Tópicos de Teoria Algébrica dos Números

Lorenzo Andreaus

1. Introdução

Nesse trabalho, serão apresentados e provados alguns dos resultados que constituem a base da Teoria Algébrica dos Números, além de exemplos práticos do uso desses resultados na Teoria dos Números tradicional. O objetivo principal deste trabalho é apresentar o conceito de anéis de inteiros algébricos e provar propriedades fundamentais sobre eles, mais especificamente provar que eles sempre são $\mathbb{Z}$-módulos livres finitamente gerados (Teorema da Base Integral) e provar o Teorema da Finitude do Número de Classes, que em certo sentido mede o quão longe um tal anel está de ser um domínio de ideais principais. Este trabalho é baseado principalmente no livro [1]. Comecemos com uma pequena motivação sobre por que estudar os inteiros algébricos:

Grande parte da Teoria dos Números clássica trata da resolução de equações diofantinas. Enquanto não há grande dificuldade em resolver um sistema linear de equações diofantinas, problemas começam a surgir quando aparecem equações de graus maiores. Consideremos os seguintes exemplos:

Dado um n inteiro fixado, a equação diofantina $x^2 - y^2 = n$ não oferece grandes dificuldades, pois podemos fatorar o lado esquerdo para obter $(x-y)(x+y) = n$. Por outro lado, problemas aparecem alterando apenas um sinal: a equação diofantina $x^2 + y^2 = n$ é bem mais difícil de lidar. Uma ideia que surge da resolução da primeira equação é que fatorações em geral simplificam muito um problema. No entanto, $x^2 + y^2$ não se fatora em $\mathbb{Z}$, e sim em $\mathbb{Z}[i]$: $x^2 + y^2 = (x+iy)(x-iy)$. Assim, nada mais natural do que estudar esse anel maior, e torcer para que ele seja "bem comportado"que nem o anel $\mathbb{Z}$. De fato, como veremos, esse anel é um domínio euclidiano.

Infelizmente, nem tudo são flores: há anéis como $\mathbb{Z}[\sqrt{-5}]$ que, como veremos, não são nem sequer um domínio de fatoração única. Podemos tentar corrigir isso olhando para os ideais desses anéis, ao invés de seus elementos. De fato, há um teorema de unicidade da fatoração de ideais em um tipo especial de domínio chamado Domínio de Dedekind, o que é o caso de $\mathbb{Z}[\sqrt{-5}]$ e, na verdade, como veremos, de qualquer anel de inteiros algébricos!

2. Extensões de Corpos

Nessa seção relembraremos alguns conceitos da teoria de extensões de corpos, e enunciaremos sem demonstração os resultados que utilizaremos sobre o assunto. Para um estudo mais detalhado dessa teoria, pode-ser ler [2], que aborda o tema desde os seus princípios básicos. Alguns fatos aqui citados que não se encontram nesse primeiro livro podem ser encontrados na seção "Algebraic Supplement"do livro [3]. No resto dessa seção, K sempre denotará um corpo, e Ω um corpo algebricamente fechado que contém K.

Notação. Seja L/K uma extensão de corpos e $\alpha \in L$ algébrico. O polinômio minimal de α em relação a K será denotado por $P_{\alpha,K}$.

Proposição 2.1. *Seja L/K uma extensão algébrica de corpos, e R um anel com $K \subseteq R \subseteq L$. Então R também é um corpo.*

Teorema 2.2. *Seja L uma extensão algébrica de K. Então existe pelo menos um isomorfismo de L em Ω que fixa K. No caso em que $[L:K]$ é finito, temos no máximo $[L:K]$ isomorfismos de L em Ω que fixam K.*

Definição (Discriminante de um polinômio)**.** Seja $f(x) \in K[x]$ um polinômio mônico de grau n, e $\alpha_1, \ldots, \alpha_n$ as n raízes de f em Ω, contadas com as respectivas multiplicidades. Então o **discriminante** de f, denotado por $\Delta(f)$, é dado por

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Definição (Separabilidade)**.** Seja $f(x) \in K[x]$. Então dizemos que f é **separável** se todas as raízes de f em Ω são simples, ou seja, f se fatora em $\Omega[x]$ como um produto de fatores lineares distintos. Isso é equivalente a termos $\Delta(f) \neq 0$, se f for mônico.

Se $\alpha \in \Omega$ for algébrico sobre K, diremos que α é **separável** se seu polinômio minimal $P_{\alpha,K}$ for separável.

Uma extensão algébrica L de K é chamada **separável** se todo elemento de L for separável sobre K.

Teorema 2.3. *Todo polinômio irredutível com coeficientes num corpo de característica* 0 *é separável.*

Corolário 2.4. *Toda extensão de um corpo de característica* 0 *é separável.*

Teorema 2.5. *Seja L uma extensão finita e separável de K. Então existem exatamente $[L : K]$ isomorfismos de L em Ω que fixam K. Além disso, existe $\alpha \in L$ tal que $L = K(\alpha)$.*

Definição. Se $L = K(\alpha)$, dizemos que L é uma **extensão simples** de K, e que α é um **elemento primitivo** dessa extensão.

Assim, toda extensão separável finita é simples. Lembremos ainda que se $L = K(\alpha)$ é uma extensão finita de K, então α é algébrico sobre K e $P_{\alpha,K}$ tem grau $[L : K]$.

Definição (Polinômio característico, traço e norma)**.** Seja L uma extensão finita de K, com $[L : K] = n$. Dado $\alpha \in L$, a função

$$\begin{array}{rccc} T_\alpha : & L & \longrightarrow & L \\ & x & \longmapsto & \alpha x \end{array}$$

é um operador linear de L visto como K-espaço. Seja $B = \{\beta_1, \ldots, \beta_n\}$ uma base da extensão L/K, e $[T_\alpha]_B$ a matriz de T_α nesta base. Definimos o **polinômio característico** de α com relação à extensão L/K como

$$F_{\alpha,L/K}(x) = \det(x \cdot \mathrm{Id} - [T_\alpha]_B) \in K[x],$$

onde Id é a matriz identidade de tamanho n.

Definimos ainda o **traço** de α, $\mathrm{Tr}_{L/K}(\alpha) \in K$, como sendo o traço de $[T_\alpha]_B$ e a **norma** de α, $N_{L/K}(\alpha) \in K$, como sendo o determinante de $[T_\alpha]_B$.

Observação. Note que o polinômio característico, o traço e a norma de α em relação a L/K não dependem da base B, pois estão associadas ao operador T_α, que só depende de α e da extensão L/K. Quando estiver clara a extensão que estamos considerando, denotaremos o polinômio característico, o traço e a norma de α simplesmente por F_α, $\mathrm{Tr}(\alpha)$ e $N(\alpha)$.

Note ainda que, se $F_\alpha(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$, onde
$a_0, a_1, \ldots, a_n \in K$, então $\mathrm{Tr}(\alpha) = -a_{n-1}$ e $N(\alpha) = (-1)^n a_0$.

Teorema 2.6. *Seja L/K uma extensão finita, e $\alpha \in L$. Então $F_{\alpha,L/K} = P^m_{\alpha,K}$, onde $m = [L : K(\alpha)]$. Em particular, $F_{\alpha,L/K}(\alpha) = 0$.*

Teorema 2.7. *Seja L uma extensão finita de K com $[L : K] = n$, $a, b \in K$, $\alpha, \beta \in L$. Então valem:*
(1) $\mathrm{Tr}(a) = na$.
(2) $N(a) = a^n$.
(3) $\mathrm{Tr}(a \cdot \alpha + b \cdot \beta) = a \cdot \mathrm{Tr}(\alpha) + b \cdot \mathrm{Tr}(\beta)$.
(4) $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

Teorema 2.8. *Seja L uma extensão separável finita de K com $[L : K] = n$. Então, se $\sigma_1, \ldots, \sigma_n$ forem os isomorfismos de L em Ω que fixam K, temos*

$$F_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)),\ \mathrm{Tr}(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha)\ \text{e}\ N(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha).$$

3. Extensões de Anéis, Corpos de Números Algébricos e Inteiros Algébricos

Nessa seção, iremos relembrar os conceitos e resultados básicos sobre a teoria de extensões de anéis. Além disso, utilizaremos essa teoria para construir a base da Teoria Algébrica dos Números, ao trabalhar com corpos de números algébricos e, mais especificamente, com os anéis de inteiros algébricos associados a eles.

Notação. Se R for um anel e M um R-módulo, denotaremos a sua localização por um conjunto multiplicativo C por M_C. Além disso, se M for um domínio, denotaremos seu corpo de frações por $Q(R)$.

Definição (Extensão de anéis/Extensão finita)**.** Dizemos que o anel S é uma **extensão** do anel R se R for um subanel de S. Indicaremos essa extensão por S/R. Dizemos que S é uma extensão **finita** de R se S for finitamente gerado como R-módulo.

Começaremos com um resultado técnico que relaciona extensões de anéis com extensões de corpos:

Proposição 3.1. *Seja R um anel, $K = Q(R)$ e L/K uma extensão algébrica de corpos. Se $S \subseteq L$ e S/R é uma extensão de anéis, então temos $S_{R\setminus\{0\}} = Q(S)$.*

Demonstração. Claramente, $S_{R\setminus\{0\}} \supseteq Q(R)$, logo $S_{R\setminus\{0\}}$ é um anel intermediário da extensão algébrica de corpos L/K, sendo assim um corpo, pela Proposição 2.1. Por outro lado, é claro que $S_{R\setminus\{0\}} \subseteq Q(S)$, e portanto temos $S_{R\setminus\{0\}} = Q(S)$. □

Já o seguinte resultado, que será usado em seções futuras, diz que independência linear sobre um domínio e sobre seu corpo de frações são a mesma coisa:

Proposição 3.2. *Seja R um domínio, $K = Q(R)$ e M um R-módulo. Então $\{m_1, \dots, m_r\} \subseteq M$ é LI sobre R se e só se $\{m_1/1, \dots, m_r/1\} \subseteq M_K$ é LI sobre K.*

Em particular, se L é uma extensão de K, os elementos $\alpha_1, \dots, \alpha_r \in L$ são LI sobre R se e só se eles são LI sobre K.

Observação. Aqui, $M_K \coloneqq K \otimes_R M \cong M_{R\setminus\{0\}}$ é o K-módulo obtido por extensão de escalares ou, equivalentemente, pela localização de M pelo conjunto $R \setminus \{0\}$. Identificamos aqui M_K com a localização $M_{R\setminus\{0\}}$, por isso a notação $m_i/1$.

Demonstração. ($\Leftarrow$) Suponhamos que $m_1/1, \dots, m_r/1 \in M_K$ são LI sobre K. Sejam $a_1, \dots, a_r \in R$ tais que $a_1m_1 + \cdots + a_rm_r = 0$. Mas então

$$\frac{a_1}{1} \cdot \frac{m_1}{1} + \cdots + \frac{a_r}{1} \cdot \frac{m_r}{1} = 0 \Rightarrow \frac{a_1}{1} = \cdots = \frac{a_r}{1} = 0 \Rightarrow a_1 = \cdots = a_r = 0,$$

já que R é domínio e portanto o mapa de localização é injetivo. Logo $m_1, \dots, m_r$ são LI sobre R.

($\Rightarrow$) Suponhamos que $m_1, \dots, m_r$ sejam LI sobre R, e que temos

$$\frac{a_1}{b_1} \cdot \frac{m_1}{1} + \cdots + \frac{a_r}{b_r} \cdot \frac{m_r}{1} = 0, \text{ para alguns } a_1, \dots, a_r \in R, b_1 \dots, b_r \in R \setminus \{0\}.$$

Então, multiplicando essa equação por $\frac{b_1 \dots b_r}{1}$, temos:

$$\frac{a_1B_1m_1 + \cdots + a_rB_rm_r}{1} = 0,$$

onde para $1 \leq i \leq r$ temos $B_i = \dfrac{\prod_{j=1}^{r} b_j}{b_i} \in R$.

Logo, existe algum $t \in R \setminus \{0\}$ tal que $t(a_1B_1m_1 + \cdots + a_rB_rm_r) = 0$, ou seja, $ta_1B_1m_1 + \cdots + ta_rB_rm_r = 0$.

Como $m_1, \dots, m_r$ são LI sobre R, temos $ta_iB_i = 0$ para $1 \leq i \leq n$. Mas tB_i é um produto de elementos não-nulos de R, logo é não-nulo, e assim temos $a_i = 0$ para todo $1 \leq i \leq n$. Isso mostra que $m_1/1, \dots, m_r/1$ são LI sobre $Q(R)$. □

Definição (Elemento integral/Extensão integral)**.** Seja S/R uma extensão de anéis e $\alpha \in S$. Dizemos que α é **integral** sobre R se α satisfaz um polinômio mônico com coeficientes em R.

A extensão de anéis S/R será chamada uma **extensão integral** se todo elemento de S for integral sobre R. Nesse caso, dizemos também que S é **integral** sobre R.

Teorema 3.3. *Seja S/R uma extensão de anéis. Então S/R é uma extensão finita se e só se $S = R[\alpha_1, \dots, \alpha_n]$, onde $\alpha_1, \dots, \alpha_n \in S$ são integrais sobre R. Nesse caso, S é uma extensão integral de R.*

Como corolário desse teorema, obtemos:

Lema 3.4 (Transitividade de extensões integrais)**.** *Seja S uma extensão de R e T uma extensão de S. Então T/R é integral se e só se T/S e S/R são integrais.*

Demonstração. ($\Rightarrow$) Suponhamos T/R integral. Então todo elemento de T satisfaz um polinômio mônico em $R[x] \subseteq S[x]$. Assim, todo elemento de T também é integral sobre S, o que mostra que T/S é integral. Além disso, como $S \subseteq T$ e todo elemento de T é integral sobre R, é claro que a extensão S/R também é integral.

($\Leftarrow$) Suponhamos que T/S e S/R são integrais. Seja $\alpha \in T$. Então α satisfaz um polinômio mônico com coeficientes em S, ou seja:

$$s_0 + s_1\alpha + \cdots + s_{n-1}\alpha^{n-1} + \alpha^n = 0, \text{ para alguns } s_1, \ldots, s_{n-1} \in S.$$

Assim, α é integral sobre $R[s_0, \ldots, s_{n-1}]$, logo pelo Teorema 3.3 o anel $R[s_0, \ldots, s_{n-1}, \alpha]$ é integral sobre $R[s_0, \ldots, s_{n-1}]$. Mas também por esse teorema, $R[s_0, \ldots, s_{n-1}]$ é extensão integral de R, pois por hipótese todo elemento de S é integral sobre R.

Concluímos que o anel $R[s_0, \ldots, s_{n-1}, \alpha]$ é integral sobre R. Em particular, α é integral sobre R. Como α é qualquer, mostramos que a extensão T/R é integral.

□

Definição (Fecho integral)**.** Seja S uma extensão de R. Então o **fecho integral** da extensão S/R, denotado por $I_S(R)$, é definido por:

$$I_S(R) \coloneqq \{\alpha \in S \mid \alpha \text{ é integral sobre } R\}.$$

O fecho integral de uma extensão é sempre um anel, como mostra o corolário abaixo:

Corolário 3.5. *Se S é uma extensão de R, $I_S(R)$ é um subanel de S que contém R. Além disso, todo subanel S' de S que é um R-módulo finitamente gerado está contido em $I_S(R)$.*

Demonstração. É claro que $R \subseteq I_S(R) \subseteq S$. Em particular, $0, 1, -1 \in I_S(R)$. Assim, para vermos que $I_S(R)$ é um anel, basta mostrar que, se $\alpha, \beta \in I_S(R)$, então $\alpha + \beta, \alpha\beta \in I_S(R)$. Mas $\alpha + \beta, \alpha\beta \in R[\alpha, \beta]$. Como α e β são integrais sobre R, $R[\alpha, \beta]$ é integral sobre R pelo Teorema 3.3, logo $\alpha + \beta$ e $\alpha\beta$ são integrais sobre R, e portanto estão em $I_S(R)$, como gostaríamos.

Se $S' \subseteq S$ é um R-módulo finitamente gerado, então S'/S é finito, logo pelo Teorema 3.3 a extensão S'/S é integral, ou seja, $S' \subseteq I_S(R)$. □

Definição (Extensão integralmente fechada/Domínio integralmente fechado)**.** Se S/R é uma extensão de anéis, dizemos que R é **integralmente fechado** sobre S se $I_S(R) = R$. Se R for um domínio e R for integralmente fechado sobre seu corpo de frações $Q(R)$, então dizemos que R é **integralmente fechado**.

O corolário abaixo mostra que o nome fecho algébrico faz sentido:

Corolário 3.6. *Seja R' uma extensão de R e S uma extensão de R'. Então $I_S(R) \subseteq I_S(R')$. Além disso, $R \subseteq I_S(R) = I_S(I_S(R))$. Ou seja, $I_S(R)$ é integralmente fechado em S.*

Demonstração. Se $\alpha \in I_S(R)$, então α é integral sobre R, logo também é integral sobre R'. Então $\alpha \in I_S(R')$, o que mostra a inclusão desejada.

Se $\alpha \in I_S(I_S(R))$, então $I_S(R)[\alpha]/I_S(R)$ é extensão integral. Como $I_S(R)/R$ também é extensão integral, temos pelo Lema 3.4 que $I_S(R)[\alpha]/R$ é integral. Assim, α é integral sobre R, ou seja, $\alpha \in I_S(R)$. Assim, $I_S(I_S(R)) = I_S(R)$, como gostaríamos. □

Definição (Corpo de números algébricos/Anel de inteiros algébricos/Inteiro algébrico)**.** Dizemos que um subcorpo $L \subseteq \mathbb{C}$ é um **corpo de números algébricos** se $L/\mathbb{Q}$ é finita. O anel $I_L(\mathbb{Z}) \subseteq L$ é chamado de **anel dos inteiros algébricos** de L, e o denotaremos simplesmente por I_L. Um elemento qualquer de I_L é chamado de um **inteiro algébrico**.

A maioria dos resultados para anéis mais gerais que provaremos terá uma consequência imediata quando nos restringirmos ao caso dos inteiros algébricos. Denotaremos esses resultados colocando o símbolo $\mathbb{Z}$ para enfatizar que se trata de um resultado sobre inteiros algébricos.

Teorema 3.7. *Seja R um domínio de fatoração única. Então R é integralmente fechado.*

EℤEmplo 1. Temos $I_{\mathbb{Q}} = \mathbb{Z}$, pelo Teorema 3.7. Assim, se soubermos que um inteiro algébrico é racional, garantimos que esse número será inteiro.

Teorema 3.8. *Seja L um corpo que tem R como subanel. Então:*

$$Q(I_L(R)) = (I_L(R))_{R\setminus\{0\}} = I_L(Q(R)).$$

Em particular, temos $Q(I_L(R)) = L$ se e só se L for algébrico sobre $Q(R)$.

Demonstração. A igualdade $Q(I_L(R)) = (I_L(R))_{R\setminus\{0\}}$ segue diretamente da Proposição 3.1. Se $\alpha \in (I_L(R))_{R\setminus\{0\}}$, então temos $\alpha = \beta/r$, onde $\beta \in I_L(R)$, $r \in R \setminus \{0\}$. Assim,

$$a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1} + \beta^n = 0, \text{ para alguns } a_0, \ldots, a_{n-1} \in R.$$

Mas como $\beta = r\alpha$, temos

$$\begin{aligned} & a_0 + a_1 r\alpha + \cdots + a_{n-1}r^{n-1}\alpha^{n-1} + r^n\alpha^n = 0 \\ \Rightarrow \quad & \frac{a_0}{r^n} + \frac{a_1}{r^{n-1}}\alpha + \cdots + \frac{a_{n-1}}{r}\alpha^{n-1} + \alpha^n = 0, \end{aligned}$$

o que mostra que $\alpha \in I_L(Q(R))$. Logo $(I_L(R))_{R\setminus\{0\}} \subseteq I_L(Q(R))$.
Tomemos agora $\alpha \in I_L(Q(R))$. Então temos

$$\frac{r_0}{s_0} + \frac{r_1}{s_1}\alpha + \cdots + \frac{r_{n-1}}{s_{n-1}}\alpha^{n-1} + \alpha^n = 0,$$

para alguns $r_0, \ldots, r_{n-1} \in R, s_0, \ldots, s_{n-1} \in R \setminus \{0\}$.
Multiplicando essa equação por $s_0 s_1 \cdots s_{n-1}$, obtemos uma equação da forma

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0, \text{ onde } a_0, \ldots, a_n \in R, a_n \neq 0.$$

Multiplicando a equação obtida por a_n^{n-1}, temos:

$$a_0 a_n^{n-1} + a_1 a_n^{n-2}(a_n\alpha) + \cdots + a_{n-1}(a_n\alpha)^{n-1} + (a_n\alpha)^n = 0.$$

Chamando $\beta = a_n\alpha$, a equação anterior é equivalente a

$$a_0 a_n^{n-1} + a_1 a_n^{n-2}\beta + \cdots + a_{n-1}\beta^{n-1} + \beta^n = 0.$$

Assim, $\beta \in I_L(R)$, e portanto $\alpha = \beta/a_n \in (I_L(R))_{R\setminus\{0\}}$.
Concluímos que $I_L(Q(R)) \subseteq (I_L(R))_{R\setminus\{0\}}$, e então

$$(I_L(R))_{R\setminus\{0\}} = I_L(Q(R)).$$

Em particular, L é algébrico sobre $Q(R)$ se e só se $I_L(Q(R)) = L \iff Q(I_L(R)) = L$. □

Como todo corpo de números algébricos é uma extensão algébrica de $\mathbb{Q}$:

$\mathbb{Z}$eorema 3.9. *Seja L um corpo de números algébricos. Então $Q(I_L) = (I_L)_{\mathbb{Z}\setminus\{0\}} = L$.*

No caso em que L é um corpo que é extensão do domínio R, parece razoável que, dado um elemento $\alpha \in I_L(R)$, o polinômio minimal $P_{\alpha,Q(R)}$ esteja em $R[x]$. Porém, isso nem sempre é verdade:

Exemplo 1. Seja R um domínio que não é integralmente fechado, e consideremos a extensão $Q(R)/R$. Então existe $\alpha \in Q(R) \setminus R$ que é integral sobre R. Assim, $f(\alpha) = 0$ para algum $f(x) \in R[x]$ mônico. É claro que f tem grau maior ou igual a 2, caso contrário teríamos $\alpha \in R$. Por outro lado, o polinômio minimal de α em $Q(R)$ é $x - \alpha \notin R[x]$.

O exemplo acima mostra que uma condição necessária para garantirmos que $P_{\alpha,Q(R)} \in R[x]$ para $\alpha \in I_L(R)$ é que R seja integralmente fechado. De fato, nesse caso isso irá ocorrer. Para mostrar esse resultado, precisaremos do teorema abaixo:

Teorema 3.10. *Seja S/R uma extensão de domínios.*
a) Se $f, g \in S[x]$ forem dois polinômios mônicos, tais que $fg \in I_S(R)[x]$, então $f, g \in I_S(R)[x]$.
b) Seja L um corpo que tem R como subanel, e $K = Q(R)$.
Então, para todo $\gamma \in I_L(R)$, temos $P_{\gamma,K} \in I_K(R)[x]$.

Demonstração. *a*) Seja Ω um fecho algébrico de $Q(S)$. Então f e g se fatoram linearmente em $\Omega[x]$, digamos $f(x) = (x-\alpha_1)\cdots(x-\alpha_m)$ e $g(x) = (x-\beta_1)\cdots(x-\beta_n)$, com $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in \Omega$. Então

$$fg(x) = (x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)\cdots(x-\beta_n) \in I_S(R)[x].$$

Como $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ são raízes desse polinômio mônico, vemos que esses números são integrais sobre $I_S(R)$, e portanto são também integrais sobre R, já que a extensão $I_S(R)/R$ é integral. Assim, esses números pertencem a $I_\Omega(R)$, e portanto

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_m) \in (I_\Omega(R) \cap S)[x] = I_S(R)[x]$$

e

$$g(x) = (x-\beta_1)\cdots(x-\beta_n) \in (I_\Omega(R) \cap S)[x] = I_S(R)[x].$$

b) Como $\gamma \in I_L(R)$, temos $f(\gamma) = 0$ para algum $f \in R[x]$ mônico. Sabemos então que $P_{\gamma,K}$ divide f em $K[x]$, logo existe $g \in K[x]$ tal que $f = gP_{\gamma,K}$. Como f e $P_{\gamma,K}$ são mônicos, g também deve ser mônico. Como $f \in R[x] \subseteq I_K(R)[x]$, segue do item *a*) que $g, P_{\gamma,K} \in I_K(R)[x]$. □

Se R for integralmente fechado, temos $I_K(R) = R$, e então o teorema acima garante que $P_{\gamma,K} \in R[x]$. O corolário abaixo reúne essa e outras informações que podem ser obtidas com a hipótese extra de R ser integralmente fechado:

Corolário 3.11. *Seja R um domínio integralmente fechado, L uma extensão finita de $K = Q(R)$ e S um subanel de $I_L(R)$ que contém R. Então, para todo $\gamma \in S$, temos:*

a) $P_{\gamma,K} \in R[x]$, $F_{\gamma,L/K} \in R[x]$, $N_{L/K}(\gamma) \in R$ e $\mathrm{Tr}_{L/K}(\gamma) \in R$.

b) $N_{L/K}(\gamma)$ é um múltiplo de γ em S.

c) $\gamma \in U(S)$ se e só se $N_{L/K} \in U(R)$.

d) Se $N_{L/K}(\gamma)$ for irredutível em R, então γ será irredutível em S.

e) Se $\alpha, \beta \in S$ são associados em S, então $N_{L/K}(\alpha)$ e $N_{L/K}(\beta)$ são associados em R.

Demonstração. Se $\gamma = 0$, os resultados são óbvios. Suponhamos então $\gamma \neq 0$. Seja ainda $n = [L : K]$.

a) Temos que $P_{\gamma,K} \in R[x]$ pela observação que fizemos acima. Sendo $F_{\gamma,L/K}$ uma potência de $P_{\gamma,K}$, pelo Teorema 2.6, esse polinômio também está em $R[x]$. Consequentemente, a norma e o traço de γ estão em R, já que são, a menos de sinal, coeficientes do polinômio característico de γ.

b) Temos $F_\gamma(\gamma) = 0$. Escrevamos

$$F_\gamma(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n, \text{ onde } a_0, \ldots, a_{n-1} \in R.$$

Então

$$0 = F_\gamma(\gamma) = a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1} + \gamma^n,$$

o que mostra que $a_0 \equiv 0 \pmod{\gamma}$ em S. Mas $a_0 = (-1)^n N(\gamma)$, logo $\gamma \mid N(\gamma)$ em S, como gostaríamos.

c) Pelo item *b*), $\gamma \mid N(\gamma)$ em S, assim $N(\gamma) \in U(R) \Rightarrow \gamma \in U(S)$. Por outro lado, se $\gamma \in U(S)$, então

$$\gamma\gamma^{-1} = 1 \Rightarrow N(\gamma)N(\gamma^{-1}) = N(1) = 1^n = 1.$$

Como $N(\gamma), N(\gamma^{-1}) \in R$ pelo item *a*), concluímos que $N(\gamma) \in U(R)$.

d) Se γ for redutível em S, temos $\gamma = \alpha\beta$, para alguns $\alpha, \beta \in S \setminus U(S)$, e então $N(\gamma) = N(\alpha)N(\beta)$. Pelo item *c*), concluímos que $N(\alpha), N(\beta) \in R \setminus U(R)$, o que mostra que $N(\gamma)$ não será irredutível em R nesse caso.

e) Sendo α e β associados em S, existe $u \in U(S)$ tal que $\alpha = u\beta$. Então $N(\alpha) = N(u)N(\beta)$. Pelo item *c*), $N(u) \in U(R)$, e portanto $N(\alpha)$ e $N(\beta)$ são associados em R, como desejávamos. □

Como $\mathbb{Z}$ é um DFU, $\mathbb{Z}$ é integralmente fechado pelo Teorema 3.7, e portanto temos:

$\mathbb{Z}$orolário 3.12. *Seja L um corpo de números algébricos e S um subanel de I_L. Então, se $\gamma \in S$, temos:*

a) $P_{\gamma,\mathbb{Q}} \in \mathbb{Z}[x]$, $F_{\gamma,L/\mathbb{Q}} \in \mathbb{Z}[x]$, $N_{L/\mathbb{Q}}(\gamma) \in \mathbb{Z}$ e $\mathrm{Tr}_{L/\mathbb{Q}}(\gamma) \in \mathbb{Z}$.

b) $N_{L/\mathbb{Q}}(\gamma)$ é um múltiplo de γ em S.

c) $\gamma \in U(S)$ se e só se $|N_{L/\mathbb{Q}}| = 1$.

d) Se $|N_{L/\mathbb{Q}}(\gamma)|$ for um número primo, então γ será irredutível em S.

e) Se $\alpha, \beta \in S$ são associados em S, então $N_{L/\mathbb{Q}}(\alpha) = \pm N_{L/\mathbb{Q}}(\beta)$.

O teorema abaixo permite associar ideais em uma extensão integral de domínios:

Teorema 3.13. *Seja S/R uma extensão integral de domínios. Então:*

a) Se $I \in S$ é um ideal não-nulo de S, $I \cap R$ é um ideal não-nulo de R.

b) $U(S) \cap R = U(R)$.

c) S é um corpo se e só se R é um corpo.

d) Um ideal primo $\mathfrak{p}$ de S é maximal de S se e só se $\mathfrak{p} \cap R$ é maximal de R. Em particular, se todo ideal primo não-nulo de R for maximal, todo ideal primo não-nulo de S também será maximal.

Demonstração. *a*) Como I e R são grupos aditivos, $I \cap R$ também é um grupo aditivo. Se $r \in R$, $i \in I \cap R$, então $ir \in I \cap R$, pois I é ideal de S e R é anel. Logo $I \cap R \lhd R$.

Seja agora $\alpha \in I$ não-nulo. Como S/R é integral, temos

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0, \text{ para alguns } a_0, \ldots, a_{n-1} \in R.$$

Podemos supor sem perda de generalidade $a_0 \neq 0$, pois S é um domínio. Assim, $a_0 \in \langle\alpha\rangle_S \subseteq I$, e portanto $I \cap R \ni a_0$ é não-nulo.

b) É claro que $U(R) \subseteq U(S) \cap R$. Seja agora $u \in U(S) \cap R$. Como S/R é integral, u^{-1} é integral sobre R, e assim

$$a_0 + \frac{a_1}{u} + \cdots + \frac{a_{n-1}}{u^{n-1}} + \frac{1}{u^n} = 0, \text{ para alguns } a_0, \ldots, a_{n-1} \in R.$$

Multiplicando essa equação por u^{n-1}:

$$\begin{aligned} & a_0u^{n-1} + a_1u^{n-2} + \cdots + a_{n-1} + u^{-1} = 0 \\ \Rightarrow \quad & u^{-1} = -a_{n-1} - \cdots - a_0u^{n-1} \in R. \end{aligned}$$

Assim, o inverso de u está em R, o que mostra que $u \in U(R)$. Logo
$U(S) \cap R \subseteq U(R)$, e então $U(R) = U(S) \cap R$.

c) Se S for um corpo,

$$U(S) = S \setminus \{0\} \Rightarrow U(R) = U(S) \cap R = S \setminus \{0\} \cap R = R \setminus \{0\},$$

pelo item *b*). Logo R é um corpo.

Se R for um corpo, os únicos ideais de R são 0 e R. Se $I \lhd S$ é não-nulo temos, pelo item *a*), que $I \cap R \lhd R$ é não-nulo, logo $I \cap R = R$. Mas então $1 \in I \Rightarrow I = S$. Logo os únicos ideais de S são 0 e S, e portanto S é um corpo.

d) Seja $\mathfrak{p} \lhd S$ primo. Notemos inicialmente que também temos $\mathfrak{p} \cap R \lhd R$ primo. Consideremos

$$\begin{array}{rccc} \varphi: & R/(\mathfrak{p} \cap R) & \longrightarrow & S/\mathfrak{p} \\ & x + \mathfrak{p} \cap R & \longmapsto & x + \mathfrak{p} \end{array}$$

Então φ é um homomorfismo injetor de anéis, logo podemos ver $S/\mathfrak{p}$ como uma extensão de $R/(\mathfrak{p}\cap R)$. Seja $\alpha+\mathfrak{p}\in S/\mathfrak{p}$. Como $\alpha\in S$ é integral sobre R, temos

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}+\alpha^n=0,\ \text{para alguns } a_0,\ldots,a_{n-1}\in R.$$

Então

$$(a_0+\mathfrak{p})+(a_1+\mathfrak{p})(\alpha+\mathfrak{p})+\cdots+(a_{n-1}+\mathfrak{p})(\alpha+\mathfrak{p})^{n-1}+(\alpha+\mathfrak{p})^n=0,$$

ou seja,

$$\varphi(a_0+\mathfrak{p}\cap R)+\varphi(a_1+\mathfrak{p}\cap R)(\alpha+\mathfrak{p})+\cdots+\varphi(a_{n-1}+\mathfrak{p}\cap R)(\alpha+\mathfrak{p})^{n-1}+(\alpha+\mathfrak{p})^n=0.$$

Logo $\alpha+\mathfrak{p}$ é integral sobre $R/(\mathfrak{p}\cap R)$. Como $\alpha+\mathfrak{p}\in S/\mathfrak{p}$ é qualquer, concluímos que $S/\mathfrak{p}$ é uma extensão integral de $R/(\mathfrak{p}\cap R)$. Sendo essa extensão integral, pelo item c) o anel $S/\mathfrak{p}$ é um corpo se e só se $R/(\mathfrak{p}\cap R)$ é um corpo (já que ambos os anéis em questão são domínios). Ou seja, $\mathfrak{p}$ é um ideal maximal de S se e só se $\mathfrak{p}\cap R$ for um ideal maximal de R.

A última observação segue diretamente de a) e de d). □

Como todo ideal primo não-nulo de $\mathbb{Z}$ é maximal:

$\mathbb{Z}$orolário 3.14 (Anéis de inteiros algébricos têm dimensão 1)**.** *Se L for um corpo de números algébricos, então todo ideal primo não-nulo de I_L é um ideal maximal de I_L.*

4. Corpos Quadráticos

Nessa seção, apresentaremos alguns dos exemplos mais simples de anéis de inteiros algébricos, os anéis de inteiros algébricos de corpos quadráticos, e os relacionaremos com os conceitos desenvolvidos na seção anterior:

Definição (Corpo quadrático)**.** Dizemos que um corpo de números algébricos L é um **corpo quadrático** se $[L:\mathbb{Q}]=2$.

Nesse caso, se $\alpha\in L\setminus\mathbb{Q}$, temos $1<[\mathbb{Q}(\alpha):\mathbb{Q}]\leq[L:\mathbb{Q}]=2$, logo $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$, assim $\mathbb{Q}(\alpha)=L$. Portanto, todo $\alpha\in L\setminus\mathbb{Q}$ é um elemento primitivo de $L/\mathbb{Q}$.

Mostraremos abaixo que todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, $d\neq 0,1$:

Teorema 4.1. *Seja $\mathcal{D}=\{d\in\mathbb{Z}\setminus\{0,1\}\mid d \text{ é livre de quadrados}\}$, e seja $\mathcal{L}_2=\{L\subseteq\mathbb{C}\mid L \text{ é corpo quadrático}\}$. Então*

$$\begin{array}{rccc} f: & \mathcal{D} & \longrightarrow & \mathcal{L}_2 \\ & d & \longmapsto & \mathbb{Q}(\sqrt{d}) \end{array}$$

é uma bijeção. Mais do que isso, se d_1 e d_2 pertencem a $\mathcal{D}$, então $\mathbb{Q}(\sqrt{d_1})$ é isomorfo a $\mathbb{Q}(\sqrt{d_2})$ se e só se $d_1=d_2$.

Demonstração. Claramente, $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$ para $d\in\mathcal{D}$, então de fato temos $\mathbb{Q}(\sqrt{d})\in\mathcal{L}_2$, de modo que f está bem-definida.

Suponhamos que exista uma bijeção $\varphi:\mathbb{Q}(\sqrt{d_1})\to\mathbb{Q}(\sqrt{d_2})$, onde $d_1,d_2\in\mathcal{D}$.

Então $\varphi(\sqrt{d_1})^2=\varphi(d_1)=d_1$, logo d_1 tem uma raiz quadrada em $\mathbb{Q}(\sqrt{d_2})$. Sejam então $a,b\in\mathbb{Q}$ tais que $\sqrt{d_2}=a+b\sqrt{d_1}$. Elevando essa equação ao quadrado, obtemos $d_2=a^2+d_1b^2+2ab\sqrt{d_1}$.

Se $a,b\neq 0$, chegamos em

$$\sqrt{d_1}=\frac{d_2-a^2-d_1b^2}{2ab}\in\mathbb{Q},$$

absurdo! Logo $a=0$ ou $b=0$. Se $b=0$, $\sqrt{d_2}=a\in\mathbb{Q}$, absurdo! Então $a=0$, e portanto

$$\sqrt{d_2}=b\sqrt{d_1}\Rightarrow d_2=b^2d_1.$$

Como $b^2\mid d_2$ e d_2 é livre de quadrados, temos $b^2=1$, e assim $d_2=d_1$. Isso garante que f é injetivo, e prova a última afirmação do enunciado.

Falta apenas provar que f é sobrejetor. Seja $L \in \mathcal{L}_2$. Então $[L:\mathbb{Q}] = 2$. Como vimos, se $\alpha \in L \setminus \mathbb{Q}$, temos $L = \mathbb{Q}(\alpha)$. Além disso, α satisfaz uma equação de segundo grau em $\mathbb{Q}[x]$, e portanto em $\mathbb{Z}[x]$, limpando os denominadores se necessário. Então $a\alpha^2 + b\alpha + c = 0$, para alguns $a, b, c \in \mathbb{Z}, a \neq 0$. Assim, obtemos

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Isso mostra que $L = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4ac})$. Podemos escrever $b^2 - 4ac = k^2 d$, onde k é um inteiro positivo e $d \in \mathcal{D}$. Mas então $\sqrt{b^2 - 4ac} = k\sqrt{d}$, e

$$L = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4ac}) = \mathbb{Q}(\sqrt{d}) = f(d).$$

Assim f é sobrejetora, e portanto é uma bijeção, como gostaríamos.

□

Se $L = \mathbb{Q}(\sqrt{d})$ é uma extensão quadrática com $d \in \mathcal{D}$, então $\{1, \sqrt{d}\}$ é uma base dessa extensão.
Seja $\alpha = a + b\sqrt{d} \in L$ qualquer. Então:

$$\begin{aligned} \alpha \cdot 1 &= a + b\sqrt{d}, \\ \alpha \cdot \sqrt{d} &= bd + a\sqrt{d}. \end{aligned}$$

Dessa forma, a matriz de multiplicação por α nessa base é

$$M_\alpha = \begin{bmatrix} a & bd \\ b & a \end{bmatrix}.$$

Então, em relação à extensão $L/\mathbb{Q}$:

$$F_\alpha(x) = \det(x\,\mathrm{Id} - M_\alpha) = \det \begin{pmatrix} x-a & -bd \\ -b & x-a \end{pmatrix} = x^2 - 2ax + (a^2 - db^2).$$

Assim, $\mathrm{Tr}(a + b\sqrt{d}) = 2a$ e $N(a + b\sqrt{d}) = a^2 - db^2$. Note que, se $d < 0$, $N(a + b\sqrt{d}) \geq 0$ sempre, com igualdade se e só se $a = b = 0$.

Buscaremos agora determinar, para $L = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, o anel I_L, que mostraremos ser um $\mathbb{Z}$-módulo livre de dimensão 2. Continuaremos por ora a usar a base $\{1, \sqrt{d}\}$ de L, embora como logo veremos essa nem sempre será uma base de I_L como $\mathbb{Z}$-módulo:

Lema 4.2. *Seja $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$. Então*

$$I_L = \left\{ \frac{m}{2} + \frac{n}{2}\sqrt{d} \mid m, n \in \mathbb{Z}; m^2 - dn^2 \equiv 0 \pmod 4 \right\}.$$

Demonstração. ($\subseteq$) Suponhamos $\alpha = a + b\sqrt{d} \in I_L$. Então pelo Zorolário 3.12, $F_\alpha(x) \in \mathbb{Z}[x]$. Como já vimos,

$$F_\alpha(x) = x^2 - 2ax + (a^2 - db^2).$$

Disso tiramos que $2a \in \mathbb{Z}$ e que $a^2 - db^2 \in \mathbb{Z}$. Seja $r = a^2 - db^2$. Dessa forma, $4a^2 - 4db^2 = 4r$, ou seja, $d(2b)^2 = (2a)^2 - 4r \in \mathbb{Z}$, pois $2a \in \mathbb{Z}$. Podemos escrever $2b = p/q$, com $p, q \in \mathbb{Z}$, $q \neq 0$, primos entre si. Então $d(2b)^2 \in \mathbb{Z} \Rightarrow q^2 \mid dp^2$, e como d é livre de quadrados temos $q^2 \mid p^2$. Assim, $q = \pm 1$, de modo que $2b$ é inteiro.
Portanto, $m \coloneqq 2a$ e $n \coloneqq 2b$ são números inteiros, e como vimos temos

$$m^2 - dn^2 = 4r \equiv 0 \pmod 4.$$

Isso mostra que $\alpha = \dfrac{m}{2} + \dfrac{n}{2}\sqrt{d}$ está no conjunto da direita do enunciado.

($\supseteq$) Seja

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d},$$

onde $m, n \in \mathbb{Z}$ satisfazem $m^2 - dn^2 \equiv 0 \pmod 4$. Então

$$F_\alpha(x) = x^2 - mx + \frac{m^2 - dn^2}{4}$$

Como $m^2 - dn^2 \equiv 0 \pmod 4$, temos $F_\alpha(x) \in \mathbb{Z}[x]$, e como $F_\alpha(\alpha) = 0$, temos $\alpha \in I_L$.

□

Agora sim podemos mostrar que $L = \mathbb{Q}(\sqrt{d})$ é sempre um $\mathbb{Z}$-módulo livre:

Teorema 4.3. *Seja $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$. Então:*

a) Se $d \equiv 2$ ou $3 \pmod 4$, então $B = \{1, \sqrt{d}\}$ é uma base de I_L como $\mathbb{Z}$-módulo.

b) Se $d \equiv 1 \pmod 4$, então $B = \left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ é uma base de I_L como $\mathbb{Z}$-módulo.

Demonstração. Notemos que, em ambos os casos, basta mostrar que $\langle B \rangle = I_L$, pois B é um conjunto LI sobre $\mathbb{Q}$, e portanto também é LI sobre $\mathbb{Z}$ pela Proposição 3.2.

a) É imediato verificar que os elementos 1 e $\sqrt{d}$ estão em I_L, utilizando o lema anterior. Assim, $\langle 1, \sqrt{d} \rangle \subseteq I_L$. Seja agora $\alpha \in I_L$. Então, pelo lema anterior,

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in I_L, \text{ com } m^2 - dn^2 \equiv 0 \pmod 4.$$

Se $d \equiv 2 \pmod 4$, então $m^2 \equiv 0 \pmod 2$, e assim m é par. Logo $4 \mid dn^2$, e como d é livre de quadrados temos $2 \mid n$. Isso mostra que n também é par, e assim

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in \langle 1, \sqrt{d} \rangle.$$

Se $d \equiv 3 \pmod 4$, então $m^2 + n^2 \equiv 0 \pmod 4$. Como o quadrado de um ímpar deixa resto 1 na divisão por 4, a única possibilidade é termos $m \equiv n \equiv 0 \pmod 2$. Assim:

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in \langle 1, \sqrt{d} \rangle.$$

Logo, em ambos os casos, temos $I_L = \langle 1, \sqrt{d} \rangle$.

b) É imediato verificar que os elementos 1 e $\dfrac{1+\sqrt{d}}{2}$ estão em I_L, utilizando o lema anterior.

Assim, $\left\langle 1, \dfrac{1+\sqrt{d}}{2} \right\rangle \subseteq I_L$. Seja agora $\alpha \in I_L$. Então, pelo lema anterior,

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \in I_L, \text{ com } m^2 - dn^2 \equiv 0 \pmod 4.$$

Como $d \equiv 1 \pmod 4$, temos $m^2 \equiv n^2 \pmod 4$. Logo m e n possuem a mesma paridade, e podemos escrever $m = 2k + n$, com $k \in \mathbb{Z}$. Assim:

$$\alpha = \frac{2k+n}{2} + \frac{n}{2}\sqrt{d} = k + n\Big(\frac{1+\sqrt{d}}{2}\Big) \in \left\langle 1, \frac{1+\sqrt{d}}{2} \right\rangle.$$

Logo temos $I_L = \left\langle 1, \dfrac{1+\sqrt{d}}{2} \right\rangle$. □

Exemplo 2. O anel $R = \mathbb{Z}[\sqrt{d}]$, para $d \in \mathcal{D}$ congruente a 1 módulo 4, não é integralmente fechado. De fato, é claro que seu corpo de frações é $K = \mathbb{Q}(\sqrt{d})$, e que, como $R/\mathbb{Z}$ é uma extensão integral,

$$I_K(R) = I_K(\mathbb{Z}) = \left\langle 1, \frac{1+\sqrt{d}}{2} \right\rangle \supsetneq R.$$

Em particular, R não é um DFU.

Uma vez que $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ é base de I_L no caso $d \equiv 1 \pmod 4$, é razoável querermos saber calcular o polinômio característico, o traço e a norma de um elemento α de I_L escrito na forma $\alpha = a + b\Big(\dfrac{1+\sqrt{d}}{2}\Big)$, com $a, b \in \mathbb{Z}$:

Temos

$$a + b\Big(\frac{1+\sqrt{d}}{2}\Big) = \Big(a + \frac{b}{2}\Big) + \frac{b}{2}\sqrt{d},$$

e portanto

$$F_\alpha(x) = x^2 - (2a+b)x + \Big(a^2 + ab + b^2\Big(\frac{1-d}{4}\Big)\Big).$$

Logo

$$\mathrm{Tr}\left(a + b\Big(\frac{1+\sqrt{d}}{2}\Big)\right) = 2a + b,$$

e

$$N\Big(a + b\Big(\frac{1+\sqrt{d}}{2}\Big)\Big) = a^2 + ab + b^2\Big(\frac{1-d}{4}\Big).$$

É interessante se perguntar quando I_L é um DFU, um DIP ou um DE (Domínio Euclidiano), para podermos deduzir propriedades mais profundas desse anel. Às vezes, I_L pode não ser nem mesmo um DFU:

Exemplo 3. O anel $I_L = \mathbb{Z}[\sqrt{-5}]$ não é um DFU. De fato, temos que

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

são duas fatorações distintas de 21 nesse anel.

Temos $N(3) = 9$, $N(7) = 49$, e $N(1 + 2\sqrt{-5}) = N(1 - 2\sqrt{-5}) = 21$. Assim, pelos itens c) e e) do Zorolário 3.12, os elementos 3, 7, $1 + 2\sqrt{-5}$ e $1 - 2\sqrt{-5}$ não são invertíveis em I_L, e 3 e 7 não são associados a $1 + 2\sqrt{-5}$ nem a $1 - 2\sqrt{-5}$. Assim, basta provarmos que esses quatro elementos são irredutíveis em I_L. Se algum desses elementos não for irredutível, então garantimos a existência de um elemento em I_L com norma ± 3 ou ± 7, o que é impossível, pois não existem, $a, b \in \mathbb{Z}$ tais que $N(a + b\sqrt{-5}) = a^2 + 5b^2$ seja ± 3 ou ± 7. Assim, I_L não é DFU.

Observe que esse exemplo ainda prova que a volta do item d) do Corolário 3.11 é falsa: por exemplo 3 é irredutível em I_L mas $N(3) = 9$ não é irredutível em $\mathbb{Z}$.

Analisemos agora a questão de I_L ser um DE. O melhor candidato à "função grau"é o valor absoluto da norma correspondente à extensão, pois já sabemos de antemão que essa é uma função com valores naturais que é multiplicativa.

Teorema 4.4. *Seja $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$.*

a) As seguintes condições são equivalentes:

(i) I_L é euclidiano em relação à norma absoluta.

(ii) Para qualquer $\lambda \in L$, existe $q \in I_L$ tal que $|N_{L/\mathbb{Q}}(\lambda - q)| < 1$.

(iii) Para quaisquer $r, s \in \mathbb{Q}$, existem $m, n \in \mathbb{Z}$ tais que:

$$\begin{cases} |(r-m)^2 - d(s-n)^2| < 1, \ \textit{se } d \equiv 2 \textit{ ou } 3 \pmod 4; \\ \left|(r - m + \frac{s-n}{2})^2 - d(\frac{s-n}{2})^2\right| < 1, \ \textit{se } d \equiv 1 \pmod 4. \end{cases}$$

b) I_L é euclidiano com a norma absoluta se $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 13\}$, e isso não acontece para nenhum outro valor negativo de $d \in \mathcal{D}$.

Demonstração. a) (i)⇒(ii): Suponhamos que valha (i). Seja $\lambda \in L$ qualquer. Pelo Zeorema 3.9, temos $L = \mathbb{Q}(I_L)$, logo temos $\lambda = a/b$, para alguns $a, b \in I_L$, $b \neq 0$. Por hipótese, existem $q, r \in I_L$ tais que $a = bq + r$ e $|N(r)| < |N(b)|$. Assim:

$$|N(\lambda - q)| = \Big|N\Big(\frac{a}{b} - q\Big)\Big| = \Big|N\Big(\frac{r}{b}\Big)\Big| = \frac{|N(r)|}{|N(b)|} < 1,$$

provando (ii)

(ii)⇒(i) Suponhamos que valha (ii). Sejam $a, b \in I_L$ quaisquer, $b \neq 0$. Então existe $q \in I_L$ tal que $\left|N\left(\frac{a}{b} - q\right)\right| < 1$. Chamemos $r = a - bq \in I_L$. Assim, $a = bq + r$ e temos:

$$\left|N\left(\frac{a}{b} - q\right)\right| < 1 \Rightarrow \left|N\left(\frac{r}{b}\right)\right| < 1 \Rightarrow \frac{|N(r)|}{|N(b)|} < 1 \Rightarrow |N(r)| < |N(b)|,$$

provando (i).

(ii) $\iff$ (iii): Basta, se $d \equiv 2$ ou $3 \pmod 4$, tomar $\lambda = r + s\sqrt{d} \in L$ e $q = m + n\sqrt{d} \in I_L$, e notar que a desigualdade em (iii) equivale a termos $|N(\lambda - q)| < 1$. Da mesma forma, se $d \equiv 1 \pmod 4$, basta tomar $\lambda = r + s\left(\frac{1+\sqrt{d}}{2}\right) \in L$ e $q = m + n\left(\frac{1+\sqrt{d}}{2}\right) \in I_L$ e notar que a desigualdade em (iii) equivale a termos $|N(\lambda - q)| < 1$.

b) Provaremos que para esses valores de d vale (iii), e que para qualquer outro valor negativo de $d \in \mathcal{D}$ não vale (iii):

Caso 1: $d < 0$. Chamemos $\ell = -d > 0$. Como observado anteriormente, nesse caso a norma é sempre não-negativa, então podemos ignorar os valores absolutos em (iii).

Caso 1.1: $d \equiv 2$ ou $3 \pmod 4$. Suponhamos $\ell < 3$. Sejam $r, s \in \mathbb{Q}$. Então existem inteiros $m, n \in \mathbb{Z}$ tais que $|r - m| \leq 1/2$ e $|s - n| \leq 1/2$. Então,

$$(r-m)^2 + \ell(s-n)^2 < \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2 = 1,$$

logo vale (iii). Assim, se $d \in \{-2, -1\}$, I_L é DE. Se $\ell \geq 5$, tomemos $r = s = 1/2$. Então, para quaisquer $m, n \in \mathbb{Z}$, temos $|r - m| \geq 1/2$ e $|s - n| \geq 1/2$. Assim:

$$(r-m)^2 + \ell(s-n)^2 \geq \left(\frac{1}{2}\right)^2 + 5\left(\frac{1}{2}\right)^2 = \frac{3}{2} > 1,$$

mostrando que nesse caso não vale (iii).

Caso 1.2: $d \equiv 1 \pmod 4$. Suponhamos $\ell \leq 11$. Sejam $r, s \in \mathbb{Q}$. Então existe um inteiro n tal que $|s - n| \leq 1/2$. Queremos agora achar $m \in \mathbb{Z}$ tal que

$$\left|r - m + \frac{s-n}{2}\right| \leq 1/2,$$

ou seja,

$$-\frac{1}{2} \leq r - m + \frac{s-n}{2} \leq \frac{1}{2} \iff r + \frac{s-n-1}{2} \leq m \leq r + \frac{s-n+1}{2}.$$

Como a diferença entre os números nos extremos da última desigualdade é de 1, podemos tomar m como sendo um número inteiro no intervalo correspondente. Para esses valores de m e n, temos:

$$\left(r - m + \frac{s-n}{2}\right)^2 + \ell\left(\frac{s-n}{2}\right)^2 \leq \left(\frac{1}{2}\right)^2 + 11\left(\frac{1}{4}\right)^2 = \frac{15}{16} < 1,$$

logo vale (iii). Assim, se $d \in \{-11, -7\}$, I_L é DE. Se $\ell \geq 15$, tomemos $r = s = 1/2$. Sejam $m, n \in \mathbb{Z}$. Se $n \notin \{0, 2\}$, então $s - n > 1$, e portanto

$$\ell\left(\frac{s-n}{2}\right)^2 > 15\left(\frac{1}{2}\right)^2 = \frac{15}{4} > 1,$$

o que já mostra que não temos a desigualdade de (iii). Se $n = 0$ ou $n = 2$, então é claro que os valores de m que minimizam $\left|r - m + \frac{s-n}{2}\right|$ são $m = 1$ e $m = 0$, respectivamente. De qualquer forma, vemos que $\left|r - m + \frac{s-n}{2}\right| \geq \frac{1}{4}$. Assim:

$$\left(r - m + \frac{s-n}{2}\right)^2 + \ell(s-n)^2 \geq \left(\frac{1}{4}\right)^2 + 15\left(\frac{1}{4}\right)^2 = 1,$$

mostrando que nesse caso não vale (iii).

Caso 2: $d > 0$:

Caso 2.1: $d \in \{2, 3\}$. Dados $r, s \in \mathbb{Q}$, sejam $m, n \in \mathbb{Z}$ tais que $|r - m| \leq 1/2$ e $|s - n| \leq 1/2$. Assim, como $d > 0$:

$$\left|(r-m)^2 - d(s-n)^2\right| \leq \max\left\{(r-m)^2, d(s-n)^2\right\}.$$

Mas

$$(r-m)^2 \leq \left(\frac{1}{2}\right)^2 = \frac{1}{4} \text{ e } d(s-n)^2 \leq 3\left(\frac{1}{2}\right)^2 = \frac{3}{4},$$

portanto vale (iii).

Caso 2.2: $d \in \{5, 13\}$. Dados $r, s \in \mathbb{Q}$, sejam $m, n \in \mathbb{Z}$ tais que $\left|r - m + \frac{s-n}{2}\right| \leq 1/2$ e $|s - n| \leq 1/2$ (podemos achar tais inteiros procedendo como no Caso 1.2). Assim, como $d > 0$:

$$\left|\left(r - m + \frac{s-n}{2}\right)^2 - d\left(\frac{s-n}{2}\right)^2\right| \leq \max\left\{\left(r - m + \frac{s-n}{2}\right)^2, d\left(\frac{s-n}{2}\right)^2\right\}.$$

Mas

$$\left(r - m + \frac{s-n}{2}\right)^2 \leq \left(\frac{1}{2}\right)^2 = \frac{1}{4} \text{ e } d\left(\frac{s-n}{2}\right)^2 \leq 13\left(\frac{1}{4}\right)^2 = \frac{13}{16},$$

portanto vale (iii). □

Observação. Pode-se provar que, se $d \in \{6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$, então $I_{\mathbb{Q}(\sqrt{d})}$ também é euclidiano com relação à norma absoluta, e esses valores, junto com os do teorema acima, são os únicos valores de $d \in \mathcal{D}$ tais que isso acontece.

Podemos agora nos perguntar para que valores de d o anel I_L será um DIP ou um DFU. De fato, veremos mais adiante que I_L será um DIP se e só se I_L for um DFU (e isso não vale apenas para corpos quadráticos, mas em geral).

No caso em que $d < 0$, é fácil caracterizarmos os elementos inversíveis de I_L.

Teorema 4.5. *Seja $L = \mathbb{Q}(\sqrt{d})$, com $d \in \mathcal{D}$ e $d < 0$.*

a) Se $d = -1$, então $U(I_L) = \{1, i, -i, -1\}$ é gerado por i.

b) Se $d = -3$, então $U(I_L) = \{1, \zeta, \zeta^2, \zeta^3 = -1, \zeta^4, \zeta^5\}$ é gerado por $\zeta = \frac{1+\sqrt{-3}}{2}$, uma raiz sexta primitiva da unidade.

c) Se $d \notin \{-1, -3\}$, então $U(I_L) = \{1, -1\}$.

Demonstração. Pelo item *c)* do Zorolário 3.12, se $\alpha \in I_L$ então $\alpha \in U(I_L)$ se e só se $N(\alpha) = 1$, já que para $d < 0$ a norma é sempre não-negativa.

a) Seja $a + bi \in \mathbb{Z}[i]$, com $a, b \in \mathbb{Z}$. Então $N(a + bi) = a^2 + b^2$, e temos

$$\begin{aligned} N(a+bi) = 1 \iff a^2 + b^2 = 1 &\iff (a, b) = (\pm 1, 0) \text{ ou } (a, b) = (0, \pm 1) \\ &\iff a + bi = \pm 1, \pm i. \end{aligned}$$

b) Seja $a + b\zeta \in \mathbb{Z}[\zeta]$, com $a, b \in \mathbb{Z}$. Então $N(a + b\zeta) = a^2 + ab + b^2$, e temos

$$N(a + b\zeta) = 1 \iff a^2 + ab + b^2 = 1.$$

Fixado a, obtemos

$$b = \frac{-a \pm \sqrt{4-3a^2}}{2}.$$

Assim, devemos ter $4 - 3a^2 \geq 0 \Rightarrow a \in \{0, 1, -1\}$. Para cada um desses valores de a, obtemos dois valores possíveis para b, obtendo assim seis pares (a, b) possíveis, a saber $(0, 1), (0, -1), (1, 0), (-1, 0), (1, -1)$ e $(-1, 1)$. É fácil verificar que os seis números $a + b\zeta$ correspondentes a esses pares são aqueles indicados no enunciado.

c) Chamemos $\ell = -d \geq 2$. Se $d \equiv 2$ ou $3 \pmod 4$, um elemento genérico de I_L é da forma $a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$. Então $N(a + bi) = a^2 + \ell b^2$, e temos

$$N(a + b\sqrt{d}) = 1 \iff a^2 + \ell b^2 = 1.$$

Se $b = 0$, obtemos $a = \pm 1$. Se $b \neq 0$, então $a^2 + \ell b^2 \geq \ell \geq 2 > 1$. Assim, nesse caso $U(I_L) = \{1, -1\}$.

Se $d \equiv 1 \pmod 4$, temos $\ell \geq 7$, e um elemento genérico de I_L é da forma $a + b\Big(\frac{1+\sqrt{d}}{2}\Big)$, com $a, b \in \mathbb{Z}$. Então

$$N\Big(a + b\Big(\frac{1+\sqrt{d}}{2}\Big)\Big) = a^2 + ab + b^2\Big(\frac{1+\ell}{4}\Big) \geq a^2 + ab + 2b^2,$$

e temos

$$N\Big(a + b\Big(\frac{1+\sqrt{d}}{2}\Big)\Big) = 1 \iff a^2 + ab + b^2\Big(\frac{1+\ell}{4}\Big) = 1 \Rightarrow a^2 + ab + 2b^2 \leq 1.$$

Se $b = 0$, obtemos $a = \pm 1$. Se $b \neq 0$, então

$$a^2 + ab + 2b^2 = N_{\mathbb{Q}(\sqrt{3})/\,\mathbb{Q}}(a + b\zeta) + b^2 \geq 1 + 1 = 2 > 1.$$

Assim, nesse caso $U(I_L) = \{1, -1\}$.

□

5. O Discriminante

Nosso foco nessas próximas seções é provar que todo anel de inteiros algébricos possui uma base integral. Para isso, provaremos alguns resultados técnicos que nos permitirão ver todo anel de inteiros algébricos como um submódulo de um módulo livre. Por fim, provaremos e utilizaremos um resultado clássico da teoria de módulos livres sobre Domínios de Ideais Principais. Começaremos definindo o discriminante de uma n-upla de elementos de uma extensão de grau n:

Definição (Discriminante de uma n-upla)**.** Seja L/K uma extensão finita e separável, $[L : K] = n$. Se $\alpha_1, \ldots, \alpha_n \in L$, o **discriminante** da n-upla $\alpha_1, \ldots, \alpha_n$ é dado por:

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) \in K.$$

Observação. Quando a extensão L/K estiver clara, indicaremos o discriminante de $\alpha_1, \ldots, \alpha_n$ simplesmente por $\Delta(\alpha_1, \ldots, \alpha_n)$.

Proposição 5.1. *Sejam $\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_n \in L$, e suponhamos que, para $1 \leq i \leq n$, temos*

$$\gamma_i = \sum_{j=1}^{n} c_{ij}\alpha_j, \ \textit{onde } c_{i1}, \ldots, c_{in} \in K.$$

Então temos

$$\Delta_{L/K}(\gamma_1, \ldots, \gamma_n) = (\det(c_{ij}))^2 \Delta_{L/K}(\alpha_1, \ldots, \alpha_n).$$

Demonstração. Notemos que, para $1 \leq i, j \leq n$, temos

$$\gamma_i\gamma_j \quad = \quad \left(\sum_{r=1}^{n} c_{ir}\alpha_r\right)\left(\sum_{s=1}^{n} c_{js}\alpha_s\right) = \sum_{r=1}^{n}\sum_{s=1}^{n} c_{ir}c_{js}\alpha_r\alpha_s.$$

Tomando o traço, temos:

$$\mathrm{Tr}(\gamma_i\gamma_j) = \sum_{r=1}^{n}\sum_{s=1}^{n} c_{ir}c_{js}\,\mathrm{Tr}(\alpha_r\alpha_s).$$

Desse modo, temos a igualdade de matrizes:

$$(\mathrm{Tr}(\gamma_i\gamma_j)) = (c_{ij})(\mathrm{Tr}(\alpha_i\alpha_j))(c_{ij})^{\intercal}.$$

Tomando o determinante, obtemos a igualdade desejada. □

Como L/K é finita de grau n e separável, podemos considerar os n isomorfismos de L num fecho algébrico Ω de L que fixam K, e escrevermos o traço de um elemento em função desses isomorfismos.

Proposição 5.2. *Sejam $\sigma_1, \ldots, \sigma_n$ os n isomorfismos de L em Ω que fixam K. Então temos*

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = [\det(\sigma_i(\alpha_j))]^2.$$

Demonstração. Sabemos que, para $1 \leq i, j \leq n$, vale

$$\mathrm{Tr}(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j).$$

Então temos a igualdade de matrizes

$$(\mathrm{Tr}(\alpha_i\alpha_j)) = (\sigma_i(\alpha_j))^{\intercal}(\sigma_i(\alpha_j))$$

Tomando o determinante, obtemos a igualdade desejada. □

Podemos também, fixado um elemento $\alpha \in L$, associar o discriminante da n-upla $1, \alpha, \ldots, \alpha^{n-1}$ com o discriminante clássico de seu polinômio característico:

Proposição 5.3. *Seja $\alpha \in L$ qualquer. Então temos:*

$$\Delta_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\sigma_j(\alpha) - \sigma_i(\alpha))^2 = \Delta(F_{\alpha, L/K})$$

Demonstração. Pela Proposição 5.2, temos

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = [\det(\sigma_i(\alpha^{j-1}))]^2 = [\det(\sigma_i(\alpha)^{j-1})]^2.$$

Mas a matriz $(\sigma_i(\alpha)^{j-1})$ é uma matriz de Vandermonde, logo seu determinante é

$$\det(\sigma_i(\alpha)^{j-1}) = \prod_{1 \leq i < j \leq n} (\sigma_j(\alpha) - \sigma_i(\alpha)).$$

Disso segue a primeira igualdade. Por outro lado, a igualdade

$$\prod_{1 \leq i < j \leq n} (\sigma_j(\alpha) - \sigma_i(\alpha))^2 = \Delta(F_\alpha)$$

segue diretamente do Teorema 2.8 e da definição do discriminante de um polinômio. □

Teorema 5.4. *Sejam $\beta_1, \ldots, \beta_n \in L$. Então $\Delta_{L/K}(\beta_1, \ldots, \beta_n) \neq 0$ se e só se $\{\beta_1, \ldots, \beta_n\}$ for uma base de L/K.*

Demonstração. Tomemos $\alpha \in L$ elemento primitivo da extensão L/K. Então cada isomorfismo σ de L em Ω que fixa K é determinado inteiramente por α. Portanto, sendo $\sigma_1, \ldots, \sigma_n$ os n isomorfismos de L em Ω que fixam K distintos, temos para $1 \leq i < j \leq n$ que $\sigma_i(\alpha) \neq \sigma_j(\alpha)$. Isso mostra, pela Proposição 5.3, que $\Delta(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$.

Como $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de L/K, podemos escrever para $1 \leq i \leq n$:

$$\beta_i = \sum_{j=1}^{n} b_{ij}\alpha^{j-1}, \text{ com } b_{i1}, \ldots, b_{in} \in K.$$

Segue da álgebra linear que $\{\beta_1, \ldots, \beta_n\}$ será uma base de L/K se e só se $\det(b_{ij}) \neq 0$. Pela Proposição 5.1, temos

$$\Delta(\beta_1, \ldots, \beta_n) = [\det(b_{ij})]^2 \Delta(1, \alpha, \ldots, \alpha^{n-1}),$$

logo o resultado segue. □

Lema 5.5. *Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de L/K. Para quaisquer $c_1, \ldots, c_n \in K$, existe um único $\alpha \in L$ que satisfaça $\mathrm{Tr}_{L/K}(\beta_i\alpha) = c_i$, para todo i inteiro, $1 \leq i \leq n$.*

Demonstração. Seja $\alpha = \sum_{j=1}^{n} a_j\beta_j$. Então, para $1 \leq i \leq n$, temos:

$$\beta_i\alpha = \sum_{j=1}^{n} a_j\beta_i\beta_j \Rightarrow \mathrm{Tr}(\beta_i\alpha) = \sum_{j=1}^{n} a_j \,\mathrm{Tr}(\beta_i\beta_j).$$

Assim, procuramos $a_1, \ldots, a_n$ tais que

$$\begin{bmatrix} \mathrm{Tr}(\beta_1^2) & \mathrm{Tr}(\beta_1\beta_2) & \ldots & \mathrm{Tr}(\beta_1\beta_n) \\ \mathrm{Tr}(\beta_2\beta_1) & \mathrm{Tr}(\beta_2^2) & \ldots & \mathrm{Tr}(\beta_2\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\beta_n\beta_1) & \mathrm{Tr}(\beta_n\beta_2) & \ldots & \mathrm{Tr}(\beta_n^2) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}.$$

Como $\det(\mathrm{Tr}(\beta_i\beta_j)) = \Delta(\beta_1, \ldots, \beta_n) \neq 0$ pelo Teorema 5.4, o sistema acima tem uma única solução $(a_1, \ldots, a_n) \in K^n$, o que mostra que existe um único $\alpha \in L$ satisfazendo as condições do enunciado. □

Teorema 5.6. *Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de L/K. Então existe uma única base (que é chamada de **base dual** da base $\{\beta_1, \ldots, \beta_n\}$) $\{\beta_1', \ldots, \beta_n'\}$ de L/K tal que, para todos i, j inteiros com $1 \leq i, j \leq n$, vale $\mathrm{Tr}(\beta_i\beta_j') = \delta_{ij}$. Além disso, para todo $\alpha \in L$ temos:*

$$\alpha = \sum_{j=1}^{n} \mathrm{Tr}_{L/K}(\beta_j\alpha)\beta_j'.$$

Demonstração. Para cada j, temos que existe um único $\beta_j' \in L$ que satisfaz as condições acima, pelo Lema 5.5. Seja agora $\alpha = \sum_{j=1}^{n} a_j\beta_j'$. Então, para $1 \leq i \leq n$, temos:

$$\mathrm{Tr}(\beta_i\alpha) = \sum_{j=1}^{n} a_j \,\mathrm{Tr}(\beta_i\beta_j') = \sum_{j=1}^{n} a_j\delta_{ij} = a_i.$$

Assim, temos

$$\alpha = \sum_{j=1}^{n} \mathrm{Tr}(\beta_j\alpha)\beta_j'.$$

Em particular, se $\alpha = 0$, temos $a_1 = a_2 = \cdots = a_n = 0$, logo $\{\beta_1', \ldots, \beta_n'\}$ é um conjunto LI e portanto uma base de L/K. Assim, todo $\alpha \in L$ pode ser escrito na forma acima. □

Suponhamos a partir de agora que R seja um domínio integralmente fechado, $K = Q(R)$ e L uma extensão finita e separável de K de grau n. Se $\{\gamma_1, \ldots, \gamma_n\}$ for uma base de L/K, então é claro que para todo $d \in R \setminus \{0\}$ o conjunto $\{d\gamma_1, \ldots, d\gamma_n\}$ é também uma base de L/K. Pelo Teorema 3.8, $L = (I_L(R))_{R\setminus\{0\}}$. Assim, podemos tomar d de forma que cada $d\gamma_i$ esteja em $I_L(R)$. Isso mostra que podemos tomar uma base $\{\beta_1, \ldots, \beta_n\}$ de L/K com $\beta_1, \ldots, \beta_n \in I_L(R)$.

Teorema 5.7. *Suponhamos que $\beta_1, \ldots, \beta_n \in I_L(R)$ formem uma base de L/K, e que $\{\beta'_1, \ldots, \beta'_n\}$ seja sua base dual. Então $I_L(R)$ está entre dois R-módulos livres de posto n:*

$$\langle \beta_1, \ldots, \beta_n \rangle_R \subseteq I_L(R) \subseteq \langle \beta'_1, \ldots, \beta'_n \rangle_R.$$

Demonstração. $\beta_1, \ldots, \beta_n$ e $\beta'_1, \ldots, \beta'_n$ são conjuntos LI sobre $K = Q(R)$, logo também são LI sobre R. Isso mostra que os módulos indicados são de fato R-módulos livres de posto n.

Como cada $\beta_i \in I_L(R)$, é claro que $\langle \beta_1, \ldots, \beta_n \rangle_R \subseteq I_L(R)$. Por outro lado, se $\alpha \in I_L(R)$, temos, para $1 \leq j \leq n$, $\beta_j \alpha \in I_L(R)$. Então, pelo item a) do Corolário 3.11, temos $\mathrm{Tr}(\beta_j \alpha) \in R$. Assim, pelo Teorema 5.6, nós temos

$$\alpha = \sum_{j=1}^{n} \mathrm{Tr}(\beta_j \alpha) \beta'_j \in \langle \beta'_1, \ldots, \beta'_n \rangle_R,$$

concluindo a prova. □

Esse teorema, junto com o teorema sobre módulos livres sobre DIP's que será demonstrado na próxima seção, é suficiente para garantir que $I_L(R)$ é um R-módulo livre de posto n.

Proposição 5.8. *Seja S um anel tal que $R \subseteq S \subseteq I_L(R)$. Para quaisquer $\alpha_1, \ldots, \alpha_n \in S$, temos*

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) \in R.$$

Demonstração. Segue diretamente da definição do discriminante de uma n-upla e do Corolário 3.11 que

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)) \in R.$$

□

Esse resultado nos garante que a definição a seguir faz sentido:

Definição (Ideal discriminante)**.** Seja S um anel tal que $R \subseteq S \subseteq I_L(R)$. Então o **ideal discriminante** de S/R, denotado $\mathfrak{D}_{S/R}$, é o ideal de R gerado pelos elementos da forma $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n)$, onde $\alpha_1, \ldots, \alpha_n$ percorrem todos os elementos de S.

Proposição 5.9. *Seja S um anel tal que $R \subseteq S \subseteq I_L(R)$, e suponhamos que S seja um R-módulo livre com base $\beta_1, \ldots, \beta_n$. Então:*

a) $\mathfrak{D}_{S/R}$ é um ideal principal, gerado por $\Delta_{L/K}(\beta_1, \ldots, \beta_n)$. Além disso, para quaisquer $\alpha_1, \ldots, \alpha_n \in S$, temos:

b) $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = a^2 \Delta_{L/K}(\beta_1, \ldots, \beta_n)$, para algum $a \in R$.

c) $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de S como R-módulo se, e só se, $a \in U(R)$.

Demonstração. Escrevamos, para cada i, $\alpha_i = \sum_{j=1}^{n} a_{ij} \beta_j$, com cada $a_{ij} \in R$. Então pela Proposição 5.1 temos $\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = a^2 \Delta_{L/K}(\beta_1, \ldots, \beta_n)$, para $a = \det(a_{ij}) \in R$. Isso prova a) e b). Para provar c), notemos que $\alpha_1, \ldots, \alpha_n$ será uma base de S se e só se a matriz (a_{ij}) for inversível, ou seja, se e só se $a \in U(R)$. □

$\mathbb{Z}$eorema 5.10. *Seja $S \subseteq I_L$ um anel que é um $\mathbb{Z}$-módulo livre de posto n. Então existe $d_L(S)$ tal que, para toda base $\{\beta_1, \ldots, \beta_n\}$ de S temos $\Delta_{L/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = d_L(S)$.*

Demonstração. Sejam $\{\beta_1, \ldots, \beta_n\}$ e $\{\alpha_1, \ldots, \alpha_n\}$ duas bases de S como $\mathbb{Z}$-módulo. Então pelos itens b) e c) da Proposição 5.9, existe $a \in \{1, -1\}$ tal que

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = a^2 \Delta_{L/K}(\beta_1, \ldots, \beta_n).$$

Mas $a^2 = 1$, logo

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = \Delta_{L/K}(\beta_1, \ldots, \beta_n).$$

Assim, basta definir $d_L(S)$ como o discriminante de qualquer base de S. □

Como veremos, I_L é um $\mathbb{Z}$-módulo livre de posto n, e portanto o $\mathbb{Z}$eorema acima se aplica a I_L. Assim, na definição abaixo não precisamos do "se".

$\mathbb{Z}$efinição. Se I_L for um $\mathbb{Z}$-módulo livre de posto n, o **discriminante do corpo** L é definido por $d_L(I_L)$, e é denotado simplesmente por d_L.

E$\mathbb{Z}$emplo 2. Seja $L = \mathbb{Q}(\sqrt{d})$ um corpo quadrático. Sabemos que I_L possui uma base integral, dada por $\{1, \sqrt{d}\}$ se $d \equiv 2$ ou $3 \pmod 4$ e $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ se $d \equiv 1 \pmod 4$. Calculemos d_L:

Se $d \equiv 2$ ou $3 \pmod 4$,

$$d_L = \Delta(1, \sqrt{d}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Assim, nesse caso $d_L = 4d$.

Se $d \equiv 1 \pmod 4$,

$$\begin{aligned} d_L = \Delta\Big(1, \frac{1+\sqrt{d}}{2}\Big) &= \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) \\ \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) & \mathrm{Tr}\left(\frac{1+d+2\sqrt{d}}{4}\right) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d. \end{aligned}$$

Assim, nesse caso, $d_L = d$.

Note ainda que podemos encontrar todas as bases integrais de I_L usando o discriminante: Se $\alpha, \beta \in I_L$, então $\{\alpha, \beta\}$ será uma base de I_L se e só se $\Delta(\alpha, \beta) = 4d$, se $d \equiv 2$ ou $3 \pmod 4$, e se e só se $\Delta(\alpha, \beta) = d$, se $d \equiv 1 \pmod 4$.

6. Módulos Livres sobre DIP's e o Teorema da Base Integral

O principal objetivo dessa seção é provar que o submódulo de um módulo livre finitamente gerado sobre um DIP também é livre. Como consequência imediata deste resultado, vê-se que $I_L(R)$ será um R-módulo livre se fizermos hipóteses suficientes sobre R e L. Deste teorema sai ainda um corolário que nos será importante posteriormente. Em toda esta seção, R denotará um domínio e $K = Q(R)$ seu corpo de frações. Comecemos com uma definição:

Definição (Posto de um módulo sobre um domínio)**.** Seja M um R-módulo. Então o **posto** de M é a cardinalidade máxima de um conjunto linearmente independente de elementos de M. Equivalentemente, o posto de M é a dimensão do K-espaço vetorial $M_K = K \otimes_R M \cong M_{R\setminus\{0\}}$.

As duas definições dadas são equivalentes, devido à Proposição 3.2.

Observação. É claro que, se $N \subseteq M$ são R-módulos, então o posto de N é menor ou igual ao posto de M.

Mostraremos agora que, para módulos livres finitamente gerados, a definição acima equivale à noção usual de posto:

Proposição 6.1. *Um R-módulo livre M é isomorfo a R^n se e só se M tem posto n (no sentido da definição acima).*

Demonstração. ($\Rightarrow$) Suponhamos $M \cong R^n$. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base de M. Então esse conjunto é LI sobre R, e portanto o conjunto correspondente $\left\{\frac{\beta_1}{1}, \ldots, \frac{\beta_n}{1}\right\} \subseteq M_K$ é LI sobre $K = Q(R)$. Por outro lado, é claro que $\left\{\frac{\beta_1}{1}, \ldots, \frac{\beta_n}{1}\right\}$ gera M_K e portanto M_K é um espaço vetorial de dimensão n. Logo M tem posto n.

($\Leftarrow$) Suponhamos que o posto de M seja n, e seja B uma base de M. Como B é um conjunto LI, temos $|B| \leq n$. Em particular, B é finito, digamos $|B| = m$. Então $M \cong R^m$. Por ($\Rightarrow$), M tem posto m. Logo $m = n$, o que mostra que $M \cong R^n$. □

Exemplo 4. Seja I um ideal não-nulo de R. Tomemos $i \in I \setminus \{0\}$. Então $I_K \subseteq R_K = K$. Por outro lado, dado $\frac{a}{b} \in K$ com $a, b \in R$ e $b \neq 0$, temos $\frac{a}{b} = \frac{ai}{bi} \in I_K$. Isso mostra que $I_K = K$ (com as devidas identificações), logo I é um R-módulo de dimensão 1.

Suponhamos que R tenha a propriedade de que qualquer submódulo de um R-módulo livre também seja livre. Como R é um R-módulo livre, isso significa em particular que todo ideal não-nulo I de R seja livre. Nesse caso, pelo exemplo acima, I necessariamente tem que ser livre de posto 1, e portanto é gerado por um de seus elementos. Ou seja, I é um ideal principal. Sendo 0 obviamente principal, isso mostra que um R que satisfaça essas condições precisa ser um DIP. O seguinte teorema mostra que essa hipótese também é suficiente:

Teorema 6.2. *Seja R um DIP, M um R-módulo livre de posto n e M' um submódulo de M de posto q, com $q \leq n$. Então:*

a) M' é um R-módulo livre.

b) Existem uma base $\{\beta_1, \ldots, \beta_n\}$ de M e elementos $a_1, \ldots, a_q \in R$ tais que $a_1 \mid a_2 \mid \cdots \mid a_q$ e $\{a_1\beta_1, \ldots, a_q\beta_q\}$ é uma base de M'.

Demonstração. Provaremos o resultado por indução em q. Se $q = 0$, $M' = 0$ e o resultado é claro. Se um submódulo de M tiver posto 1, ele é da forma $\langle m \rangle$ para algum $m \in M$ não-nulo (isso é verdade porque M é Noetheriano). Como $(\langle m \rangle)_K$ é um espaço gerado por $m/1$, queremos mostrar que $m/1 \neq 0$. Então para mostrar que $\langle m \rangle$ tem posto 1, basta mostrar que para todo $r \in R \setminus \{0\}$ temos $rm \neq 0$. Suponhamos então que $rm \in R$ seja tal que $rm = 0$. Seja $B = \{\gamma_1 \ldots, \gamma_n\}$ uma base de M. Então podemos escrever

$$m = \sum_{j=1}^{n} m_j \gamma_j, \text{ onde } m_1, \ldots, m_n \in R.$$

Assim, $0 = rm = \sum_{j=1}^{n} rm_j\gamma_j$. Como os γ_j são LI, temos $rm_1 = \cdots = rm_n = 0$. Como $m \neq 0$, pelo menos algum dos m_j é diferente de 0, e como R é domínio concluímos que $r = 0$. Assim, o resultado vale também para $q = 1$.

Suponhamos que o resultado valha para todos os submódulos de M de posto $q - 1$, e que o posto de M' é q, com $2 \leq q \leq n$. Consideremos $\mathrm{Hom}_R(M, R)$. Para todo $\psi \in \mathrm{Hom}_R(M, R)$, o conjunto $\psi(M')$ é um ideal de R. Assim, o conjunto $\Lambda = \{\psi(M') \mid \psi \in \mathrm{Hom}_R(M, R)\}$ é um conjunto de ideais de R. Como $0 \lhd R$ é a imagem do homomorfismo nulo, $0 \in \Lambda$, logo $\Lambda \neq \emptyset$. Como R é Noetheriano, esse conjunto tem um elemento maximal $\varphi(M')$, onde $\varphi \in \mathrm{Hom}_R(M, R)$. Então temos $\varphi(M') = \langle a \rangle$, para algum $a \in R$. Em particular, $a = \varphi(\beta')$ para algum $\beta' \in M'$. Mostraremos que $a \neq 0$:

Para $1 \leq j \leq n$, seja $\pi_j \in \mathrm{Hom}_R(M, R)$ a projeção na j-ésima coordenada com respeito à base B. Como $M' \neq 0$, existe um $m' \in M' \setminus \{0\}$, e podemos escrevê-lo como

$$m' = \sum_{j=1}^{n} m'_j \gamma_j, \text{ onde } m'_1, \ldots, m'_n \in R.$$

Como $m' \neq 0$, temos $m'_k \neq 0$ para algum $k \in \{1, \ldots, n\}$, e portanto $\pi_k(M') \ni \pi_k(m') = m'_k \neq 0$. Como $\varphi(M') = \langle a \rangle$ é maximal em Λ, vemos que $a \neq 0$. Em particular, $\beta' \neq 0$. Afirmamos agora que a divide $\psi(\beta')$ para todo $\psi \in \mathrm{Hom}_R(M, R)$. De fato, fixemos um tal ψ, e consideremos o ideal $\langle a, \psi(\beta') \rangle$. Como R é DIP, temos $\langle a, \psi(\beta') \rangle = \langle d \rangle$ para algum $d \in R$. Logo d é da forma $d = ra + s\psi(\beta') = r\varphi(\beta') + s\psi(\beta')$, onde $r, s \in R$. Consideremos então $r\varphi + s\psi \in \mathrm{Hom}_R(M, R)$. Temos

$$\langle a \rangle \subseteq \langle a, \psi(\beta') \rangle = \langle d \rangle = \langle (r\varphi + s\psi)(\beta') \rangle \subseteq (r\varphi + s\psi)(M') \in \Lambda.$$

Devido à maximalidade de $\langle a\rangle$ em Λ, todas as continências acima são igualdades. Em particular, $a \mid \psi(\beta')$, como gostaríamos. Tomando $\psi = \pi_j$ para $1 \leq j \leq n$, o que fizemos garante que $a \mid \pi_j(\beta')$, e assim temos $\pi_j(\beta') = a\beta'_j$ para algum $\beta'_j \in R$. Definamos $\beta = \sum_{j=1}^n \beta'_j\gamma_j$. Então

$$a\beta = \sum_{j=1}^n a\beta'_j\gamma_j = \sum_{j=1}^n \pi_j(\beta')\gamma_j = \beta'.$$

Além disso, $a = \varphi(\beta') = \varphi(a\beta) = a\varphi(\beta)$. Como R é um domínio, segue que $\varphi(\beta) = 1$. O próximo passo é mostrar que $M = \ker\ \varphi \oplus \langle\beta\rangle$ (soma direta interna). Primeiramente, um elemento em $\ker\ \varphi \cap \langle\beta\rangle$ é da forma $t\beta$ para algum $t \in R$. Então

$$0 = \varphi(t\beta) = t\varphi(\beta) = t \cdot 1 = t \Rightarrow t\beta = 0.$$

Logo $\ker\ \varphi \cap \langle\beta\rangle = \{0\}$. Por outro lado, seja $x \in M$ qualquer. Então $x = (x - \varphi(x)\beta) + \varphi(x)\beta$. Temos

$$\varphi(x - \varphi(x)\beta) = \varphi(x) - \varphi(x)\varphi(\beta) = \varphi(x) - \varphi(x) = 0,$$

logo $x - \varphi(x)\beta \in \ker\ \varphi$, o que mostra que $x \in \ker\ \varphi + \langle\beta\rangle$, e assim de fato temos $M = \ker\ \varphi \oplus \langle\beta\rangle$. Isso por sua vez implica que $M' = (M' \cap \ker\ \varphi) \oplus \langle\beta'\rangle$. Com efeito,

$$(M' \cap \ker\ \varphi) \cap \langle\beta'\rangle \subseteq \ker\ \varphi \cap \langle\beta\rangle = \{0\}.$$

Além disso, similarmente ao que fizemos acima, dado $x \in M'$ temos $x = (x - \varphi(x)\beta) + \varphi(x)\beta$,
com $x - \varphi(x)\beta \in \ker\ \varphi$. Mas

$$\varphi(x)\beta \subseteq \varphi(M')\beta = \langle a\rangle\beta = \langle a\beta\rangle = \langle\beta'\rangle \subseteq M',$$

e também temos $x - \varphi(x)\beta \in M'$. Assim, $x \in (M' \cap \ker\ \varphi) + \langle\beta'\rangle$, e realmente vale $M' = (M' \cap \ker\ \varphi) \oplus \langle\beta'\rangle$. Notemos agora que temos:

$$\begin{aligned} M'_K = K \otimes_R M' &= K \otimes_R ((M' \cap \ker\ \varphi) \oplus \langle\beta'\rangle) \\ &\cong K \otimes_R (M' \cap \ker\ \varphi) \oplus K \otimes_R \langle\beta'\rangle \\ &= (M' \cap \ker\ \varphi)_K \oplus (\langle\beta'\rangle)_K. \end{aligned}$$

Como $\beta' \neq 0$, pelo que já vimos $\langle\beta'\rangle$ é um R-módulo livre de posto 1, logo $(\langle\beta'\rangle)_K$ é um K-espaço de dimensão 1. Então $(M' \cap \ker\ \varphi)_K$ tem dimensão $q-1$, já que M'_K tem dimensão q. Concluímos que $M' \cap \ker\ \varphi$ é um R-módulo de posto $q-1$, e segue da hipótese de indução que ele é um R-módulo livre. Consequentemente, $M' = (M' \cap \ker\ \varphi) \oplus \langle\beta'\rangle$ é um R-módulo livre de posto q.

b) A prova será por indução em n. Para $n = 0$, o resultado é trivial. Então tomemos $n > 0$ e suponhamos por indução que, para todo R-módulo livre N de posto $n-1$ e todo submódulo N' de N de posto p, exista uma base $\{\varepsilon_1, \ldots, \varepsilon_n\}$ de N e elementos $r_1, \ldots, r_p$ de R tais que $r_1 \mid r_2 \mid \cdots \mid r_p$ e $\{r_1\,\varepsilon_1, \ldots, r_p\,\varepsilon_p\}$ seja uma base de N'.

Utilizemos a mesma notação que usamos no item *a*). Então $\ker\ \varphi \subseteq M$ é livre, pelo item *a*), e como $M = \ker\ \varphi \oplus \langle\beta\rangle$, temos $M_k = (\ker\ \varphi)_K \oplus (\langle\beta\rangle)_K$. Sabemos que M_k tem dimensão n e $(\langle\beta\rangle)_K$ tem dimensão 1, logo $(\ker\ \varphi)_K$ tem dimensão $n-1$, ou seja, $\ker\ \varphi$ tem posto $n-1$. Além disso, já vimos no item *a*) que $M' \cap \ker\ \varphi$ tem posto $q-1$.

Aplicando a hipótese de indução para $N = \ker\ \varphi$ e $N' = M' \cap \ker\ \varphi$, garantimos a existência de uma base $\{\beta_2, \ldots, \beta_n\}$ de $\ker\ \varphi$ e de elementos $a_2, \ldots, a_q \in R$ tais que $a_2 \mid a_3 \cdots \mid a_q$ e que $\{a_2\beta_2, \ldots, a_q\beta_q\}$ seja uma base de $M' \cap \ker\ \varphi$. Como $M = \ker\ \varphi \oplus \langle\beta\rangle$ e $M' = (M' \cap \ker\ \varphi) \oplus \langle\beta'\rangle$, vemos que $\{\beta, \beta_2, \ldots, \beta_n\}$ é uma base de M e que $\{a\beta, a_2\beta_2, \ldots, a_n\beta_n\}$ é uma base de M' (lembremos que $\beta' = a\beta$). Tomaremos então $\beta_1 = \beta$ e $a_1 = a$. Só falta provarmos que $a_1 = a$ divide a_2. Seja

$$\begin{array}{rccc} \rho: & M & \longrightarrow & R \\ & \sum_{j=1}^n m_j\beta_j & \longmapsto & m_1 + m_2 \end{array}.$$

Então é claro que $\rho \in \mathrm{Hom}_R(M, R)$. Temos ainda $\rho(\beta') = \rho(a\beta) = a$,
e portanto $\langle a\rangle \subseteq \rho(M') \in \Lambda \Rightarrow \langle a\rangle = \rho(M')$, pois $\langle a\rangle$ é maximal em Λ. Concluímos finalmente que

$$a_2 = \rho(a_2\beta_2) \in \rho(M') = \langle a\rangle \Rightarrow a_1 = a \mid a_2,$$

o que completa a demonstração. □

Assim, temos:

Teorema 6.3. *Seja R um domínio integralmente fechado e L uma extensão separável de $K = Q(R)$, de grau n. Então:*

a) $I_L(R)$ é um R-módulo de posto n.

b) Se R for um domínio principal, então para um anel intermediário $R \subseteq S \subseteq L$, são equivalentes:

(i) $S \subseteq I_L(R)$.

(ii) S é um R-módulo livre de posto $q \leq n$.

(iii) S é um R-módulo finitamente gerado.

Em particular, $I_L(R)$ é um R-módulo livre de posto n.

Demonstração. *a*) Segue diretamente do Teorema 5.7, que mostra que I_L está entre dois R-módulos livres de posto n.

b) (i) $\Rightarrow$(ii): Pelo Teorema 6.2 e pelo Teorema 5.7, $I_L(R)$ é um R-módulo livre de posto n. Assim, se S for um anel entre R e L, S será um submódulo de $I_L(R)$, sendo portanto livre pelo Teorema 6.2, de posto no máximo n já que $I_L(R)$ tem posto n pelo item a).

(ii)$\Rightarrow$(iii): Sendo S um R-módulo livre de posto finito, ele é finitamente gerado.

(iii)$\Rightarrow$(i): Segue diretamente do Corolário 3.5. □

E, finalmente:

$\mathbb{Z}$eorema 6.4 (Teorema da Base Integral)**.** *Seja $[L : \mathbb{Q}] = n$. Então I_L é um $\mathbb{Z}$-módulo livre de posto n. Ou seja, todo corpo de números algébricos possui uma base integral.*

Para fechar a seção, provaremos um corolário direto do Teorema 6.2, e que usaremos mais adiante:

Corolário 6.5. *Com as notações do Teorema 6.2, temos um isomorfismo de R-módulos:*

$$M/M' \cong R/\langle a_1\rangle \times \cdots \times R/\langle a_q\rangle \times \underbrace{R \times \cdots \times R}_{n-q \text{ vezes}}.$$

Demonstração. A função

$$\begin{array}{rccc} f: & R^n & \longrightarrow & M/M' \\ & (r_1,\ldots,r_n) & \longmapsto & \sum_{j=1}^n r_j\beta_j + M' \end{array}$$

é um homomorfismo sobrejetor de R-módulos. Além disso,

$$(r_1,\ldots,r_n) \in \ker\ f \iff \sum_{j=1}^n r_j\beta_j \in M'.$$

Como $\{a_1\beta_1,\ldots,a_q\beta_q\}$ é uma base de M', pela indepedência linear dos β_j concluímos que

$$(r_1,\ldots,r_n) \in \ker\ f \iff a_1 \mid r_1,\ldots,a_q \mid r_q \text{ e } a_{q+1} = \cdots = a_n = 0,$$

o que mostra que

$$\ker\ f = \langle a_1\rangle \times \cdots \times \langle a_q\rangle \times \underbrace{\{0\} \times \cdots \times \{0\}}_{n-q \text{ vezes}}.$$

Assim:

$$\begin{aligned} M/M' = \text{im}\ f \cong \frac{R^n}{\ker\ f} &= \frac{R^n}{\langle a_1\rangle \times \cdots \times \langle a_q\rangle \times \underbrace{\{0\} \times \cdots \times \{0\}}_{n-q \text{ vezes}}} \\ &\cong R/\langle a_1\rangle \times \cdots \times R/\langle a_q\rangle \times \underbrace{R \times \cdots \times R}_{n-q \text{ vezes}}. \end{aligned}$$

□

7. Domínios de Dedekind

Uma vez provado que todo anel de inteiros algébricos possui uma base integral, podemos avançar ainda mais a teoria. Nesta seção, utilizaremos resultados sobre domínios de Dedekind para mostrar que, ainda que não haja a unicidade da fatoração para os elementos de I_L, vale um teorema de unicidade da fatoração para objetos um pouco diferentes: os ideais de I_L. Terminaremos a seção definindo o número de classes h_L de um corpo de números algébricos L. Como foi dito na introdução, o número h_L dá uma ideia do quão perto o anel de inteiros algébricos I_L está de ser um DIP. Para começar, definamos o que é um domínio de Dedekind:

Definição (Domínio de Dedekind)**.** Seja R um domínio. Então R é chamado de **domínio de Dedekind** se R for integralmente fechado, Noetheriano e todo ideal primo não-nulo de R for maximal.

O seguinte teorema diz que a propriedade de um anel ser um domínio de Dedekind é preservada em certos tipos de extensões:

Teorema 7.1. *Seja R um domínio de Dedekind e L uma extensão finita e separável de $K = Q(R)$. Então $I_L(R)$ é um domínio de Dedekind.*

Demonstração. Temos $Q(I_L(R)) = L$, pelo Teorema 3.8. Além disso, $I_L(I_L(R)) = I_L(R)$, pelo Corolário 3.6. Logo $I_L(R)$ é integralmente fechado.

Pelo Teorema 5.7, $I_L(R)$ é submódulo de um módulo livre de posto finito. Como um módulo livre de posto finito sobre um anel Noetheriano é Noetheriano e como todo submódulo de um módulo Noetheriano é Noetheriano, concluímos que $I_L(R)$ é um R-módulo Noetheriano. Mas todo ideal de $I_L(R)$ é também um R-submódulo de $I_L(R)$. Isso mostra que $I_L(R)$ é um anel Noetheriano.

Finalmente, todo ideal primo não-nulo de $I_L(R)$ é maximal, pelo item d) do Teorema 3.13. □

ℤeorema 7.2. *Seja L um corpo de números algébricos. Então I_L é um domínio de Dedekind.*

Seja R um domínio e $K = Q(R)$ seu corpo de frações. Então podemos ver K como R-módulo com a multiplicação de K.

Definição (Ideal fracionário)**.** Dizemos que um submódulo $M \subseteq K$ é um **ideal fracionário** de R se existir $d \in R \setminus \{0\}$ tal que $dM \subseteq R$.

Nesse caso, é fácil ver que dM será um ideal $\mathfrak{a}$ de R, de modo que $M = d^{-1}\mathfrak{a}$.

Notação. Indicaremos o conjunto dos ideais fracionários não-nulos de R por $\mathscr{F}$, o conjunto dos ideais não-nulos de R por $\mathscr{J}$ e o conjunto dos ideais primos não-nulos de R por $\mathscr{P}$.

Munindo $\mathscr{F}$ com a operação de multiplicação de R-módulos, vemos que $\mathscr{F}$ é um monóide comutativo, que tem R como unidade.

Definição (Ideal fracionário inversível)**.** Dizemos que um $M \in \mathscr{F}$ é **inversível** se existir $N \in \mathscr{F}$ tal que $MN = R$. Como $\mathscr{F}$ é um monoide comutativo, nesse caso tal N será único, e é denotado M^{-1}.

Proposição 7.3. *Seja $x \in K \setminus \{0\}$. Então o submódulo $\langle x \rangle_R \subseteq K$ é um ideal fracionário de R. Além disso, dado $y \in K \setminus \{0\}$, temos $\langle x \rangle_R \langle y \rangle_R = \langle xy \rangle_R$. Em particular, $\langle x \rangle_R$ é inversível, com inverso $\langle x^{-1} \rangle_R$.*

Demonstração. É claro que $\langle x \rangle_R \langle y \rangle_R = \langle xy \rangle_R$, de onde segue também a última afirmação. Chamando $x = r/s$, onde $r, s \in R$, $s \neq 0$, temos $sx = r \in R$, e portanto $s\langle x \rangle_R \in R$. Isso mostra que $\langle x \rangle_R$ é um ideal fracionário de R. □

Essa proposição mostra que a seguinte definição faz sentido:

Definição (Ideal fracionário principal)**.** Chamaremos um ideal fracionário de R de **principal** se ele for da forma $\langle x \rangle_R$, para $x \in K \setminus \{0\}$. O conjunto dos ideais fracionários principais de R forma um grupo, que será denotado $\mathscr{H}$.

Usaremos sem demonstração os seguintes resultados sobre domínios de Dedekind:

Teorema 7.4 (Fatoração única dos ideais em domínios de Dedekind)**.** *Seja R um domínio de Dedekind. Então $\mathscr{F}$ é um grupo, e:*

a) Todo ideal $\mathfrak{a} \in \mathscr{J}$ se escreve de modo único na forma

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{k_i}, \text{ com } \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathscr{P}, k_1, \ldots, k_n \in \mathbb{N}.$$

b) Todo ideal fracionário $M \in \mathscr{F}$ se escreve de modo único na forma

$$M = \prod_{i=1}^{n} \mathfrak{p}_i^{k_i}, \text{ com } \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathscr{P}, k_1, \ldots, k_n \in \mathbb{Z}.$$

Podemos, de forma similar ao que fazemos com os inteiros, definir uma relação de divisibilidade em $\mathscr{F}$:

Definição (Divisibilidade em $\mathscr{F}$)**.** Sejam $M, N \in \mathscr{F}$. Então dizemos que M **divide** N, ou ainda que N é um **múltiplo** de M, se $N = \mathfrak{a}M$ para algum $\mathfrak{a} \in \mathscr{J}$. Denotamos $M \mid N$.

Essa definição, juntamente com o Teorema 7.4, nos dá um resultado bastante similar ao que acontece com os DFU's:

Corolário 7.5. *Seja R um domínio de Dedekind, e sejam*

$$M = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}, N = \mathfrak{p}_1^{\ell_1} \cdots \mathfrak{p}_r^{\ell_r},$$

onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathscr{P}, k_1, \ldots, k_r, \ell_1, \ldots, \ell_r \in \mathbb{Z}$. Então:

a) $M \supseteq N \iff M \mid N \iff k_1 \leq \ell_1, \ldots, k_r \leq \ell_r$.

b) $M + N = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$, onde para $1 \leq j \leq r$ temos $m_j = \min\{k_j, \ell_j\}$.

c) $M \cap N = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$, onde para $1 \leq j \leq r$ temos $n_j = \max\{k_j, \ell_j\}$.

d) $MN = \mathfrak{p}_1^{k_1+\ell_1} \cdots \mathfrak{p}_r^{k_r+\ell_r}$.

Ainda utilizaremos o seguinte resultado que diz respeito a relações entre ideais em domínios de Dedekind:

Corolário 7.6. *Seja R um domínio de Dedekind. Então:*

a) Para todo $\mathfrak{a} \in \mathscr{J}$, o conjunto dos ideais de R que contêm $\mathfrak{a}$ é finito.

b) Para todo $\mathfrak{a} \in \mathscr{J}$, os ideais $\mathfrak{ap}$, onde $\mathfrak{p}$ percorre $\mathscr{P}$, são os elementos maximais do conjunto dos ideais de R que estão estritamente contidos em $\mathfrak{a}$.

Ainda temos o seguinte teorema:

Teorema 7.7. *Seja R um domínio. Então as seguintes condições são equivalentes:*

(i) R é um DIP.

(ii) R é um DFU e um domínio de Dedekind.

Esse teorema nos permite afirmar, como havíamos comentado, que DIP's e DFU's são a mesma coisa quando tratamos de um anel de inteiros algébricos:

$\mathbb{Z}$eorema 7.8. *Seja L um corpo de números algébricos. Então I_L é um DIP se e só se I_L é um DFU.*

Pelo Teorema 7.4, se R for um domínio de Dedekind então $\mathscr{H}$ é um subgrupo do grupo $\mathscr{F}$. Assim, podemos considerar o grupo quociente $\mathscr{C}\ell := \mathscr{F}/\mathscr{H}$, que é chamado de **grupo de classes de ideais** de R. Esse nome é devido ao seguinte resultado:

Proposição 7.9. *A função* $\begin{array}{rccc}\pi: & \mathscr{J} & \longrightarrow & \mathscr{C}\ell \\ & \mathfrak{a} & \longmapsto & \mathfrak{a}\mathscr{H}\end{array}$ *é uma função sobrejetora, e dados* $\mathfrak{a}, \mathfrak{b} \in \mathscr{J}$*, temos* $\pi(\mathfrak{a}) = \pi(\mathfrak{b})$ *se e só se existirem* $c, d \in R \setminus \{0\}$ *tais que* $c\mathfrak{a} = d\mathfrak{b}$*.*

Demonstração. Dados dois ideais fracionários $M, N \in \mathscr{F}$, temos $M\mathscr{H} = N\mathscr{H} \iff M^{-1}N \in \mathscr{H}$. Isso, por sua vez, acontece se e só se existir um $x \in K \setminus \{0\}$ tal que $M^{-1}N = \langle x \rangle_R$. Escrevendo $x = c/d$, com $c, d \in R \setminus \{0\}$, temos $M^{-1}N = \langle c/d \rangle_R \iff cM = dN$. Em particular, se $M = \mathfrak{a}$ e $N = \mathfrak{b}$ estão em $\mathscr{J}$, obtemos a equivalência desejada. Seja agora $M\mathscr{H} \in \mathscr{C}\ell$ qualquer, com $M \in \mathscr{F}$. Então existe $r \in R \setminus \{0\}$ tal que $rM \in \mathscr{J}$. Mas $r \cdot M = 1 \cdot (rM)$, logo pela equivalência mais geral que mostramos temos $M\mathscr{H} = (rM)\mathscr{H} = \pi(rM) \in \text{im } \pi$, mostrando que π é sobrejetora. □

O fato de π ser sobrejetora mostra que todo elemento de $\mathscr{C}\ell$ é a classe de algum ideal de R, o que justifica chamarmos esse grupo de "grupo das classes de ideais de R".

Definição (Número de classes)**.** O número cardinal $|\mathscr{C}\ell|$ é chamado de o **número de classes** de R, e será denotado por h_R. Se $R = I_L$ for o anel de inteiros algébricos de um corpo L, denotamos h_{I_L} simplesmente por h_L.

Temos imediatamente o seguinte corolário:

Corolário 7.10. *Um domínio de Dedekind* R *será um DIP se e só se o grupo* $\mathscr{C}\ell$ *for trivial, ou seja, se* $h_R = 1$*.*

8. Norma de ideais

Nosso objetivo nessa seção é definir uma função $\mathfrak{N}$ do conjunto de ideais não-nulos de R para os números inteiros positivos que funcione como uma norma. Não à toa, esta função será chamada de "norma de ideais". Mais do que uma simples norma, ela em certo sentido generaliza a norma que já conhecemos, e será fundamental para a demonstração do Teorema da Finitude do Número de Classes.

Proposição 8.1. *Sejam* R *um domínio de Dedekind,* $\mathfrak{m}$ *um ideal maximal de* R *e* $\mathfrak{a}$ *um ideal não-nulo de* R*. Então* $\mathfrak{a}/(\mathfrak{m}\mathfrak{a})$ *é um* $R/\mathfrak{m}$*-espaço vetorial de dimensão* 1*.*

Demonstração. É claro que $\mathfrak{a}/(\mathfrak{m}\mathfrak{a})$ é um $R/\mathfrak{m}$ espaço vetorial, da maneira natural. Do item b) do Corolário 7.6, $\mathfrak{m}\mathfrak{a}$ é um elemento maximal do conjunto dos ideais de R que estão estritamente contidos em $\mathfrak{a}$. Assim, $\mathfrak{a}/(\mathfrak{m}\mathfrak{a}) \neq 0$ é simples como R-módulo. Mas todo $R/\mathfrak{m}$-subespaço vetorial próprio não-nulo de $\mathfrak{a}/(\mathfrak{m}\mathfrak{a})$ pode ser considerado também como um R-submódulo próprio não-nulo desse conjunto, logo concluímos que $\mathfrak{a}/(\mathfrak{m}\mathfrak{a}) \neq 0$ é um $R/\mathfrak{m}$-espaço vetorial simples, e portanto de dimensão 1. □

Note que, no enunciado da proposição acima, "$\mathfrak{m}$ ideal maximal"poderia ser substituído por "$\mathfrak{m}$ ideal primo não-nulo", já que R é um domínio de Dedekind.

Notação. A partir de agora, L denotará um corpo de números algébricos, com $[L : \mathbb{Q}] = n$.

Teorema 8.2. *Seja* $\mathfrak{p}$ *um ideal primo não-nulo de* I_L*. Então:*

a) $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle_{\mathbb{Z}}$*, onde* p *é o único número primo (positivo) no ideal* $\mathfrak{p}$*.*

b) $I_L/\mathfrak{p}$ *é uma extensão finita do corpo* $\mathbb{F}_p$*, de grau* $[I_L/\mathfrak{p} : \mathbb{F}_p] \leq n$*.*

Demonstração. *a*) Sendo $\mathfrak{p} \lhd I_L$ maximal, temos que $\mathfrak{p} \cap \mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, pelo item d) do Teorema 3.13. Então temos $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle_{\mathbb{Z}}$, para algum primo $p \in \mathbb{N}$. Assim, é claro que $p \in \mathfrak{p}$, o que não ocorre para nenhum outro primo positivo em $\mathbb{Z}$.

b) É claro que $I_L/\mathfrak{p}$ é um corpo, pois $\mathfrak{p}$ é maximal. Consideremos a restrição a $\mathbb{Z}$ da projeção canônica de I_L em $I_L/\mathfrak{p}$,

$$\begin{array}{rccc}\varphi: & \mathbb{Z} & \longrightarrow & I_L/\mathfrak{p} \\ & x & \longmapsto & x + \mathfrak{p}\end{array}.$$

Então é claro que $\ker \varphi = \mathfrak{p} \cap \mathbb{Z} = \langle p \rangle_{\mathbb{Z}}$, e portanto temos $\mathbb{Z}/\mathfrak{p} = \varphi(\mathbb{Z}) \cong \mathbb{Z}/\langle p \rangle_{\mathbb{Z}} \cong \mathbb{F}_p$.
Assim, como $\mathbb{Z}/\mathfrak{p} \subseteq I_L/\mathfrak{p}$, podemos enxergar $\mathbb{F}_p$ como o subcorpo $\mathbb{Z}/\mathfrak{p}$ de $I_L/\mathfrak{p}$. Finalmente, seja $\{\beta_1, \ldots, \beta_n\} \subseteq I_L$ uma base integral. Então esse conjunto gera I_L como $\mathbb{Z}$-módulo, e portanto $\{\beta_1 + \mathfrak{p}, \ldots, \beta_n + \mathfrak{p}\} \subseteq I_L/\mathfrak{p}$ gera $I_L/\mathfrak{p}$ como $\mathbb{F}_p$-espaço vetorial. Isso mostra que $[I_L/\mathfrak{p} : \mathbb{F}_p] \leq n$. □

Definição (Grau de inércia)**.** Nas notações do teorema acima, o número inteiro positivo $[I_L/\mathfrak{p} : \mathbb{F}_p]$ é chamado o **grau de inércia** de $\mathfrak{p}$. Denotaremos ainda $[I_L/\mathfrak{p} : \mathbb{F}_p] = f(\mathfrak{p})$.

Finalmente, definimos a desejada norma de ideal:

Definição (Norma de um ideal)**.** Seja $\mathfrak{a}$ um ideal não-nulo de I_L. Definimos a **norma** do ideal $\mathfrak{a}$, que denotaremos $\mathfrak{N}(\mathfrak{a})$, como sendo o número cardinal $|I_L/\mathfrak{a}|$, ou seja, como o número de classes de congruência módulo $\mathfrak{a}$.

Mostraremos que a norma de ideais é sempre finita e, mais do que isso, merece o nome que tem, pois é multiplicativa:

Teorema 8.3. *a) Para todo ideal primo não-nulo $\mathfrak{p}$ de I_L temos $\mathfrak{N}(\mathfrak{p}) = p^{f(\mathfrak{p})}$, onde p é o único número primo em $\mathfrak{p}$.*

b) Para todo ideal não-nulo $\mathfrak{a}$ de I_L, temos que $\mathfrak{N}(\mathfrak{a})$ é um inteiro positivo. Além disso, $\mathfrak{N}(\mathfrak{a}) = 1$ se e só se $\mathfrak{a} = I_L$.

c) Para quaisquer ideais não-nulos $\mathfrak{a}, \mathfrak{b}$ de I_L, temos $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.

Demonstração. a) Temos que $[I_L/\mathfrak{p} : \mathbb{F}_p] = f(\mathfrak{p})$ é um número inteiro positivo, pelo teorema anterior. Portanto temos $\mathfrak{N}(\mathfrak{p}) = |I_L/\mathfrak{p}| = p^{[I_L/\mathfrak{p}:\mathbb{F}_p]} = p^{f(\mathfrak{p})}$.

b) e *c*): Seja $\mathfrak{b}$ um ideal não-nulo de I_L e $\mathfrak{p}$ um ideal primo não-nulo (e portanto maximal) de I_L. Então $\mathfrak{b}/(\mathfrak{bp})$ é um $I_L/\mathfrak{p}$-espaço vetorial de dimensão 1 pela Proposição 8.1, e portanto tem $|I_L/\mathfrak{p}| = \mathfrak{N}(\mathfrak{p})$ elementos. Suponhamos agora que $\mathfrak{N}(\mathfrak{b}) = |I_L/\mathfrak{b}|$ seja finita. Mas nós temos que

$$I_L/\mathfrak{b} \cong \frac{I_L/(\mathfrak{bp})}{\mathfrak{b}/(\mathfrak{bp})}.$$

Assim, $\mathfrak{N}(\mathfrak{bp}) = |I_L/(\mathfrak{bp})|$ é finita, e vale a relação

$$|I_L/\mathfrak{b}| = \frac{|I_L/(\mathfrak{bp})|}{|\mathfrak{b}/(\mathfrak{bp})|} \Rightarrow \mathfrak{N}(\mathfrak{bp}) = \mathfrak{N}(\mathfrak{b})\mathfrak{N}(\mathfrak{p}).$$

Pelo Teorema 7.4, todo ideal não-nulo $\mathfrak{a}$ de I_L é da forma $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ são ideais primos não-nulos de I_L. Então do que fizemos é fácil ver por indução em m que vale a igualdade $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1) \cdots \mathfrak{N}(\mathfrak{p}_m)$, de onde também segue imediatamente a multiplicidade de $\mathfrak{N}$. Finalmente, para todo ideal primo $\mathfrak{p}$, $\mathfrak{N}(\mathfrak{p}) = p^{f(\mathfrak{p})}$ é um múltiplo de p, logo pela fórmula acima o único jeito de termos $\mathfrak{N}(\mathfrak{a}) = 1$ é se $m = 0$, ou seja, se $\mathfrak{a} = I_L$, e é claro que $\mathfrak{N}(I_L) = 1$. □

Com isso, podemos mostrar que a norma de ideais é mais similar ainda à norma de um elemento:

Corolário 8.4. *Seja $\mathfrak{a}$ um ideal não-nulo de I_L. Então:*

a) $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$, ou seja, o ideal $\langle \mathfrak{N}(\mathfrak{a}) \rangle_{I_L}$ é um múltiplo de $\mathfrak{a}$.

b) Se $\mathfrak{N}(\mathfrak{a})$ for um número primo, então $\mathfrak{a}$ será um ideal primo.

c) Se $\mathfrak{a}$ for um múltiplo do ideal $\mathfrak{b}$ e $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})$, então $\mathfrak{a} = \mathfrak{b}$.

Demonstração. a) O grupo $(I_L/\mathfrak{a}, +)$ tem ordem $\mathfrak{N}(\mathfrak{a})$. Assim, $\mathfrak{N}(\mathfrak{a}) \cdot (1 + \mathfrak{a}) = \mathfrak{a}$, o que mostra que $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$.

b) Escrevamos $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, onde $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ são ideais primos não-nulos de I_L. Então, como vimos,

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1) \cdots \mathfrak{N}(\mathfrak{p}_m) = p_1^{f(\mathfrak{p}_1)} \cdots p_m^{f(\mathfrak{p}_m)}, \text{ onde } p_1, \ldots, p_m \in \mathbb{N} \text{ são primos.}$$

Então é claro que $\mathfrak{N}(\mathfrak{a})$ só pode ser prima se $m = 1$, e nesse caso $\mathfrak{a}$ é um ideal primo de I_L.

c) Se $\mathfrak{a}$ for um múltiplo de $\mathfrak{b}$, então existe $\mathfrak{c}$ ideal não-nulo de I_L tal que $\mathfrak{a} = \mathfrak{bc}$. Então temos $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})\mathfrak{N}(\mathfrak{c})$. Como $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})$, concluímos que $\mathfrak{N}(\mathfrak{c}) = 1$, o que nos garante que $\mathfrak{c} = I_L$, e portanto $\mathfrak{a} = \mathfrak{b}$. □

O seguinte corolário será essencial na prova da finitude de h_L:

Corolário 8.5. *Para todo m inteiro positivo, existe somente um número finito de ideais não-nulos $\mathfrak{a}$ de I_L tais que $\mathfrak{N}(\mathfrak{a}) = m$.*

Demonstração. Pelo item *a)* do corolário anterior, $\mathfrak{N}(\mathfrak{a}) = m \Rightarrow \mathfrak{a} \mid \langle m \rangle_{I_L}$. Mas pelo item *a)* do Corolário 7.6, o conjunto dos ideais que dividem $\langle m \rangle_{I_L}$ é finito, o que prova o corolário. □

O seguinte teorema mostra que a norma de ideais, em certo sentido, é na verdade uma extensão do valor absoluto da norma usual! Este teorema, de fato, mistura vários dos conceitos vistos até agora:

Teorema 8.6. *a) Todo ideal não-nulo $\mathfrak{a}$ de I_L é um $\mathbb{Z}$-módulo livre de posto n, e para toda base $\{\alpha_1, \ldots, \alpha_n\}$ deste $\mathbb{Z}$-módulo temos $\Delta_{L/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = (\mathfrak{N}(\mathfrak{a}))^2 d_L$.*

b) Para todo $\alpha \in I_L \setminus \{0\}$, temos $\mathfrak{N}(\langle \alpha \rangle_{I_L}) = |N_{L/\mathbb{Q}}(\alpha)|$.

Demonstração. a) Pelo Teorema 6.4, I_L é um $\mathbb{Z}$-módulo livre de posto n. Assim, $\mathfrak{a} \subseteq I_L$ é um $\mathbb{Z}$-módulo livre de posto $q \leq n$, pelo Teorema 6.2. Ainda por esse teorema, sabemos que existem uma base integral $\{\beta_1, \ldots, \beta_n\}$ de I_L e inteiros $a_1, \ldots, a_q$ com $a_1 \mid a_2 \mid \cdots \mid a_q$ tais que $\{a_1\beta_1, \ldots, a_q\beta_q\}$ é uma base de $\mathfrak{a}$. Pelo Corolário 6.5, temos

$$I_L/\mathfrak{a} \cong \mathbb{Z}/\langle a_1 \rangle_{\mathbb{Z}} \times \cdots \times \mathbb{Z}/\langle a_q \rangle_{\mathbb{Z}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n-q \text{ vezes}}.$$

Como $|I_L/\mathfrak{a}| = \mathfrak{N}(\mathfrak{a})$ é finito, devemos ter $q = n$, e comparando cardinalidades:

$$\mathfrak{N}(\mathfrak{a}) = |I_L/\mathfrak{a}| = |\mathbb{Z}/\langle a_1 \rangle_{\mathbb{Z}}| \times \cdots \times |\mathbb{Z}/\langle a_n \rangle_{\mathbb{Z}}| = |a_1||a_2| \cdots |a_n| = |a_1 a_2 \cdots a_n|.$$

Então, pela Proposição 5.1 temos:

$$\Delta(a_1\beta_1, \ldots, a_n\beta_n) = |a_1 a_2 \cdots a_n|^2 \Delta(\beta_1, \ldots, \beta_n) = (\mathfrak{N}(\mathfrak{a}))^2 d_L.$$

Seja agora $\{\alpha_1, \ldots, \alpha_n\}$ uma base qualquer de $\mathfrak{a}$. Então $(\alpha_1, \ldots, \alpha_n) = T(a_1\beta_1, \ldots, a_n\beta_n)$ para alguma matriz inversível T com coeficientes em $\mathbb{Z}$. Novamente pela Proposição 5.1, temos:

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(T))^2 \Delta(a_1\beta_1, \ldots, a_n\beta_n) = \Delta(a_1\beta_1, \ldots, a_n\beta_n) = (\mathfrak{N}(\mathfrak{a}))^2 d_L,$$

pois toda matriz inversível com coeficientes em $\mathbb{Z}$ tem determinante ± 1.

b) Novamente, seja $B = \{\beta_1, \ldots, \beta_n\}$ uma base integral de I_L. Então $\{\alpha\beta_1, \ldots, \alpha\beta_n\}$ é claramente uma base do ideal $\langle \alpha \rangle_{I_L}$ como $\mathbb{Z}$-módulo. Seja $T_\alpha : L \to L$ o operador $\mathbb{Q}$-linear que leva cada $\beta \in L$ em $\alpha\beta$, e $[T_\alpha]_B$ a matriz desse operador na base B. Então por *a)* e pela Proposição 5.1:

$$\mathfrak{N}(\langle \alpha \rangle_{I_L})^2 d_L = \Delta(\alpha\beta_1, \ldots, \alpha\beta_n) = \Delta([T_\alpha]_B(\beta_1, \ldots, \beta_n)) = \det([T_\alpha]_B)^2 \Delta(\beta_1, \ldots, \beta_n) = (N(\alpha))^2 d_L.$$

Isso nos dá $\mathfrak{N}(\langle \alpha \rangle_{I_L}) = |N(\alpha)|$, como desejado. □

Como consequência desse teorema, temos o seguinte corolário:

Corolário 8.7. *Seja $p \in \mathbb{N}$ um número primo tal que a fatoração de $\langle p \rangle_{I_L}$ em ideais primos seja $\langle p \rangle_{I_L} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$, com todos os expoentes positivos e $\mathfrak{p}_i \neq \mathfrak{p}_j$ para $i \neq j$. Então:*

a) $\mathfrak{p}_1 \ldots, \mathfrak{p}_r$ são os únicos ideais primos de I_L que contêm p.

b) $\sum_{j=1}^{r} k_j f(\mathfrak{p}_j) = n$.

Demonstração. a) Dado um ideal primo $\mathfrak{p}$ de I_L, temos $p \in \mathfrak{p} \iff \mathfrak{p} \mid \langle p \rangle_{I_L}$, e pela unicidade da fatoração obtemos o resultado desejado.

b) Temos $N(p) = p^n$, logo pelo item *b)* do teorema anterior temos $\mathfrak{N}(\langle p \rangle_{I_L}) = |N(p)| = p^n$. Então:

$$p^n = \mathfrak{N}(\langle p \rangle_{I_L}) = \mathfrak{N}(\mathfrak{p}_1)^{k_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{k_r} = (p^{f(\mathfrak{p}_1)})^{k_1} \cdots (p^{f(\mathfrak{p}_r)})^{k_r} = p^{\sum_{j=1}^{r} k_j f(\mathfrak{p}_j)},$$

e portanto $\sum_{j=1}^{r} k_j f(\mathfrak{p}_j) = n$, como queríamos. □

9. O Teorema da Finitude do Número de Classes

Nesta última seção, finalmente provaremos que para todo corpo de números algébricos L o número de classes h_L é finito. Já temos todas as ferramentas necessárias para provar esse fato, e tudo que faltam são dois lemas técnicos, um que relaciona ideais de $\mathscr{J}$ com classes de $\mathscr{C}\ell$, e outro que garante que certo conjunto de inteiros positivos é limitado superiormente, e que no fundo nada mais é do que uma aplicação esperta do Princípio da Casa dos Pombos.

Definamos, para qualquer $\mathfrak{a} \in \mathscr{J}$, o número

$$t(\mathfrak{a}) = \min\{\mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\langle\alpha\rangle_{I_L}) \mid \alpha \in \mathfrak{a} \setminus \{0\}\}.$$

Para qualquer $\alpha \in \mathfrak{a} \setminus \{0\}$, temos que $\mathfrak{a} \mid \langle\alpha\rangle_{I_L}$. Logo, pela multiplicatividade da norma de ideais,

$\mathfrak{N}(\mathfrak{a}) \mid \mathfrak{N}(\langle\alpha\rangle_{I_L})$, o que mostra que $t(\mathfrak{a})$ é o mínimo de um conjunto de inteiros positivos, sendo portanto bem-definido e um inteiro positivo. Além disso, pelo item c) do Corolário 8.4 temos que $t(\mathfrak{a}) = 1$ se e só se $\mathfrak{a} = \langle\alpha\rangle_{I_L}$ para algum $\alpha \in \mathfrak{a} \setminus \{0\}$, ou seja, se e só se $\mathfrak{a} \in \mathscr{H}$.

Por outro lado, dada uma classe $\mathfrak{B} \in \mathscr{C}\ell$, definimos

$$u(\mathfrak{B}) = \min\{\mathfrak{N}(\mathfrak{b}) \mid \mathfrak{b} \in \mathscr{J} \cap \mathfrak{B}\}.$$

Pela Proposição 7.9, a interseção $\mathscr{J} \cap \mathfrak{B}$ é não-vazia, o que mostra que $u(B)$ está bem-definido. Note que $u(B)$ é um inteiro positivo. Temos uma importante relação entre essas duas funções t e u que definimos:

Lema 9.1. *Sejam $\mathfrak{B} \in \mathscr{C}\ell$ e $\mathfrak{a} \in \mathscr{J}$ tais que $\mathfrak{a}^{-1} \in \mathfrak{B}$. Então $u(\mathfrak{B}) = t(\mathfrak{a})$. Em particular, temos*

$$\{t(\mathfrak{a}) \mid \mathfrak{a} \in \mathscr{J}\} = \{u(\mathfrak{B}) \mid \mathfrak{B} \in \mathscr{C}\ell\}.$$

Demonstração. Seja $\alpha \in \mathfrak{a} \setminus \{0\}$ tal que $t(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\langle\alpha\rangle_{I_L})$. Então $\alpha\mathfrak{a}^{-1} \in \mathscr{J} \cap \mathfrak{B}$, pela Proposição 7.9 e usando que $\alpha\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = I_L$. Notemos que

$$(\alpha\mathfrak{a}^{-1})\mathfrak{a} = \langle\alpha\rangle_{I_L} \Rightarrow \mathfrak{N}(\alpha\mathfrak{a}^{-1})\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\langle\alpha\rangle_{I_L}),$$

e portanto

$$u(\mathfrak{B}) \leq \mathfrak{N}(\alpha\mathfrak{a}^{-1}) = \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\langle\alpha\rangle_{I_L}) = t(\mathfrak{a}).$$

Por outro lado, seja $\mathfrak{b} \in \mathscr{J} \cap \mathfrak{B}$ tal que $u(\mathfrak{B}) = \mathfrak{N}(\mathfrak{b})$. Então, como $\mathfrak{a}^{-1}, \mathfrak{b} \in \mathfrak{B}$, existe $\beta \in L \setminus \{0\}$ tal que $\beta\mathfrak{a}^{-1} = \mathfrak{b}$. Mas então $\langle\beta\rangle_{I_L} = \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$. Disso tiramos que $\beta \in \mathfrak{a} \setminus \{0\}$. Além disso,

$$\mathfrak{N}(\langle\beta\rangle_{I_L}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})u(\mathfrak{B}).$$

Logo

$$t(\mathfrak{a}) \leq \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\langle\beta\rangle_{I_L}) = u(\mathfrak{B}).$$

Então de fato temos $u(\mathfrak{B}) = t(\mathfrak{a})$. Para a última afirmação basta notar, de um lado, que para $\mathfrak{a} \in \mathscr{J}$ temos $t(\mathfrak{a}) = u(\mathfrak{a}^{-1}\mathscr{H})$, e de outro que, se $\mathfrak{B} \in \mathscr{C}\ell$, então existe um $\mathfrak{a} \in \mathfrak{B}^{-1} \cap \mathscr{J}$. Assim, $\mathfrak{a}^{-1} \in \mathfrak{B}$, e temos $u(\mathfrak{B}) = t(\mathfrak{a})$. □

Ainda temos um último lema técnico a provar antes de chegarmos ao resultado desejado:

Lema 9.2. *Existe uma constante $C > 0$ tal que $t(\mathfrak{a}) \leq C$, para todo $\mathfrak{a} \in \mathscr{J}$.*

Demonstração. Sejam $\sigma_1, \ldots, \sigma_n$ os isomorfismos de L em $\mathbb{C}$, e seja $\{\beta_1, \ldots, \beta_n\}$ uma base integral de L. Definamos

$$C = \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|\sigma_j(\beta_i)|\right).$$

Mostraremos que, para todo $\mathfrak{a} \in \mathscr{J}$, temos $t(\mathfrak{a}) \leq C$, o que terminará a demonstração. Tomemos então $\mathfrak{a} \in \mathscr{J}$ qualquer. Então existe k inteiro positivo tal que $k^n \leq \mathfrak{N}(\mathfrak{a}) < (k+1)^n$. Definamos

$$\mathscr{L} = \left\{\sum_{i=1}^{n} d_i\beta_i \mid d_1, \ldots, d_n \in \{0, \ldots, k\}\right\}.$$

Notemos que $|\mathscr{L}| = (k+1)^n > \mathfrak{N}(\mathfrak{a})$, logo pelo Princípio da Casa dos Pombos existem $\lambda, \nu \in \mathscr{L}$ distintos tais que $\lambda + \mathfrak{a} = \nu + \mathfrak{a}$. Então temos

$$\lambda - \nu = \sum_{i=1}^{n} a_i \beta_i \in \mathfrak{a}, \text{ onde } a_1, \ldots, a_n \in \{-k, \ldots, k\}.$$

Assim:

$$\begin{aligned} |N(\lambda-\nu)| = \left|\prod_{j=1}^{n} \sigma_j(\lambda-\nu)\right| &= \left|\prod_{j=1}^{n} \sigma_j\Big(\sum_{i=1}^{n} a_i\beta_i\Big)\right| = \prod_{j=1}^{n}\left|\sum_{i=1}^{n} a_i\sigma_j(\beta_i)\right| \\ &\leq \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|a_i||\sigma_j(\beta_i)|\right) \leq \prod_{j=1}^{n}\left(\sum_{i=1}^{n} k|\sigma_j(\beta_i)|\right) \\ &= k^n \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|\sigma_j(\beta_i)|\right) = k^n C \leq \mathfrak{N}(\mathfrak{a})C. \end{aligned}$$

Concluímos finalmente do item b) do Teorema 8.6 que

$$t(\mathfrak{a}) \leq \mathfrak{N}(\mathfrak{a})^{-1}\mathfrak{N}(\langle\lambda-\nu\rangle_{I_L}) = \mathfrak{N}(\mathfrak{a})^{-1}|N(\lambda-\nu)| \leq C.$$

□

Enfim, chegamos ao resultado que tanto almejávamos:

Teorema 9.3 (Finitude do Número de Classes)**.** *O número de classes h_L é finito.*

Demonstração. Pelo Lema 9.2, o conjunto $\{t(\mathfrak{a}) \mid \mathfrak{a} \in \mathscr{J}\}$ é limitado superiormente por um $C > 0$. Mas pelo Lema 9.1, esse conjunto é igual a $\{u(\mathfrak{B}) \mid \mathfrak{B} \in \mathscr{C}\ell\}$, que portanto também é limitado por C. Seja agora $\mathfrak{B} \in \mathscr{C}\ell$. Então existe $\mathfrak{b} \in \mathfrak{B}$ tal que $\mathfrak{N}(\mathfrak{b}) \leq C$. Mas pelo Corolário 8.5, existe um número finito m de ideais de $\mathscr{J}$ tais que $\mathfrak{N}(\mathfrak{b}) \leq C$. Assim, $\mathfrak{B}$ é a classe de um desses m ideais. Isso mostra que $\mathscr{C}\ell$ é finito, como desejávamos. □

Um corolário direto deste teorema é:

Corolário 9.4. *Para todo $\mathfrak{a} \in \mathscr{J}$, $\mathfrak{a}^{h_L}$ é um ideal principal.*

Esse teorema, embora fortíssimo, não é totalmente satisfatório para o cálculo efetivo de h_L para um corpo de números algébricos L dado. Afirmamos, sem demonstração, que existe a seguinte cota para h_L, conhecida como a cota de Minkowski:

$$h_L \leq \mu_L = \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|d_L|},$$

em que t é a metade do número de isomorfismos σ de L em $\mathbb{C}$ tais que $\sigma(L) \not\subseteq \mathbb{R}$ (pode-se mostrar que o número de tais isomorfismos é sempre par, ou seja, t é inteiro).

Para finalizar, mostraremos como toda a teoria que desenvolvemos pode ser utilizada num exemplo concreto:

EℤEmplo 3. Na introdução, falamos sobre como a Teoria Algébrica dos Números aparece naturalmente no estudo das equações diofantinas. Caso o anel de inteiros algébricos necessário para resolver uma equação diofantina não seja um DFU, entretanto, não está claro como devemos prosseguir. Como já vimos, $\mathbb{Z}[\sqrt{-5}]$ não é um DFU. No entanto, veremos como resolver a equação diofantina $y^3 = x^2 + 5$ utilizando este anel. Este exemplo se encontra em [4]

Para começar, utilizando a cota de Minkowski para $L = \mathbb{Q}(\sqrt{-5})$, e pelo EℤEmplo 2, temos

$$\mu_L = \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n}\sqrt{|d_L|} = \Big(\frac{4}{\pi}\Big)^1 \frac{2!}{2^2}\sqrt{|d_L|} = \frac{4}{\pi}\cdot\frac{1}{2}\sqrt{|4\cdot(-5)|} \approx 2,847 < 3.$$

Logo $h_L = 1$ ou $h_L = 2$. Como $\mathbb{Z}[\sqrt{-5}]$ não é um DFU, temos $h_L = 2$. Assim, $\mathscr{C}\ell$ possui dois elementos. Além disso, pelo item c) do Teorema 4.5, $U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$. Indicaremos ainda a classe de um ideal $\mathfrak{j}$ em $\mathscr{C}\ell$ por $[\mathfrak{j}]$. Finalmente, consideremos a equação diofantina $y^3 = x^2 + 5$. Se x fosse ímpar, teríamos

$y^3 \equiv 1^2 + 5 \equiv 6 \pmod 8$, o que não é possível. Logo x é par, e portanto y é ímpar.

Se $y \equiv 0 \pmod 5$, então $x^2 \equiv 0 \pmod 5$, logo $x \equiv 0 \pmod 5$. Mas então $5 \equiv x^2 + 5 = y^3 \equiv 0 \pmod{25}$, absurdo! Logo $y \not\equiv 0 \pmod 5$.

Em $\mathbb{Z}[\sqrt{-5}]$, temos $y^3 = (x + \sqrt{-5})(x - \sqrt{-5})$. Chamemos agora os ideais $\mathfrak{a} = \langle x + \sqrt{-5}\rangle$ e $\mathfrak{b} = \langle x - \sqrt{-5}\rangle$ (para simplificar, denotaremos o ideal gerado por um elemento $\alpha \in \mathbb{Z}[\sqrt{-5}]$ por $\langle\alpha\rangle$, ao invés de $\langle\alpha\rangle_{\mathbb{Z}[\sqrt{-5}]}$). Então temos a igualdade de ideais $\langle y\rangle^3 = \langle x + \sqrt{-5}\rangle\langle x - \sqrt{-5}\rangle = \mathfrak{ab}$.

Suponhamos que exista um ideal primo não-nulo $\mathfrak{p}$ que divida $\mathfrak{a}$ e $\mathfrak{b}$. Então $\mathfrak{p} \ni (x+\sqrt{-5})-(x-\sqrt{-5}) = 2\sqrt{-5}$. Assim, $\mathfrak{p}$ divide $\langle 2\sqrt{-5}\rangle = \langle 2\rangle\langle\sqrt{-5}\rangle$. É simples verificar que $\langle 2\rangle = \langle 2, 1 + \sqrt{-5}\rangle^2$, e pela multiplicatividade da norma de ideais e pelo Teorema 8.6 temos

$$\mathfrak{N}(\langle 2, 1 + \sqrt{-5}\rangle)^2 = \mathfrak{N}(\langle 2\rangle) = |N(2)| = |2^2| = 4 \Rightarrow \mathfrak{N}(\langle 2, 1 + \sqrt{-5}\rangle) = 2,$$

que é um número primo, logo pelo item b) do Corolário 8.4 o ideal $\langle 2, 1 + \sqrt{-5}\rangle$ é primo.

Além disso, $\mathfrak{N}(\langle\sqrt{-5}\rangle) = |N(\sqrt{-5})| = 5$, logo pelo mesmo corolário o ideal $\langle\sqrt{-5}\rangle$ é primo. Assim, temos a fatoração em ideais primos:

$$\langle 2\sqrt{-5}\rangle = \langle 2, 1 + \sqrt{-5}\rangle^2\langle\sqrt{-5}\rangle.$$

Assim, $\mathfrak{p} = \langle 2, 1 + \sqrt{-5}\rangle$ ou $\mathfrak{p} = \langle\sqrt{-5}\rangle$. Se $\mathfrak{p} = \langle 2, 1 + \sqrt{-5}\rangle$, então

$$\mathfrak{p} \mid \langle y\rangle \Rightarrow 2 = \mathfrak{N}(\mathfrak{p}) \mid \mathfrak{N}(\langle y\rangle) = |N(y)| = y^2.$$

Mas y é ímpar, absurdo! Se $\mathfrak{p} = \langle\sqrt{-5}\rangle$, temos

$$\mathfrak{p} \mid \langle y\rangle \Rightarrow 5 = \mathfrak{N}(\mathfrak{p}) \mid \mathfrak{N}(\langle y\rangle) = |N(y)| = y^2.$$

Mas y não é múltiplo de 5, absurdo! Isso mostra que os ideais $\mathfrak{a}$ e $\mathfrak{b}$ são primos entre si. Assim, como $\langle y\rangle^3 = \mathfrak{ab}$, existem ideais $\mathfrak{c}$ e $\mathfrak{d}$ de $\mathbb{Z}[\sqrt{-5}]$ tais que $\mathfrak{a} = \mathfrak{c}^3$ e $\mathfrak{b} = \mathfrak{d}^3$. Pelo Corolário 9.4, $[\mathfrak{c}^2] = [\langle 1\rangle]$, logo como $\mathfrak{a}$ é principal:

$$\mathfrak{a} = \mathfrak{c}^3 \Rightarrow [\langle 1\rangle] = [\mathfrak{a}] = [\mathfrak{c}]^3 = [\mathfrak{c}]^2[\mathfrak{c}] = [\langle 1\rangle][\mathfrak{c}] = [\mathfrak{c}].$$

Isso mostra que $\mathfrak{c}$ é principal. Então existem $a, b \in \mathbb{Z}$ tais que $\mathfrak{c} = \langle a + b\sqrt{-5}\rangle$, ou seja,

$$\langle x + \sqrt{-5}\rangle = \mathfrak{a} = \mathfrak{c}^3 = \langle a + b\sqrt{-5}\rangle^3.$$

Assim, os elementos $x + \sqrt{-5}$ e $(a + b\sqrt{-5})^3$ são associados. Como $U(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$, temos:

$$x + \sqrt{-5} = \pm(a + b\sqrt{-5})^3 = \pm((a^3 - 15ab^2) + (3a^2b - 5b^3)\sqrt{-5}).$$

Então

$$\pm 1 = 3a^2b - 5b^3 = b(3a^2 - 5b^2) \Rightarrow |b| = |3a^2 - 5b^2| = 1.$$

Tanto para $b = 1$ quanto para $b = -1$, precisamos ter

$$3a^2 - 5 = \pm 1 \Rightarrow 3a^2 = 6 \text{ ou } 3a^2 = 4,$$

o que é impossível. Portanto, a equação $y^3 = x^2 + 5$ não tem soluções inteiras.

Referências

[1] O. Endler, *Teoria dos Números Algébricos*. Projeto Euclides, IMPA, 2014.

[2] P. A. Martin, *Grupos, Corpos e Teoria de Galois*. Editora Livraria da Física, 2010.

[3] Z. I. Borevich and I. R. Shafarevich, *Number Theory*. Academic press, 1966.

[4] F. B. Martinez, C. G. Moreira, N. Saldanha, and E. Tengan, *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. Projeto Euclides, IMPA, 2013.

[5] D. Dummit and R. Foote, *Abstract algebra*. Wiley, 2004.