\sigma(1)}...a_{m\sigma(m)}\mathfrak{a}_1...\mathfrak{a}_m$, $\sigma \in S_m$. Sendo $\delta := \det(a_{ij})$ temos que δ é soma de produtos $\prod a_{k\sigma(k)}$ com sinal possivelmente negativo. Portanto, $\mathfrak{b}_1...\mathfrak{b}_m \supseteq \delta\mathfrak{a}_1...\mathfrak{a}_m$. Por outro lado, para cada $1 \leq j \leq m$ existem elementos $b_{ij} \in \mathfrak{a}_j$, $1 \leq i \leq m$ tais que $\theta(b_{1j}, ..., b_{mj}) = 1_j \in \mathfrak{b}_j$. Segue que $(b_{ij})(a_{ij})$ (produto de matrizes) é a matriz identidade donde $\det(b_{ij}) = \delta^{-1}$. O argumento acima mostra então que $\mathfrak{a}_1...\mathfrak{a}_m \supseteq \delta^{-1}\mathfrak{b}_1...\mathfrak{b}_m$ donde $\mathfrak{b}_1...\mathfrak{b}_m = \delta\mathfrak{a}_1...\mathfrak{a}_m$ e do lema A.2.1 $\mathfrak{b}_1...\mathfrak{b}_m$ e $\mathfrak{a}_1...\mathfrak{a}_m$ estão na mesma classe. □

O teorema acima é mais importante do que parece. Em efeito, o que foi demonstrado é a caracterização completa dos módulos projetivos finitamente gerado sobre domínios de Dedekind. De fato, dado M um tal módulo, existe um natural n (o posto) tal que $M \cong A^{n-1} \oplus \mathfrak{a}$ onde A é o domínio de Dedekind em questão e $\mathfrak{a} \in \mathrm{Id}(A)$. Para o leitor interessado ou conhecedor, podemos adiantar que a K-teoria algébrica trata desta, entre outras, questões e, nesta linguagem, o que foi demonstrado aqui é que o grupo $K_0(A) \cong \mathbb{Z} \oplus \mathrm{Id}(A)$. Para mais informações indicamos a referência **[Ros94]** onde, entre outros resultados interessantes, é exposto também uma relação interessante entre o teorema das unidades de Dirichlet e o chamado grupo K_1 de A.

Voltando ao nosso estudo, vejamos agora mais dois lemas, o primeiro sendo um reforço do corolário 2.4.18.

LEMA A.2.9. *Sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais fracionários de A sendo $\mathfrak{a}$ inteiro. Então existe $\mathfrak{c}$, ideal inteiro de A, primo com $\mathfrak{a}$, tal que $\mathfrak{bc}$ é principal.*

DEMONSTRAÇÃO. Escreva $\mathfrak{b} = \mathfrak{b}^+ (\mathfrak{b}^-)^{-1}$ onde $\mathfrak{b}^+$,$\mathfrak{b}^-$ são ideais inteiros. Então pelo corolário 2.4.18 existem ideais inteiros $\mathfrak{c}'$, $\mathfrak{c}''$ primos com $\mathfrak{a}$ tais que $\mathfrak{b}^+\mathfrak{c}'$ e $\mathfrak{b}^-\mathfrak{c}''$ são principais. Também existe $\mathfrak{c}'''$, inteiro, primo com $\mathfrak{a}$ tal que $\mathfrak{c}''c'''$é principal. Assim, sendo $\mathfrak{c} = \mathfrak{c}'\mathfrak{c}'''$, que é inteiro e primo com $\mathfrak{a}$ temos

$$\mathfrak{bc} = \mathfrak{b}^+ \left(\mathfrak{b}^-\right)^{-1} \mathfrak{c}'\mathfrak{c}''' = \left(\mathfrak{b}^+\mathfrak{c}'\right) \left(\mathfrak{b}^-\mathfrak{c}''\right)^{-1} \left(\mathfrak{c}''\mathfrak{c}'''\right)$$

que é principal como queríamos. □

LEMA A.2.10. *Sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais fracionários de A sendo $\mathfrak{a}$ inteiro. Então $A/\mathfrak{a} \cong \mathfrak{b}/\mathfrak{ab}$ como A-módulos.*

DEMONSTRAÇÃO. Pelo lema A.2.9, existe $\mathfrak{c}$ inteiro primo com $\mathfrak{a}$ tal que $\mathfrak{bc}$ é principal, digamos, $\mathfrak{bc} = \rho A$, $\rho \in K$. Defina $\varphi : A \longrightarrow \mathfrak{b}/\mathfrak{ab}$ por $\varphi(\alpha) = \alpha\rho + \mathfrak{ab}$ que é um A-homomorfismo. Afirmamos que φ é sobrejetor e que $\ker\varphi = \mathfrak{a}$. De fato,

$$\varphi(A) = \rho A + \mathfrak{ab} = \mathfrak{bc} + \mathfrak{ab} = (\mathfrak{a} + \mathfrak{c})\,\mathfrak{b} = \mathfrak{b}$$

e temos a sobrejetividade. Agora, se $\alpha \in \mathfrak{a}$ então $\alpha\rho \in \mathfrak{ab}$ pois $\rho \in \mathfrak{b}$ donde $\mathfrak{a} \subseteq \ker\varphi$. Reciprocamente, seja $\alpha \in \ker\varphi$ então $\alpha\rho \in \mathfrak{ab}$ donde $\alpha\rho\mathfrak{c} \subseteq \mathfrak{abc} = \rho\mathfrak{a}$ e $\alpha\mathfrak{c} \subseteq \mathfrak{a}$. Como $\mathfrak{a}+\mathfrak{c} = A$ existem $\alpha_0 \in \mathfrak{a}$, $\gamma \in \mathfrak{c}$ tais que $\alpha_0+\gamma = 1$ donde $\alpha = \alpha\alpha_0+\alpha\gamma \in \mathfrak{a}$. Logo, $\ker\varphi = \mathfrak{a}$ como afirmado. O resultado segue agora do primeiro teorema do homomorfismo. □

A seguir o principal resultado da seção: o teorema dos fatores invariantes para módulos sobre domínios de Dedekind.

THEOREM A.2.11. *(Teorema dos fatores Invariantes)Sejam M, N módulos finitamente gerados, livre de torção sobre um domínio de Dedekind A e de mesmo posto k e tais que $N \subseteq KM$. Então existem elementos $m_1, ..., m_k \in M$ e ideais fracionários $\mathfrak{a}_1, ..., \mathfrak{a}_k, \mathfrak{b}_1, ..., \mathfrak{b}_k$ de A tais que $\mathfrak{b}_j \supseteq \mathfrak{b}_{j+1},\ 1 \leq j \leq k-1$ e*

$$M = \mathfrak{a}_1 m_1 \oplus ... \oplus \mathfrak{a}_k m_k \ ;\ N = \mathfrak{b}_1\mathfrak{a}_1 m_1 \oplus ... \oplus \mathfrak{b}_k\mathfrak{a}_k m_k.$$

Os ideais $\mathfrak{b}_1, ..., \mathfrak{b}_k$ são unicamente determinados pelo par M, N e são denominados os fatores invariantes de N em M.

DEMONSTRAÇÃO. Dividiremos a demonstração em oito etapas procedendo por indução sobre k:

(1) Assuma $k \geq 1$ e suponha o resultado válido para $k-1$ se $k > 1$. Como $N \subseteq KM$ podemos supor M e N imersos no mesmo espaço vetorial k-dimensional. Isto

é, $KM = KN$. Assim, para todo $m \in M$ existe $\alpha \in A\backslash\{0\}$ tal que $\alpha m \in N$, de fato, existe $\beta/\alpha \in K$ e $n \in N$ tal que $m = (\beta/\alpha)\, n \in KN$ donde $\alpha m = \beta n \in AN = N$. Como M é finitamente gerado, usando o argumento acima em um conjunto finito de geradores de M obtemos um elemento $\gamma \in A\backslash\{0\}$ tal que $\gamma M \subseteq N$. Analogamente existe $\delta \in A\backslash\{0\}$ tal que $\delta N \subseteq M$. Defina $\mathfrak{b}' := \{\xi \in K : \xi N \subseteq M\} \ni \delta$ que é um A-submódulo de K não nulo. Além disso, se $\xi \in \mathfrak{b}'$ então $\xi N \subseteq M \implies \gamma\xi N \subseteq N$. Pelo lema A.2.3 concluímos que $\gamma\xi \in A$, ou seja, $\xi \in \gamma^{-1}A$. Segue que $\mathfrak{b}'$ é um submódulo de $\gamma^{-1}A$ e, portanto, um ideal fracionário de A. Por construção, $\mathfrak{b}'$ é o maior ideal fracionário tal que $\mathfrak{b}'N \subseteq M$. Colocando $\mathfrak{b} := (\mathfrak{b}')^{-1}$ concluímos que $\mathfrak{b}$ é o único ideal fracionário minimal tal que $N \subseteq \mathfrak{b}M$. Isto é, para qualquer ideal fracionário não trivial $(\notin \{(0), A\})$, $\mathfrak{c}$, temos $N \nsubseteq \mathfrak{c}\mathfrak{b}M$.

(2) Sejam $\mathfrak{p}_1, ..., \mathfrak{p}_s$ os ideais primos distintos que contém o ideal fracionário principal γA e/ou ocorrem com expoentes negativos na fatoração de $\mathfrak{b}$. Para cada $1 \leq i \leq s$ podemos tomar $n_i \in N$ tal que $n_i \notin \mathfrak{p}_i\mathfrak{b}M$. O teorema chinês do resto nos dá elementos $\mu_i, 1 \leq i \leq s$ tais que $\mu_i \equiv 0 \mod \prod_{i\neq j} \mathfrak{p}_j$ e $\mu_i \equiv 1 \mod \mathfrak{p}_i$. Seja $n := \sum \mu_i n_i \in N$. Afirmamos que $n \notin \mathfrak{p}_i\mathfrak{b}M$, $\forall i$, de fato, suponha por exemplo que $n \in \mathfrak{p}_1\mathfrak{b}M$, como $\mu_i n_i \in \mathfrak{p}_1 N \subseteq \mathfrak{p}_1\mathfrak{b}M$ $\forall i \neq 1$ seguirá que $\mu_1 n_1 \in \mathfrak{p}_1\mathfrak{b}M$. Como $\mathfrak{p}_1$ é ideal maximal podemos tomar $\mu \in A$, $p \in \mathfrak{p}_1$ tal que $p + \mu\mu_1 = 1$ donde $n_1 = pn_1 + \mu\mu_1 n_1 \in \mathfrak{p}_1\mathfrak{b}M$ o que é impossível como afirmado. Obtemos portanto um elemento $n \in N$ tal que $n \notin \mathfrak{p}_i\mathfrak{b}M$, $\forall i$.

(3) Os módulos $Kn \cap N \leq N$ e $Kn \cap M \leq M$ são módulos finitamente gerados, livres de torção e de posto 1. Pelo lema A.2.2 existem ideais $\mathfrak{i}, \mathfrak{j}$ tais que $Kn \cap N = \mathfrak{i}n$ e $Kn \cap M = \mathfrak{j}n$. Então $\mathfrak{b}'\mathfrak{i}n \subseteq \mathfrak{b}'N \subseteq M$ implica $\mathfrak{b}'\mathfrak{i}n \subseteq \mathfrak{j}n$ de maneira que $\mathfrak{j} = \mathfrak{k}^{-1}\mathfrak{b}'\mathfrak{i}$ onde $\mathfrak{k}$ é um ideal inteiro. Em seguida temos $\gamma\mathfrak{j}n \subseteq \gamma M \subseteq N$ donde $\gamma\mathfrak{j} \subseteq \mathfrak{i}$, ou seja, $\gamma \in \mathfrak{i}\mathfrak{j}^{-1} = \mathfrak{k}\mathfrak{b}$. Portanto, $\mathfrak{k}\mathfrak{b}$ contém o ideal fracionário principal γA de maneira que os fatores primos de $\mathfrak{k}$ contém γA ou aparecem com expoentes negativos na fatoração de $\mathfrak{b}$. Sendo assim, os fatores primos de $\mathfrak{k}$ estão entre $\mathfrak{p}_1, ..., \mathfrak{p}_s$. Mas se $\mathfrak{p}_i \supseteq \mathfrak{k}$ então $n \in \mathfrak{i}n = \mathfrak{k}\mathfrak{b}\mathfrak{j}n \subseteq \mathfrak{k}\mathfrak{b}M \subseteq \mathfrak{p}_i\mathfrak{b}M$ o que vimos ser impossível. Logo, $\mathfrak{k} = A$ e $\mathfrak{j} = \mathfrak{b}'\mathfrak{i}$.

(4) Sejam $N_1 := \mathfrak{i}n = Kn \cap N$ e $M_1 := \mathfrak{j}n = \mathfrak{b}'\mathfrak{i}n = Kn \cap M$ que são submódulos livres de torção de M e N respectivamente. Já vimos no teorema A.2.6 que M/N é livre de torção. Como ele é finitamente gerado, pelo mesmo teorema, ele é isomorfo à uma soma direta de ideais de A. Pelo lema A.2.5 ele é A-módulo projetivo. Segue que $0 \longrightarrow M_1 \longrightarrow M \longrightarrow M/M_1 \longrightarrow 0$ cinde e M_1 é somando direto de M. Escreva $M = M_1 \oplus M_1'$ e seja $N_1' := KM_1' \cap N$. Afirmamos que $KN_1' = KM_1'$. Como $\gamma M \subseteq N$ temos $\gamma M_1' \subseteq N_1'$ pois se $x \in M_1' \subseteq M$ então $\gamma x \in N \cap KM_1' = N_1'$. Segue que $KM_1' \subseteq KN_1'$. Reciprocamente, $N_1' \subseteq M = M_1 \oplus M_1'$ donde $KN_1 \subseteq KM_1 \oplus KM_1'$ (basta notar que $K \otimes (M_1 \oplus M_1') \cong (K \otimes M_1) \oplus (K \otimes M_1')$).

Agora, dado $KN_1' \ni \zeta y = \rho x_1 + \xi x_1' \in KM_1 \oplus KM_1'$ temos $\rho x_1 = \zeta y - \xi x_1' \in KM_1'$ pois $y \in N_1' \subseteq KM_1'$. Assim, $\rho x_1 = 0$ e $\zeta y \in KM_1'$ donde $KN_1' \subseteq KM_1'$ provando o afirmado.

(5) Afirmamos agora que $N = N_1 \oplus N_1'$. De fato, da definição de N_1 e M_1 temos que $KN_1 = KM_1$ donde

$$N_1 \cap N_1' \subseteq KN_1 \cap KN_1' = KM_1 \cap KM_1' = (0).$$

Do fato que $KN = KM = KM_1 \oplus KM_1'$ temos que dado $x \in N$ podemos escrever $x = \zeta n + y$, $\zeta \in K, y \in KM_1'$. Então $\mathfrak{b}'x = \mathfrak{b}'\zeta n + \mathfrak{b}'y$. Mas, $\mathfrak{b}'x \subseteq M$ pela construção de $\mathfrak{b}'$. Também, $\mathfrak{b}'\zeta n \subseteq KM_1$ e $\mathfrak{b}'y \subseteq KM_1'$ pois $\zeta n \in KM_1$ e $y \in KN_1'$. Segue que $\mathfrak{b}'\zeta n \subseteq M_1$ donde $\zeta n \in \mathfrak{b}M_1 = N_1$. Assim, $y = x - \zeta n \in N \cap KM_1' = N_1'$ demonstrando o afirmado. Em suma temos, $M = \mathfrak{j}n \oplus M_1'$, $N = \mathfrak{b}\mathfrak{j}n \oplus N_1'$ com $KM_1' = KN_1'$. Fazendo $\mathfrak{a} := \mathfrak{j}$ provamos o primeiro passo da indução.

(6) Aplicando agora a hipótese de indução sobre M_1' e N_1' obtemos elementos $m_1, ..., m_{k-1} \in M_1'$ e ideais $\mathfrak{a}_1, ..., \mathfrak{a}_{k-1}, \mathfrak{b}_1, ..., \mathfrak{b}_{k-1}$ de A tais que $\mathfrak{b}_j \supseteq \mathfrak{b}_{j+1}$, $1 \leq j \leq k-2$ e tais que

$$M_1' = \mathfrak{a}_1 m_1 \oplus ... \oplus \mathfrak{a}_{k-1} m_{k-1} \ ; \ N_1' = \mathfrak{b}_1\mathfrak{a}_1 m_1 \oplus ... \oplus \mathfrak{b}_{k-1}\mathfrak{a}_{k-1} m_{k-1}.$$

Para demonstrar a existência da decomposição é, por fim, suficiente mostrarmos que $\mathfrak{b} \supseteq \mathfrak{b}_1$. Da construção, $\mathfrak{b}_1$ é caracterizado como o único ideal fracionário minimal em relação a propriedade que $\mathfrak{b}_1 M_1' \supseteq N_1'$. Como $\mathfrak{b}M_1' \supseteq N_1'$ segue que $\mathfrak{b} \supseteq \mathfrak{b}_1$ como queremos.

(7) Finalmente, nestas duas últimas etapas, provemos a unicidade dos ideais $\mathfrak{b}_i$. Substituindo M por $\mathfrak{b}_1 M$ podemos supor sem perda de generalidade que os $\mathfrak{b}_i$ são ideais inteiros de A. Do lema A.2.10 temos:

$$M/N \cong \frac{\mathfrak{a}_1}{\mathfrak{b}_1\mathfrak{a}_1} \oplus ... \oplus \frac{\mathfrak{a}_k}{\mathfrak{a}_k\mathfrak{b}_k} \cong \frac{A}{\mathfrak{b}_1} \oplus ... \oplus \frac{A}{\mathfrak{b}_1} \ ; \ \mathfrak{b}_1 \supseteq ... \supseteq \mathfrak{b}_k.$$

Suponha que também temos

$$M/N \cong \frac{A}{\mathfrak{b}_1'} \oplus ... \oplus \frac{A}{\mathfrak{b}_1'} \ ; \ \mathfrak{b}_1' \supseteq ... \supseteq \mathfrak{b}_k'.$$

Note que os módulos $A/\mathfrak{b}_i$ e $A/\mathfrak{b}_i'$ contém apenas umas quantidade finita de submódulos (os módulos da forma $A/\mathfrak{c}$ com $\mathfrak{b} \subseteq \mathfrak{c}$) e são, portanto, Artinianos e Noetherianos. Pelo teorema de Krull-Schmidt [**Cur62**, Seção 14.5, pg.83] cada um deles se decompõe, a menos de permutação, de maneira única em módulos indecomponíveis. Afirmamos que se π é uma potência de um primo então A/π é indecomponível. De fato, A/π possui um único submódulo minimal (em relação a inclusão) donde $A/\pi \cong P \oplus Q$ é impossível visto que este último possui pelo

menos dois. Assim, usando o teorema chinês do resto, vemos que a única decomposição de M/N em indecomponíveis só possui módulos da forma A/π com π uma potência de primo. Segue que as potências de primos presentes na família $\{\mathfrak{b}_i\}$ é a mesma que na família $\{\mathfrak{b}'_i\}$. Seja $\Pi_k = \{\mathfrak{p}_1^{m_1}, ..., \mathfrak{p}_n^{m_n}\}$ tais potências de primos.

(8) Como $\mathfrak{b}_1 \supseteq ... \supseteq \mathfrak{b}_k$ temos que $\mathfrak{b}_k = \operatorname{mmc} \Pi_k$. De fato, $\mathfrak{b}_k$ é múltiplo de comum de Π_k pois cada $\mathfrak{p}_l^{m_l}$ aparece em algum $\mathfrak{b}_i$ e, portanto, em $\mathfrak{b}_k$. Que ele é mínimo com essa propriedade segue do fato que na decomposição de $\mathfrak{b}_k$ só pode aparecer um único elemento de Π_k para cada primo $\mathfrak{p}$ distinto, caso contrário, se $\mathfrak{p}_l^{m_l}, \mathfrak{p}_r^{m_r} \supseteq \mathfrak{b}_k$ com $\mathfrak{p}_l = \mathfrak{p}_r$ então $\mathfrak{p}_l^{m_l+m_r} \supseteq \mathfrak{b}_k$ mas $\mathfrak{p}_l^{m_l+m_r} \notin \Pi_k$ o que é absurdo. Logo, $\mathfrak{b}_k = \operatorname{mmc} \Pi_k = \mathfrak{b}'_k$. Fica agora claro que se Π_{k-1}
, \$é o conjunto obtido a partir de Π_k ao cancelarmos os fatores de $\mathfrak{b}_k$ então $\mathfrak{b}_{k-1} = \operatorname{mmc} \Pi_{k-1} = \mathfrak{b}'_{k-1}$ e o argumento segue demonstrando a unicidade dos $\mathfrak{b}_i$.

(9) Note que, no teorema acima, se $N \subseteq M$ então, por construção (a propriedade de minimalidade), cada $\mathfrak{b}_i$ é ideal inteiro de A.

(10) Como $m_1, ..., m_k \in M$ temos que $1 \in \mathfrak{a}_i$, $\forall i$ donde $\mathfrak{a}_i \supseteq A$, $\forall i$.

□

Uma pequena modificação na prova do último teorema estabelece o seguinte resultado mais geral:

THEOREM A.2.12. *Sejam M e N módulos finitamente gerados, livre de torção sobre um domínio de Dedekind A tal que M tem posto k e $N \subseteq KM$. Então existem elementos $m_1, ..., m_k \in M$ e ideais fracionários $\mathfrak{a}_1, ..., \mathfrak{a}_k, \mathfrak{b}_1, ..., \mathfrak{b}_l$ (onde $l = (N : A)$) de A tais que $\mathfrak{b}_j \supseteq \mathfrak{b}_{j+1}$, $1 \leq j \leq l-1$ e*

$$M = \mathfrak{a}_1 m_1 \oplus ... \mathfrak{a}_k m_k \ ; \ N = \mathfrak{b}_1 \mathfrak{a}_1 m_1 \oplus ... \oplus \mathfrak{b}_l \mathfrak{a}_l m_l.$$

Se $N \subseteq M$ então cada $\mathfrak{b}_i$ é um ideal inteiro de A.□

COROLÁRIO A.2.13. *Todo A-módulo finitamente gerado é isomorfo a uma soma direta de ideais fracionários de A e quocientes da forma $A/\mathfrak{a}$ onde $\mathfrak{a}$ é ideal inteiro de A.*

DEMONSTRAÇÃO. Seja $\mathfrak{b}$ uma A-módulo finitamente gerado e $\beta = \{\beta_i\}_{i=1}^n$ um conjunto finito de geradores para $\mathfrak{b}$. Sendo L o A-módulo livre com base $l = \{l_i\}_{i=1}^n$, o A-epimorfismo $\theta : L \longrightarrow \mathfrak{b}$ dado por $\theta\left(\sum \alpha_i l_i\right) = \sum \alpha_i \beta_i$ induz um isomorfismo $L/M \cong \mathfrak{b}$ onde $M = \ker \theta$. Como A é Noetheriano e L é finitamente gerado segue que L é Noetheriano e, portanto, M é finitamente gerado. É claro que M é livre de torção pois L o é. Assim, usando o teorema A.2.12 temos $L = \oplus_{k=1}^n \mathfrak{a}_k m_k$ e $M = \oplus_{l=1}^m \mathfrak{b}_l \mathfrak{a}_l m_l$ onde m é o posto de M, $m_i \in L$

e $\mathfrak{a}_i$ e $\mathfrak{b}_i$ são ideais de A sendo $\mathfrak{b}_i$ inteiros. Logo,

$$\mathfrak{b} \cong L/M = \frac{\bigoplus_{k=1}^{n} \mathfrak{a}_k m_k}{\bigoplus_{l=1}^{m} \mathfrak{b}_l \mathfrak{a}_l m_l} \cong \left(\bigoplus_{k=1}^{m} \frac{\mathfrak{a}_k m_k}{\mathfrak{b}_k \mathfrak{a}_k m_k} \right) \oplus \left(\bigoplus_{l=m+1}^{n} \mathfrak{a}_l m_l \right).$$

Mas como $\mathfrak{a}_j m_j \cong \mathfrak{a}_j$ pois L é livre de torção e $(\mathfrak{a}_i m_i) / (\mathfrak{b}_i \mathfrak{a}_i m_i) \cong \mathfrak{a}_i / \mathfrak{a}_i \mathfrak{b}_i \cong A/\mathfrak{b}_i$ pelo lema A.2.10, segue o desejado. □

Referências Bibliográficas

[Coh96] H. Cohen, *A course in computational number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 1996.

[Cur62] I. Curtis, C. W.; Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, vol. 11, John Wiley and Sons, 1962.

[Edw77] M. E. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, 1 ed., Graduate Texts in Mathematics, vol. 50, Springer-Verlag, 1977.

[Fro91] M. J. Frohlich, A.; Taylor, *Algebraic number theory*, Cambridge University Press, 1991.

[Lor95] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, AMS, 1995.

[Mil97] J. S. Milne, *Class field theory*, 1997, www.jmilne.org.

[Mil98a] ———, *Algebraic number theory*, 1998, www.jmilne.org.

[Mil98b] ———, *Fields and galois theory*, 1998, www.jmilne.org.

[Rom95] S. Roman, *Field theory*, Graduate Texts in Mathematics, vol. 158, Springer-Verlag, 1995.

[Ros94] J. Rosenberg, *Algebraic k-theory and its applications*, 2 ed., Graduate Texts in Mathematics, vol. 147, Springer-Verlag, 1994.