Uma introdução ao estudo dos números algébricos

Gabriel Simon Schafaschek

2016

Sumário

1 Introdução

A Teoria dos Números costuma ser chamada de a "Rainha da Matemática", e creio que faz jus ao nome. Já foi objeto de estudo dos mais ilustres matemáticos, tais como Pierre de Fermat, Carl Friedrich Gauss, Richard Dedekind e Leonard Euler. Tal teoria está ligada, majoritariamente, ao problema de resolver equações diofantinas. Mais especificamente, ela desenvolve um estudo dos números inteiros e do seu respectivo corpo de frações $\mathbb{Q}$. Portanto, conforme já dito em [1], os números algébricos aparecem, naturalmente, como uma ferramente para tratar deste problema. O objetivo do presente trabalho é expor, de forma introdutória, alguns resultados centrais relacionados a esta teoria.

O desenvolvimento da Álgebra, durante o século XVII, desperta o interesse do matemático francês Pierre de Fermat (1601 - 1665) pelo assunto. Dos teoremas enunciados por Fermat, provavelmente o que atingiu maior destaque tenha sido o chamado Último Teorema de Fermat, que afirma a não existência de inteiros positivos x, y, z, n com $n > 2$, tais que $x^n + y^n = z^n$. A teoria de números álgébricos permite uma demonstração de tal teorema no caso em que n é um número primo ímpar, escrevendo-se $x^n + y^n = (x + y) \cdot (x + \zeta_n y) \cdot ... \cdot (x + \zeta_n^{n-1} y)$, em que $\zeta_n \neq 1$ é uma raiz n-ésima da unidade. Daí, vem a importância do estudo do anel $\mathbb{Z}[\zeta_n]$

Em 1796, o matemático Karl Friedrich Gauss (1777 – 1855), prova um fato empolgante, conhecido como Lei da Reciprocidade Quadrática, ja observado pelo suíço Leonard Euler, em 1783. Ao tentar demonstrar resultados semelhantes para potências maiores do que o quadrado, Gauss percebe que os cálculos tornavam-se bem mais eficientes se trabalhasse com os inteiros de Gauss, ao invés de somente números inteiros. Com isso, se dá o início da teoria dos inteiros gaussianos, a qual será cuidadosamente mensionada no capítulo 4.

Mais um exemplo de aplicação da Teoria em questão se dá ao estudar a Equação de Pell, da forma $x^2 - dy^2 = 1$. Uma maneira de se determinar soluções inteiras para tal é escrevendo-a como o produto $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$. Verifica-se que (a,b) é uma solução inteira da equação acima se, e somente se, $a + b\sqrt{d}$ é invertível de norma igual a 1 no anel quadrático $\mathbb{Z}[\sqrt{d}]$. Com isso, percebe-se a importância do estudo de tal anel, o qual trataremos no capítulo 4.

Quanto ao conteúdo, escrevi estas notas em 5 curtas seções. O capítulo 2 visa estabelecer as noções preliminares mais fundamentais, que serão utilizadas durante grande parte das seções posteriores. Trata-se, resumidamente, de uma curta apresentação das propriedades mais importantes a respeito da teoria de extensões de corpos, dando prioridade aos resultados referentes a extensões algébricas. Também neste capítulo introduzo, de maneira bastante sutil, a estrutura de R-módulo sobre um anel R, que será utilizada amplamente no capítulo seguinte.

O capítulo 3, talvez, seja o mais importante para compreender a noção de inteiro algébrico. Dado um corpo $\mathbb{L}$, vamos construir o anel I_L dos inteiros algébricos sobre $\mathbb{L}$. Salientamos que, para um número algébrico α arbitrário, o anel I_L nem sempre será da forma $\mathbb{Z}[\alpha]$. Acrescento que o estudo deste anel, que quando tomado sobre o corpo $\mathbb{Q}$ dos números racionais, assume a forma $\mathbb{Z} = I_{\mathbb{Q}}$ dos números inteiros, é considerado o objetivo principal da Teoria dos Números Algébricos.

Complementando o capítulo 3, a seção 4 busca expor os conceitos mais relevantes a respeito do estudo de corpos quadráticos, os quais possuem notória importância em diversas áreas da álgebra. Em particular, um rápido comentário sobre o anel quadrático dos inteiros de Gauss é feita, também, nesta seção.

Finalmente, o capítulo 5 nos traz uma importante condição necessária para que

um número seja algébrico, a qual é enunciada como um teorema. Consiste, de certa forma, em uma bela aplicação da teoria de números algébricos, fazendo uso apropriado da Análise matemática. A seção termina com um elegante exemplo de número transcedente, que surge como corolário do teorema citado acima.

Contudo, espero que a leitura destas notas possa ser útil para aqueles que estão interessados em estudar a Teoria dos Números Algébricos. Tomei os devidos cuidados para que as demonstrações fossem bem detalhadas e para que todas as passagens tidas como óbvias sejam, acima de tudo, sinceras.

2 Conceitos básicos

Admitimos que o leitor do presente trabalho esteja familiarizado com as estruturas algébricas básicas, tais como as estruturas de anel, grupo, domínio e corpo. Também admitiremos conhecidas as noções de homomorfismos e isomorfismos entre essas estruturas, bem como a construção do anel de polinômios $A[x]$ na indeterminada x com coeficientes num anel comutativo A com unidadade.

Dito isto, faremos, neste capítulo, um resumo das principais definições e propriedades que serão utilizadas no decorrer do texto.

2.1 Extensões de Corpos

Definição 2.1. *Seja $\mathbb{F}$ um corpo. Dizemos que um par $(\mathbb{E}, i)$ é uma extensão de $\mathbb{F}$ se $\mathbb{E}$ é um corpo e $i : \mathbb{F} \to \mathbb{E}$ é um monomorfismo de aneis, isto é, um homomorfismo injetivo de aneis.*

Com efeito, se $i : \mathbb{F} \to \mathbb{E}$ é monomorfismo de aneis, então verifica-se facilmente que $i(\mathbb{F}) \subseteq \mathbb{E}$ é subcorpo de $\mathbb{E}$ e, além disso, $\mathbb{F}$ é isomorfo a $i(\mathbb{F})$. Sendo assim, costuma-se praticar um abuso de linguagem e considerar simplesmente $\mathbb{F} \subseteq \mathbb{E}$. Durante todo esse artigo, usaremos a notação $\mathbb{F} \subseteq \mathbb{E}$ para indicar que $\mathbb{E}$ é uma extensão de $\mathbb{F}$, isto é, para indicar que existe um monomorfismo $i : \mathbb{F} \to \mathbb{E}$.

Outro fato importante constitui-se em podermos considerar $\mathbb{E}$ como sendo um espaço vetorial sobre $\mathbb{F}$, tomando a adição em E e a multiplicação por elementos de $\mathbb{F}$. Dizemos que $\dim_{\mathbb{F}}(\mathbb{E})$ é o grau da extensão $\mathbb{F} \subseteq \mathbb{E}$, e escrevemos
$[\mathbb{E} : \mathbb{F}] = \dim_{\mathbb{F}}(\mathbb{E})$ para indicá-lo.

Definição 2.2. *Uma extensão $\mathbb{F} \subseteq \mathbb{E}$ chama-se finita quando $[\mathbb{E} : \mathbb{F}] < \infty$.*

Veremos, a diante, que toda extensão finita é algébrica. Embora existam extensões algébricas infinitas, nosso principal objetivo nesse trabalho é desenvolver a teoria das extensões algébricas fnitas. A proposição a seguir mostra-se de grande importância para o estudo dessas extensões, uma vez que ela torna muito mais simples o trabalho de determinar o grau de uma certa extensão dada.

Proposição 2.1. *Se $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ são extensões de corpos, então*

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{F}].$$

Demonstração. Sejam $\{x_i\}_{i\in I}$ base de $\mathbb{E}$ como $\mathbb{F}$ espaço vetorial e $\{y_j\}_{j\in J}$ base de $\mathbb{K}$ como espaço vetorial sobre $\mathbb{E}$. Vamos mostrar que $V = \{x_i y_j\}_{i\in I, j\in J}$ é base de $\mathbb{K}$ como $\mathbb{F}$ espaço vetorial. Com efeito, seja $\sum_{j\in J, i\in I} a_{ij} x_i y_j = 0$ soma finita, com $a_{ij} \in \mathbb{F}$.

Temos $\sum_{j\in J}\left(\sum_{i\in I} a_{ij}x_i\right)y_j = 0$, e sendo $\{y_j\}_{j\in J}$ LI, tiramos que $\sum_{i\in I} a_{ij}x_i = 0$, para todo $j \in J$ presente no somatório. Da independência linear de $\{x_i\}_{i\in I}$, segue que $a_{ij} = 0$, para todo $i \in I, j \in J$ incluídos na soma. Portanto $\{x_iy_j\}_{i\in I, j\in J}$ é LI.

Resta mostar que V gera $\mathbb{K}$. De fato, tome $\alpha \in \mathbb{K}$. Escreva $\alpha = \sum_{j\in J} a_jy_j$, com $a_j \in \mathbb{E}$ para finitos $j \in J$. Além disso, para cada j, escreva $a_j = \sum_{i\in I} a_{ij}x_i$, para finitos $i \in I$. Isso nos dá $\alpha = \sum_{j\in J} a_jy_j = \sum_{j\in J}\sum_{i\in I} a_{ij}x_iy_j$, para finitos $i \in I, j \in J$. Concluímos, daí, que V é base de $\mathbb{K}$. Por fim, notemos que o conjunto V possui cardinalidade igual a $[\mathbb{K} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{F}]$. **(c.q.d)**

Corolário 2.1. *Se $F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$ são extensões de corpos, então*

$$[F_n : F_1] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_2 : F_1].$$

Demonstração. Basta aplicar a proposição anterior $n - 2$ vezes, tomando as extensões $F_n \subseteq F_2 \subseteq F_1$, $F_n \subseteq F_3 \subseteq F_2$,..., $F_n \subseteq F_{n-1} \subseteq F_{n-2}$. **(c.q.d)**

Corolário 2.2. *Se $\mathbb{F} \subseteq \mathbb{K}$ e $\mathbb{K} \subseteq \mathbb{E}$ são extensões finitas, então $\mathbb{F} \subseteq \mathbb{E}$ também o é.*

Demonstração. Com efeito, se $[\mathbb{E} : \mathbb{K}] < \infty$ e $[\mathbb{K} : \mathbb{F}] < \infty$, então
$[\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}] < \infty$, isto é, $[\mathbb{E} : \mathbb{F}] < \infty$ **(c.q.d)**

2.2 Adjunção de Raízes

Definição 2.3. *Seja $\mathbb{F} \subseteq \mathbb{E}$ extensão de corpos e $\alpha \in \mathbb{E}$. Definimos o subcorpo gerado por $\mathbb{F}$ e α como sendo o menor subcorpo de $\mathbb{E}$ que contém $\mathbb{F}$ e α, e o denotamos por $\mathbb{F}(\alpha)$.*

Uma consequência imediata da definição acima é que $\mathbb{F}(\alpha)$ é dado pela interseção de todos os subcorpos de $\mathbb{E}$ que contém $\mathbb{F}$ e α. De fato, é claro que $\mathbb{F}(\alpha)$ contém tal interseção, e que esta é um subcorpo de $\mathbb{E}$. Se existisse um elemento $x \in \mathbb{F}(\alpha)$ que não pertencesse a interseção, então teríamos que esta seria um subcorpo de $\mathbb{E}$ contendo $\mathbb{F}$ e α, contida em $\mathbb{F}(\alpha)$. Isso contradiria a minimalidade desse último corpo.

Costuma-se, ainda, dizer que $\mathbb{F}(\alpha)$ é o corpo gerado pela adjunção de α. Podemos estender essa ideia para um conjunto qualquer, conforme nos diz a:

Definição 2.4. *Seja $\mathbb{F} \subseteq \mathbb{E}$ extensão de corpos, e seja A um subconjunto de $\mathbb{E}$. Definimos o corpo obtido de $\mathbb{F}$ pela adjunção de A como sendo o menor subcorpo de $\mathbb{E}$ que contém A e $\mathbb{F}$,e o denotamos por $\mathbb{F}(A)$.*

No caso especial em que $A = \{a_1, ..., a_n\}$, escrevemos simplesmente
$\mathbb{F}(A) = \mathbb{F}(a_1, ..., a_n)$. Dizemos, ainda, que a extensão $\mathbb{F} \subseteq \mathbb{F}(a_1, ..., a_n)$ é do tipo *finitamente gerada*.

Definição 2.5. *Uma extensão $\mathbb{F} \subseteq \mathbb{E}$ é dita ser simples se, e somente se, existir $x \in \mathbb{E}$ tal que $\mathbb{F}(x) = \mathbb{E}$*

Notemos que toda extensão simples é finitamente gerada.

2.3 Homomorfismos de Corpos

Sejam $\mathbb{E}$ e $\mathbb{E}'$ corpos e seja $f : \mathbb{E} \to \mathbb{E}'$ homomorfismo. Temos duas opções para o núcleo de f: $ker(f) = \mathbb{E}$ ou $ker(f) = \{0\}$. No primeiro caso, f é o homomorfismo nulo entre esses corpos, e no segundo, f é monomorfismo.

Definição 2.6. *Sejam $\mathbb{K} \subseteq \mathbb{E}$ e $\mathbb{K} \subseteq \mathbb{E}'$ extensões de um corpo $\mathbb{K}$. Todo homomorfismo $f : \mathbb{E} \to \mathbb{E}'$ tal que $f(x) = x$, para todo $x \in \mathbb{K}$ é denominado $\mathbb{K}$-homomorfismo de $\mathbb{E}$ em $\mathbb{E}'$.*

Definimos, analogamente, as noções de $\mathbb{K}$ - isomorfismo e $\mathbb{K}$ - automorfismo. A proposição a seguir é de grande importância para o desenvolvimente, posteriormente, do conceito de extensão de homomorfismos.

Proposição 2.2. *Se f e g são dois monomorfismos de $\mathbb{E}$ em $\mathbb{E}'$, então o subconjunto*

$$H = \{x \in \mathbb{E} / f(x) = g(x)\}$$

é um subcorpo de $\mathbb{E}$. Se S é um sistema de geradores de $\mathbb{E}$ e $f(x) = g(x)$ para todo $x \in S$, então $f = g$.

Demonstração. Tome $x, y \in H$. Então $f(x) = g(x)$ e $f(y) = g(y)$, donde $f(x) - f(y) = g(x) - g(y)$, isto é, $f(x - y) = g(x - y)$, ou ainda, $x - y \in H$. Analogamente, mostra-se que $xy \in H$ e, se $x \neq 0$, $x^{-1} \in H$. Para a segunda afirmação, notemos que, por hipótese, $S \subseteq H \subseteq \mathbb{E}$, logo $E = (S) \subseteq H \subseteq \mathbb{E}$, donde segue que $H = S$, isto é, $f = g$ **(c.q.d)**

Os dois corolários que se seguem são consequências imediatas do teorema acima:

Corolário 2.3. *Seja $\mathbb{K} \subseteq \mathbb{E}$ extensão de corpos, e seja S sistema de geradores de $\mathbb{E}$ sobre $\mathbb{K}$, isto é, $\mathbb{E} = \mathbb{K}(S)$. Seja, também, $\mathbb{E}'$ um corpo. Se f e g são dois homomorfismos de $\mathbb{E}$ em $\mathbb{E}'$ e se $f(x) = g(x)$, $\forall x \in \mathbb{K} \cap S$, então $f = g$.*

Corolário 2.4. *Sejam $\mathbb{K} \subseteq \mathbb{E}$ e $\mathbb{K} \subseteq \mathbb{E}'$ extensões de corpos e seja S um sistema de geradores de $\mathbb{E}$ sobre $\mathbb{K}$. Para que dois $\mathbb{K}$ - homomorfismos $f, g : \mathbb{E} \to \mathbb{E}'$ sejam iguais, é necessário e suficiente que $f(x) = g(x)$, para todo $x \in S$.*

Este corolário nos mostra que um $\mathbb{K}$ - monomorfismo de $\mathbb{E}$ em $\mathbb{E}'$ fica completamente determinado pela sua ação sobre um sistema de geradores de $\mathbb{E}$ sobre $\mathbb{K}$.

2.4 Extensões Algébricas e Elementos Algébricos

Do ponto de vista da álgebra moderna, o estudo dos elementos algébricos sobre um corpo é precedido pelo estudo das extensões algébricas desse corpo. Em outras palavras, conhecendo-se as propriedades de uma certa extensão algébrica, é possível conhecer também as propriedades dos elementos algébricos segundo essa extensão. Por esse motivo, os resultados seguintes darão enfoque às propriedades de extensões.

Definição 2.7. *Seja $\mathbb{K} \subseteq \mathbb{E}$ extensão de corpos e seja α um elemento de $\mathbb{E}$. Dizemos que α é algébrico sobre $\mathbb{K}$ se, e somente se, existe um polinômio $f \in \mathbb{K}[x]$ tal que $f(\alpha) = 0$. Caso contrário, diz-se que α é transcendente sobre $\mathbb{K}$.*

Definição 2.8. *Seja $\mathbb{K} \subseteq \mathbb{E}$ extensão de corpos. Dizemos que essa extensão é algébrica se, e somente se, todo elemento de $\mathbb{E}$ for algébrico sobre $\mathbb{K}$. Caso contrário, diz-se que $\mathbb{E}$ é uma extensão transcendente de $\mathbb{K}$.*

Exemplo 1. *Considere a extensão $\mathbb{K} \subseteq \mathbb{E}$. Todo elemento μ do corpo $\mathbb{K}$ é algébrico sobre $\mathbb{K}$, pois é raiz do polinômio $g(x) = x - \mu \in \mathbb{K}[x]$.*

Exemplo 2. *Todo número complexo que é algébrico (respec. transcendente) sobre $\mathbb{Q}$ é denominado número algébrico (respec. número transcendente). É muito fácil pensar num exemplo de número algébrico (basta tomar qualquer número racional, conforme o exemplo anterior). Entretanto, é difícil dar exemplos de números transcendentes. O primeiro exemplo desses números foi dado por Liouville, em 1851. Já, em 1873, o matemático francês Charles Hermite demonstrou que o número*

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n$$

é transcendente. Mais tarde, em 1882, Carl Louis Ferdinand von Lindemann, matemático de origem alemã, mostrou que o número π é transcendente.

Tendo em vista a dificuldade de se encontrar números transcendentes, é natural sermos levados a pensar que, dado um número complexo, a probabilidade de que ele seja trascendente é pequena. Entretando, essa intuição poderia nos levar a um grave engano, se não fosse pelo matemático Georg Ferdinand Ludwig Philipp Cantor. Esse matemático russo, conhecido por elaborar a teoria dos conjuntos moderna, demonstrou que o conjunto dos números algébricos é enumerável, logo o conjunto formado por todos os números transcendentes tem a potência do contínuo. Essa demosntração é surpreendente no sentido de que estabelece a existência de números transcendentes sem dar exemplos desses números, pois a demonstração é não construtiva. A seguir, apresentamos esse teorema, munido de alguns corolários importantes:

Teorema 2.1 (Cantor)**.** *O conjunto dos números algébricos é enumerável.*

Demonstração. Primeiro, observe que se um número complexo é raiz de um polinômio com coeficientes em $\mathbb{Q}$, então ele também é raiz de um polinômio que mora em $\mathbb{Z}[x]$. Logo, para que um dado número seja algébrico, basta que ele seja algébrico sobre $\mathbb{Z}$. Dado um polinômio não constante com coeficientes inteiros $p(x) = a_0 + a_1x + \cdots + a_nx^n$, definimos sua altura como sendo o número $H = |a_0| + |a_1| + \cdots + |a_n| + n$. Note que $H > 1$, pois $n \geq 1$ e, $\forall n \geq 1$, temos $a_n \neq 0$. Além disso, p deve possuir, no máximo, n raízes complexas, das quais todas, algumas, ou nenhuma delas, podem ser reais. Agora, o número de polinômios com coeficientes inteiros com uma dada altura é apenas um número finito. Isso significa que o conjunto de todas as raízes de todos os polinômios com uma dada altura é um conjunto finito. Portanto, o conjunto de todos as raízes de todos os polinômios de todas as alturas forma um conjunto enumerável, uma vez que é dado por uma união enumerável de conjuntos finitos. **(c.q.d)**

Corolário 2.5. *Existem números transcendentes.*

Demonstração. Se, por absurdo, nenhum número complexo fosse transcendente, então todos os números complexos seriam algébricos. Pelo teorema acima, isso nos daria que $\mathbb{C}$ é um conjunto enumerável. Absurdo. **(c.q.d)**

Corolário 2.6. *O conjunto dos números transcendentes é não enumerável.*

Demonstração. O conjunto $\mathbb{C}$ é dado pela união disjunta entre o conjunto dos números algébricos e o conjunto dos números transcendentes. Se este fosse enumerável, então também $\mathbb{C}$ o seria, uma vez que a união de dois conjuntos enumeráveis também é enumerável. Novamente, chegaríamos em um absurdo. **(c.q.d)**

Notemos, ainda, que o conjunto dos números algébricos e o conjunto dos números transcendentes são ambos densos em $\mathbb{R}$. O primeiro porque contém o conjunto $\mathbb{Q}$, que é denso. O segundo porque, se um intervalo aberto não degenerado em $\mathbb{R}$ não contém números transcendentes, então que este seria formado apenas por números algébricos, isto é, seria enumerável. Isto não pode ocorrer, pois qualquer intervalo não degenerado da reta é não enumerável. Continuemos, abaixo, com o estudo das extensões algébricas.

Seja $\mathbb{K} \subseteq \mathbb{E}$ extensão de corpos e seja $\alpha \in \mathbb{E}$. A propriedade universal do anel de polinômios nos garante a existência de um único $\mathbb{K}$-homomorfismo $\phi_\alpha : \mathbb{K}[x] \to \mathbb{E}$ tal que $\phi_\alpha(x) = \alpha$. Temos que $\mathrm{Im}(\phi_\alpha) = K[\alpha]$ e $\ker(\phi_\alpha) = \{g \in \mathbb{K}[x] \mid g(\alpha) = 0\}$. Podemos, então, reformular a definição 2.7 do seguinte modo:

1. α é algébrico sobre $\mathbb{K} \Leftrightarrow \ker(f_\alpha) \neq \{0\}$.
2. α é transcendente sobre $\mathbb{K} \Leftrightarrow \ker(f_\alpha) = \{0\}$.

Definimos, também, $\mathbb{F}[\alpha] = \mathrm{Im}(\phi_\alpha)$. O teorema a seguir mostra que é possível determinar a estrutura do corpo $\mathbb{F}[\alpha]$ no no caso em que este for um elemento algébrico.

Teorema 2.2. *Sejam $\mathbb{F} \subseteq \mathbb{E}$ extensão de corpos e $\alpha \in \mathbb{E}$ elemento algébrico sobre $\mathbb{F}$. Então $\mathbb{F}[\alpha]$ é um corpo e, além disso, existe um único polinômio irredutível e mônico $p \in F[x]$ tal que $\mathbb{F}[\alpha] \cong \mathbb{F}[x]/\langle p \rangle$.*

Demonstração. Seja $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$ o único homomorfismo tal que $\phi_\alpha(x) = \alpha$. Como α é algébrico sobre $\mathbb{F}$, então $\ker(\phi_\alpha) \neq \{0\}$. O fato de $\mathbb{F}[x]$ ser um domínio principal garante que existe um único polinômio mônico $p \in \mathbb{F}[x]$ que gera o núcleo de ϕ_α, isto é, $\ker(\phi_\alpha) = \langle p \rangle$. Com efeito, $\langle p \rangle$ é um ideal primo, uma vez que $\ker(\phi_\alpha)$ também o é. Daí, segue que p é primo, ou seja, p é irredutível, ou ainda, $\langle p \rangle$ é maximal. Portanto, temos que $\mathbb{F}[x]/\langle p \rangle$ é um corpo. Segue, do teorema do isomorfismo, que $\mathbb{F}[x]/\langle p \rangle \cong \mathrm{Im}(\phi_\alpha) = \mathbb{F}[\alpha]$, o que também garante que $\mathbb{F}[\alpha]$ é um corpo. **(c.q.d)**

Definição 2.9. *O único polinômio mônico do teorema acima chama-se polinômio minimal de α sobre $\mathbb{F}$, e é denotado por $I(\alpha, \mathbb{F})$.*

Algumas consequências importantes do teorema acima podem ser reunidas nas proposições abaixo.

Proposição 2.3. *Sejam $\mathbb{F} \subseteq \mathbb{E}$ extensão de corpos, $\alpha \in \mathbb{E}$ elemento algébrico sobre $\mathbb{F}$, e $f \in \mathbb{F}[x]$ polinômio não constante mônico tal que $f(\alpha) = 0$. São equivalentes as seguintes proposições:*
i) f é o polinômio minimal de α sobre $\mathbb{F}$.
ii) Para todo $g \in \mathbb{F}[x]$, se $g(\alpha) = 0$, então $f|g$.
iii) Para todo $g \in \mathbb{F}[x]$ não nulo tal que $g(\alpha) = 0$ têm-se $\partial f \leq \partial g$.
iv) f é irredutível em $\mathbb{F}[x]$.

Demonstração. $(i) \Rightarrow (ii)$: De fato, se $g(\alpha) = 0$, então $g \in \text{Ker}(\phi_\alpha) = \langle f \rangle$, em que ϕ_α é o morfismo dado conforme o teorema anterior. Logo $f|g$.
$(ii) \Rightarrow (iii)$: Como $f|g$, então existe $q \in \mathbb{F}[c]$ tal que $g = fq$, donde segue que $\partial g = \partial f + \partial q \geq \partial f$.
$(iii) \Rightarrow (iv)$: Se fosse f redutível em $\mathbb{F}[x]$, existiriam polinômios $g, q \in \mathbb{F}[x]$ não constantes tais que $f = qg$. Claro que $\partial f > \partial g$ e $\partial f > \partial q$. Por outro lado, $0 = f(\alpha) = g(\alpha)q(\alpha)$, donde seque que $g(\alpha) = 0$ ou $q(\alpha) = 0$, ou seja, $\partial f \leq \partial g$ ou $\partial f \leq \partial q$, conforme informa a hipótese. Essas afirmações são contraditórias. Logo f é irreditível.
$(iv) \Rightarrow (i)$ Com efeito, as hipóteses nos dão que f é um polinômio mônico, irreditível e pertencente ao núcleo do morfismo ϕ_α. Sabemos que tal polinômio é único, e portanto, $f = I(\alpha, \mathbb{F})$. **(c.q.d)**

Observamos que o item (iii) do teorema anterior justifica o nome polinômio minimal.

Proposição 2.4. *Seja $\mathbb{F} \subseteq \mathbb{E}$ extensão de corpos. Seja $\alpha \in \mathbb{E}$ um elemento algébrico sobre $\mathbb{F}$. Se $\partial I(\alpha, \mathbb{F}) = n$, então*
a) $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$
b) O conjunto $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base do $\mathbb{F}$-espaço vetorial $\mathbb{F}(\alpha)$.
c) $n = [\mathbb{F}(\alpha) : \mathbb{F}]$

Demonstração. a) É evidente.
b) Tome $y \in \mathbb{F}[\alpha] = \mathbb{F}(\alpha)$. Seja g um polinômio com coeficientes em $\mathbb{F}$ tal que $g(\alpha) = y$. Tome $q, r \in \mathbb{F}[c]$ tais que $g = qf + r$, com $\partial r < \partial f$ ou $r = 0$ (f denota o polinômio minimal de α sobre $\mathbb{F}$. Então $y = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$ O fato de r ter grau menor do que n demonstra que o conjunto dado é, de fato, um sistema de geradores de $\mathbb{F}(\alpha)$ sobre $\mathbb{F}$. Se $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ fosse linearmente dependente, então existiriam $a_0, \cdots, a_{n-1} \in \mathbb{F}$, não todos nulos, tais que
$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$, o que contradiz a minimalidade do grau de f. Daí, segue o resultado.
c) É consequência imediata do item anterior. **(c.q.d)**

Em resumo, a proposição acima nos diz que toda extensão algébrica simples é finita. A seguir, dois outros teoremas importantes: O primeiro dá outra caracterização das extensões algébricas e o segundo, das extensões finitas, as quais serão as extensões mais relevantes para o decorrer deste trabalho.

Teorema 2.3. *Se $\mathbb{F} \subseteq \mathbb{E}$ é extensão de corpos, então essa extensão é algébrica se, e somente se, todo anel intermediário entre $\mathbb{F}$ e $\mathbb{E}$ é um corpo.*

Demonstração. ($\Rightarrow$) Seja R um anel entre os corpos dados. Se $a \in R \subseteq \mathbb{E}$, então a é algébrico sobre $\mathbb{F}$, ou seja, $\mathbb{F}[a]$ é um corpo e, além disso, $\mathbb{F}[a] \subseteq R$ (de fato, R contém todas as combinações lineres de potências de a com escalares em $\mathbb{F}$). Segue que $a^{-1} \in \mathbb{F}[a] \subseteq R$, isto é, R é um corpo.
($\Leftarrow$) Tome $a \in \mathbb{E}$. Temos $\mathbb{F} \subseteq \mathbb{F}[a] \subseteq \mathbb{E}$. Por hipótese, $\mathbb{F}[a]$ é corpo. Logo $a^{-1} \in \mathbb{F}[a]$. Segue que existe g em $\mathbb{F}[x]$ tal que $g(a) = a^{-1}$. Com efeito, vê-se que a é raiz do polinômio $p = xg - 1$. Portanto, a é algébrico sobre $\mathbb{F}$. **(c.q.d)**

Teorema 2.4. *Uma extensão é finita se, e somente se, é algébrica e finitamente gerada.*

Demonstração. ($\Rightarrow$) Seja $\mathbb{F} \subseteq \mathbb{E}$ extensão finita. Suponhamos $[\mathbb{E} : \mathbb{F}] = n \in \mathbb{N}$. Seja $e_1, \cdots e_n$ uma base de $\mathbb{E}$ como espaço vetorial sobre $\mathbb{F}$. Então $\mathbb{E} = \mathbb{F}(e_1, \cdots, e_n)$, isto é, a extensão é finitamente gerada. Além disso, para todo $\alpha \in \mathbb{E}$, temos que o

conjunto $\{1, \alpha, \cdots, \alpha^n\}$ é LD sobre $\mathbb{F}$, ou seja, devem existir $\beta_0, \beta_1, \cdots, \beta_n \in \mathbb{F}$ tais que $\beta_0 + \beta_1\alpha + \cdots + \beta_n\alpha^n = 0$. Portanto α é raiz do polinômio
$\beta_0 + \beta_1 x + \cdots + \beta_n x^n \in \mathbb{F}[x]$, donde segue que $\mathbb{F} \subseteq \mathbb{E}$ é algébrica.
($\Leftarrow$) Suponha $\mathbb{F} \subseteq \mathbb{E}$ extensão algébrica e finitamente gerada. Sejam $a_1, \cdots, a_n \in \mathbb{F}$ tais que $\mathbb{E} = \mathbb{F}(a_1, \cdots, a_n)$. Considere a torre de corpos
$\mathbb{F} \subseteq \mathbb{F}(a_1) \subseteq \mathbb{F}(a_1, a_2) \subseteq \cdots \subseteq \mathbb{F}(a_1, \cdots, a_n)$. Para todo $i \in \{1, ..., n-1\}$, temos que $\mathbb{F}(a_1, ..., a_i) \subseteq \mathbb{F}(a_1, ..., a_i, a_{i+1})$ é extensão algébrica simples, pois a_{i+1} é algébrico sobre $\mathbb{F}(a_1, ..., a_i)$. Pelo Teorema 2.4, seque que cada uma dessas extensões é finita, ou seja, $[\mathbb{F}(a_1, ..., a_i, a_{i+1}) : \mathbb{F}(a_1, ..., a_i)] < \infty$, para todo $i \in \{1, ..., n-1\}$, donde segue que $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}(a_1, ..., a_{n-1})] \cdots [\mathbb{F}(a_1) : \mathbb{F}] < \infty$. **(c.q.d)**

Proposição 2.5. *Sejam $\mathbb{F} \subseteq \mathbb{K}$ e $\mathbb{K} \subseteq \mathbb{E}$ extensões de corpos. Nesses termos, $\mathbb{E}$ é uma extensão algébrica de $\mathbb{F}$ se, e somente se, $\mathbb{K}$ é uma extensão algébrica de $\mathbb{F}$ e $\mathbb{E}$ é extensão algébrica de $\mathbb{K}$.*

Demonstração. Se $\mathbb{F} \subseteq \mathbb{E}$ é extensão algébrica, então, em particular, todo elemento de $\mathbb{K} \subseteq \mathbb{E}$ é algébrico sobre $\mathbb{F}$. Não obstante, todo elemento de $\mathbb{E}$ é raiz de um polinômio $p \in \mathbb{F}[x] \subseteq \mathbb{K}[x]$, ou seja, é algébrico sobre $\mathbb{K}[x]$. Reciprocamente, suponha que $\mathbb{K}$ é uma extensão algébrica de $\mathbb{F}$ e $\mathbb{E}$ é extensão algébrica de $\mathbb{K}$. Seja $\alpha \in \mathbb{E}$ e considere o polinômio minimal $f = \sum_{i=0}^{m-1} a_i x^{n-1} + x_n$ de α sobre $\mathbb{K}$, em que $a_i \in \mathbb{K}, \forall i \in \{0, 1, ..., m-1\}$. Como cada a_i é algébrico sobre $\mathbb{F}$, segue que a extensão $\mathbb{L} = \mathbb{F}(a_0, a_1, ..., a_{n-1})$ é uma extensão finita de $\mathbb{F}$. Portanto $\mathbb{L}(\alpha)$ é extensão finita de $\mathbb{F}$, ou seja, $\mathbb{L}(\alpha)$ é uma exensão algébrica de $\mathbb{F}$, e como $\alpha \in \mathbb{L}(\alpha)$, obtemos que α é algébrico sobre $\mathbb{F}$. **(c.q.d)**

Dada uma extensão $\mathbb{F} \subseteq \mathbb{E}$ qualquer, podemos nos perguntar se existe algum corpo intermediário entre $\mathbb{F}$ e $\mathbb{E}$ que seja algébrico sobre $\mathbb{F}$. Essa dúvida, porém, é sanada com o próximo teorema.

Teorema 2.5. *Seja $\mathbb{F} \subseteq \mathbb{E}$ extensão de corpos e seja $A = \{\alpha \in \mathbb{E} \mid \alpha$ é algébrico sobre $\mathbb{F}\}$. Então A é um subcorpo de $\mathbb{E}$ e todo elemento de $\mathbb{E}$ que é algébrico sobre A pertence a A.*

Demonstração. Tome $\alpha, \beta \in A$. Como ambos são algébricos sobre $\mathbb{F}$, então $\mathbb{F} \subseteq \mathbb{F}(\alpha, \beta)$ é extensão finita de $\mathbb{F}$. Logo $\mathbb{F}(\alpha, \beta)$ é extensão algébrica. Daí, temos que $\mathbb{F}(\alpha, \beta) \subseteq A$, e como $\alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1}$ (se $\alpha \neq 0$) são elementos de $\mathbb{F}(\alpha, \beta)$, segue que também são elementos de A, donde conluímos que A é subcorpo de $\mathbb{E}$. Por fim, se $y \in \mathbb{E}$ é elemento algébrico sobre A, então $A(y)$ é extensão algébrica de A, e sendo A extensão algébrica de $\mathbb{F}$, concluímos, pela proposição (2.5), que $A(y)$ é extensão algébrica de $\mathbb{F}$, ou seja, y é algébrico sobre $\mathbb{F}$, ou ainda, $y \in A$, **(c.q.d)**

Denotaremos o corpo A do teorema acima por $\text{Alg}(\mathbb{E}/\mathbb{F})$. A proposição a seguir servirá de motivação para definir a noção de corpos algebricamente fechados.

Proposição 2.6. *Seja $\mathbb{K}$ um corpo. São equivalentes as seguintes afirmações:*
1) Todo polinômio não constante $f \in \mathbb{K}[x]$ tem pelo menos uma raiz em $\mathbb{K}$.
2) Todo polinômio irredutível em $\mathbb{K}[x]$ tem grau 1.
3) Todo polinômio não constante $g \in \mathbb{K}[x]$ decompõe-se num produto de fatores lineares em $\mathbb{K}[x]$.

Demonstração. (1) $\Rightarrow$ (2): Dado um polinômio f de grau maior do que um, podemos tomar α em $\mathbb{K}$ de modo que α seja uma raiz desse polinômio. Logo

$f = (x - \alpha)q$, com $\partial q \geq 1$, donde segue que f é redutível. Logo, para um polinômio ser irredutível, necessariamente seu grau deve ser igual a um. Portanto
(2) $\Rightarrow$ (3): Segue imediatamente do fato de $\mathbb{K}[x]$ ser domínio fatorial.
(3) $\Rightarrow$ (1): Evidente. **(c.q.d)**

Definição 2.10. *Todo corpo $\mathbb{K}$ que satisfaz qualquer uma das três afirmações anteriores chama-se corpo algebricamente fechado.*

O Teorema Fundamental da Álgebra pode ser enunciado da seguinte forma: *O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado.* O leitor poderá facilmente encontrar a demonstração desse teorema em [5] ou [7].

Teorema 2.6. *Se $\mathbb{K} \subseteq \mathbb{E}$ é extensão de corpos e $\mathbb{E}$ é algebricamente fechado, então $A = Alg(\mathbb{E}/\mathbb{K})$ é um corpo algebricamente fechado.*

Demonstração. Tome $f \in \mathbb{A}[x] \subseteq \mathbb{E}[x]$ polinômio não constante. Como $\mathbb{E}$ é algebricamente fechado, existe $\alpha \in \mathbb{E}$ tal que $f(\alpha) = 0$. Logo α é algébrico sobre A, donde segue, do teorema 2.5, que $\alpha \in A$, isto é, A é algebricamente fechado. **(c.q.d)**

Definição 2.11. *Uma extensão $\mathbb{E}$ de um corpo $\mathbb{F}$ chama-se um fecho algébrico de $\mathbb{F}$ se, e somente se, $\mathbb{K} \subseteq \mathbb{E}$ é uma extensão algébrica e $\mathbb{E}$ é algebricamente fechado.*

Exemplo 3. *Como $\mathbb{C}$ é algebricamente fechado e $\mathbb{Q} \subseteq \mathbb{C}$, segue, do teorema 2.6, que o conjunto $Alg(\mathbb{C}/\mathbb{Q})$ é algebricamente fechado. Além disso, sabemos que $\mathbb{Q} \subseteq Alg(\mathbb{C}/\mathbb{Q})$ é extensão algébrica. Portanto $\mathbb{L} = Alg(\mathbb{C}/\mathbb{Q})$ é um fecho algébrico de $\mathbb{Q}$. O corpo $\mathbb{L}$ chama-se corpo dos números algébricos e, certamente, um de nossos objetivos nessas notas trata-se de estudar as propriedades do mesmo. O teorema 2.1 nos mostra que este corpo é enumerável.*

Dado um corpo qualquer, é razoável nos perguntarmos se existe um fecho algébrico para este corpo. Os teoremas 2.5 e 2.6 nos mostram que se for possível estender este corpo a um corpo algebricamente fechado, então existirá, também, um fecho algébrico para este corpo. O teorema a seguir responde posititivamente a tal pergunta. A demonstração dele faz uso de um resultado conhecido como Lema de Zorn, o qual é equivalente ao axioma da escolha, que aceitaremos como verdadeiro, desde já. Enunciemos o lema em questão:

Lema de Zorn: Seja $(X, \leq)$ um conjunto parcialmente ordenado. Se toda cadeia em $(X, \leq)$ possui uma cota superior, então $(X, \leq)$ admite elemento maximal.

O leitor curioso encontrará bons textos sobre o tema acima em [5] e [4].

Teorema 2.7. *Todo corpo admite fecho algébrico.*

Demonstração. Seja $\mathbb{F}$ um corpo. Seja A um conjunto com um elemento para cada possível zero de um polinômio qualquer de $\mathbb{F}[x]$, isto é,
$A = \{w_{f,i} \mid f \in \mathbb{F}[x], i = 0, ..., \partial f\}$. Considere um conjunto Ω com mais elementos do que A (por exemplo, tome $\Omega = P(A)$.) Substituindo Ω por $\Omega \cup \mathbb{F}$, se necessário, podemos assumir que $\mathbb{F} \subset \Omega$. Defina o conjunto $S = \{\mathbb{E} | \mathbb{E} \subseteq \Omega$ é uma extensão algébrica de $\mathbb{F}\}$. Note que S é parcialemente ordenado pela relação de inclusão. Claramente, $S \neq \varnothing$, pois $\mathbb{F} \in S$. Considere uma cadeia $\mathbb{E}_1 \subseteq \mathbb{E}_2 \subseteq \cdots \subseteq \mathbb{E}_n \subseteq \cdots$ qualquer em S.

Afirmação: A união $\mathbb{E} = \bigcup_{n=1}^{\infty} \mathbb{E}_n$ é uma cota superior para esta cadeia.

Com efeito, tome $x, y \in \mathbb{E} = \bigcup_{n=1}^{\infty} \mathbb{E}_n$. Existem $i, j \in \mathbb{N}$ tais que $x \in \mathbb{E}_i$ e $y \in \mathbb{E}_j$. Seja $k = \max\{i, y\}$. Temos $\mathbb{E}_i \subseteq \mathbb{E}_k$ e $\mathbb{E}_j \subseteq \mathbb{E}_k$. Logo $x, y \in \mathbb{E}_k$, donde segue que $x - y, xy$ e x^{-1}(se $x \neq 0$) são elementos de $\mathbb{E}_k$, isto é, as operações adição e multiplicação estão bem definidas em $\mathbb{E}$ e todo elemento não nulo de tal conjunto possui inverso no mesmo. Os outros axiomas de corpo são, também, herdados do fato de que cada $\mathbb{E}_i$ é também um corpo Isso mostra que, de fato, $\mathbb{E}$ é um corpo pertencente ao conjunto S.
Portanto, toda cadeia em S possui cota superior. Pelo Lema de Zorn, segue que S possui elemento maximal. Seja $\overline{\mathbb{F}}$ tal elemento. Afirmo que $\overline{\mathbb{F}}$ é algebricamente fechado. De fato, suponha que não o seja. Então existe um polinômio $f \in \overline{\mathbb{F}}[x]$ que não possui raízes neste corpo. Nesse caso, tome $w \in \Omega \backslash \overline{\mathbb{F}}$ tal que $f(w) = 0$. Obtemos, daí, que $\overline{\mathbb{F}} \subseteq \overline{\mathbb{F}}(w)$ é uma extensão algébrica. Como $\mathbb{F} \subseteq \overline{\mathbb{F}}$ também é extensão algébrica (pois $\overline{\mathbb{F}} \in S$), concluímos, pela proposição 2.5, que $\mathbb{F} \subseteq \overline{\mathbb{F}}(w)$ é extensão algébrica, o que contradiz a maximalidade de $\overline{\mathbb{F}}$. Finalmente, obtemos que $\overline{\mathbb{F}}$ é um fecho algébrico de $\mathbb{F}$. **(c.q.d)**

Demonstra-se que o fecho algébrico é unico, a menos de isomorfismo. Isso significa que se $\mathbb{E}$ e $\mathbb{K}$ são fechos algébricos de $\mathbb{F}$, então $\mathbb{E} \cong \mathbb{K}$. O leitor pode encontrar encontrar a prova desse fato em [6] ou [4].

Definição 2.12. *Seja $\mathbb{F}$ um corpo, e $f \in \mathbb{F}[x]$ um polinômio não constante. Dizemos que uma extensão $\mathbb{E}$ de $\mathbb{F}$ é um corpo de decomposição de f (ou corpo de raízes de f) se, e somente se, vale que:*
a) f decompõe-se num produto de fatores lineares em $\mathbb{E}[x]$.
b) Se $\mathbb{L}$ é um corpo intermediário qualquer entre $\mathbb{K}$ e $\mathbb{E}$ satisfazendo a condição anterior, então $\mathbb{L} = \mathbb{E}$.

Segue, imediatamente da definição anterior, $\mathbb{E}$ é uma extensão finita, e portanto algébrica, de $\mathbb{K}$. Com efeito, note que $\mathbb{E} = \mathbb{K}(x_1, ..., x_n)$, em que $x_1, ..., x_n$ são as raízes do polinômio f do qual $\mathbb{E}$ é corpo de raízes, com $\partial f = n$. Como cada x_i é algébrico sobre $\mathbb{K}$, segue a afirmação anterior. Podemos dizer que o corpo de decomposição de f é o menor corpo que contém $\mathbb{K}$ e todas as raízes de f. O teorema a seguir é de extrema importância para se determinar a existêcia dos corpos de raízes de polinômios.

Teorema 2.8 (Kronecker)**.** *Se $f \in \mathbb{K}[x]$ é um polinômio irredutível e mônico, então existe uma extensão $\mathbb{K}(\alpha)$ do corpo $\mathbb{K}$, em que α é uma raiz de f.*

Demonstração. Seja $\mathbb{E} = \mathbb{K}[x]/(f)$. Como f é irredutível, então (f) é ideal maximal de $\mathbb{K}[x]$, donde segue que $\mathbb{E}$ é um corpo. Podemos considerar $\mathbb{K} \subseteq \mathbb{E}$ (de fato, basta observar que a projeção canônica $\phi : \mathbb{K}[x] \to \mathbb{E}$ restrita a $\mathbb{K} \subseteq \mathbb{K}[x]$). Todo elemento de $\mathbb{E}$ é da forma $g + (f)$, em que $g = \sum_{i=0}^{m} b_i x^i \in \mathbb{K}[x]$. Defina $\alpha = x + (f)$. Com efeito, se $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$, então, em $\mathbb{E}[x]$, temos que

$$f(\alpha) = f(x + (f)) = \sum_{i=0}^{n} (a_i + (f)) \cdot (x + (f))^i = \sum_{i=0}^{n} a_i x^i + (f) = f + (f) = (f) = 0_{\mathbb{E}},$$

donde segue que α é uma raiz de f. **(c.q.d)**

Prova-se que a extensão $\mathbb{K}(\alpha)$ acima é única, a menos de $\mathbb{K}$-isomorfismo. Também, pelo teorema acima é possível demonstrar que todo polinômio não constante $g \in \mathbb{K}[x]$

admite um corpo de raízes sobre $\mathbb{K}$, e, além disso, este corpo é determinado, a menos de $\mathbb{K}$-isomorfismo. Podemos, de forma parecida, definir o corpo de decomposição de uma família Λ de polinômios. Esses fatos fogem do nosso objetivo principal e não serão demonstradas, por hora. O leitor se convecerá desses fatos em, por exemplo, [4] ou [6].

Exemplo 4. *Tome $f = x^2 + bx + c \in \mathbb{Q}[x]$. Se f é redutível em $\mathbb{Q}$, então $\mathbb{Q}$ é corpo de decomposição de f. Caso contrário, $\mathbb{K} = \mathbb{Q}(\sqrt{b^2 - 4c})$ será corpo de decomposição de f sobre $\mathbb{Q}$.*

Exemplo 5. *Considere $\Lambda = \{x^2 - p : p \geq 2 \text{ primo}\} \subseteq \mathbb{Q}[x]$. Então $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, ...\}$ é um corpo de decomposição para Λ.*

Por fim, definiremos os conceitos de separabilidade e normalidade, cuja importância se manifesta consideravelmente no estudo da Teoria de Galois.

Definição 2.13. *Seja $\mathbb{K}$ um corpo e $f \in \mathbb{K}[x]$ um polinômio. Dizemos que f é separável se, e somente se, f e sua derivada f' são primos entre si.*

Prova-se que este fato é equivalente ao fato de todas as raízes de f serem simples, isto é, terem multiplicidade 1. Uma extensão algébrica $\mathbb{F} \subseteq$ será chamada de *separável* quando todo elemento de $\mathbb{E}$ for raiz de um polinômio separável sobre $\mathbb{F}$.

Definição 2.14. *Seja $\mathbb{F}$ um corpo e Ω um corpo algebricamente fechado contendo $\mathbb{F}$. Uma extensão finita $\mathbb{F} \subseteq \mathbb{E}$ é dita ser normal se satisfizer alguma das seguintes condições equivalentes:*
a) Para todo $\mathbb{F}$-isomorfismo σ de $\mathbb{E}$ em Ω, temos que $\sigma(\mathbb{E}) = \mathbb{E}$
b) Se $\alpha \in \mathbb{E}$ é raiz de um polinômio $p \in \mathbb{F}[x]$ irredutível, então $\mathbb{E}$ contém todas as raízes de p.
c) $\mathbb{E}$ é corpo de decomposição de uma família $\Lambda \subseteq \mathbb{F}[x]$ de polinômios não constantes.

As equivalências da definição anterior, bem como a demonstração da equivalência da definição anterior pode ser encontrada em [4] ou [6]. A proposição a seguir será útil para o último capítulo, e por isso será demonstrada abaixo.

Proposição 2.7. *Todo polinômio irredutível com coeficientes num corpo de característica zero é separável.*

Demonstração. Seja $f \in \mathbb{F}[x]$ irredutível e $\mathbb{F}$ corpo de característica zero. A proposição é óbvia no caso $\partial f = 1$. Se $\partial f > 1$, então $\partial f' \geq 1$. Ora, os únicos fatores irredutíveis de f são 1 e f. Como $\partial f > \partial f' \geq 1$, segue que o único fator que f e f' podem ter em comum deve ser uma constante, isto é, $\text{mdc}(f, f') = 1$. Portanto f é separável. **(c.q.d)**

Definição 2.15. *Uma extensão chama-se Galoisiana se for normal e separável.*

2.5 Módulos

Definição 2.16. *Seja R um anel comutativo. Dizemos que um grupo abeliano $(M, +)$ é um R-módulo se existir uma operação externa $\cdot : R \times M \to M$ (usualmente conhecida como multiplicação), satisfazendo:*
1) $a \cdot (x + y) = a \cdot x + a \cdot y,\ (a + b) \cdot x = a \cdot x + b \cdot x$
2) $(a \cdot b) \cdot x = a \cdot (b \cdot x),\ 1 \cdot x = x$
para quaisquer $a, b \in R$ e $x, y \in M$.

Exemplo 6. *Todo grupo abeliano aditivo A é um $\mathbb{Z}$-módulo, definindo-se $(\pm n) \cdot x = \pm 1(x + x + \cdots + x)$, para quaisquer $n \in \mathbb{N}$, $x \in A$.*

Exemplo 7. *O produto cartesiano de R-módulos também é um R-módulo, tomando-se as operações componente a componente.*

Exemplo 8. *Todo anel R é um R-módulo. Basta notar que $(R, +)$ é um grupo abeliano, e tomar como multiplicação a própria multiplicação de R como estrutura de anel.*

De forma análoga ao que fazemos para as estruturas de aneis e grupos, define-se os conceitos de submódulo, módulos quocientes e homomorfismos entre módulos.

Definição 2.17. *Seja M um R-módulo. Um grupo abeliano $N \subseteq M$ é um R-submódulo de M se N é um R-módulo, com a operação externa induzida de M.*

Exemplo 9. *Seja M um R-módulo, e seja I um ideal de R. Dado $m \in M$, temos que $mI = \{mi : i \in I\}$ é um R-submódulo de M.*

Definição 2.18. *Seja M um R-módulo e N um R-submódulo de M. Dados $m_1, m_2 \in M$, definimos a relação $\equiv (mod\ N)$ congruência módulo N pondo $m_1 \equiv m_2 (mod N) \Leftrightarrow m_1 - m_2 \in N$.*

É facilmente verificável que a relação acima é uma relação de equivalência. Daqui por diante, se m_1 e m_2 pertencerem a mesma classe de equivalência, escreveremos apenas $m_1 + N = m_2 + N$. Isto é: $m_1 + N = m_2 + N \Leftrightarrow m_1 - m_2 \in N$.

Definição 2.19. *Seja M um R-módulo e N um R-submódulo de M. Entendemos o conjunto quociente $M/N = \{m + N : m \in M\}$ como sendo o conjunto de todas as classes de equivalência módulo N.*

O leitor não terá dificuldade em perceber que o conjunto quociente M/N é um R-módulo definindo-se a operação $\cdot : R \times M/N \to M/N$ como sendo $r \cdot (m + N) = rm + N$, para todo $r \in R$. Dessa forma, dizemos que M/N é um R-módulo quociente.

Definição 2.20. *Sejam M e N dois R-módulos. Uma aplicação $f : M \to N$ chama-se um homomorfismo de R-módulos se f satisfaz:*
1) $f(x + y) = f(x) + f(y)$
2) $f(rx) = rf(x)$,
para quaisquer $x, y \in M$, $r \in R$.

As propriedades de homomorfismos entre R-módulos são análogas às propriedades de homomorfismos de aneis e grupos. Os enunciados e as respectivas demonstrações dessas propriedades são cuidadosamente descritas em [3].

Definição 2.21. *Um R-módulo M é dito ser finitamente gerado se existirem $x_1, ..., x_n \in M$ tais que $M = R \cdot x_1 + ... + R \cdot x_n$. Nesse caso, dizemos que $x_1, ..., x_n$ formam um sistema de geradores de M.*

Definição 2.22. *Seja M um R-módulo. Os elementos $y_1, ..., y_n \in M$ são linearmente independentes sobre R se, para quaisquer $a_1, ..., a_n \in R$, a igualdade $a_1y_1 + ... + a_ny_n = 0$ implicar que $a_1 = \cdots = a_n = 0$. Se, além disso, $y_1, ..., y_n$ formarem um conjunto de geradores de M, então o conjunto $\{y_1, ..., y_n\}$ é dito ser uma base de M.*

Ressaltamos que, ao contrário da estrutura de espaço vetorial, nem todo módulo finitamente gerado possui uma base. Um R-módulo que possui uma base chama-se *Módulo Livre.*

Em particular, se S é um anel, então todo anel R que contém S será considerado um S-módulo, sendo o produto externo $s \cdot x$, em que $x \in R$ e $s \in S$. A estrutura de módulo se fará de extrema importância no capítulo que se segue.

3 Anéis de Inteiros algébricos

3.1 Inteiros Algébricos

Chamaremos de número algébrico a qualquer $x \in \mathbb{C}$ que é algébrico sobre o corpo dos números racionais $\mathbb{Q}$. O fecho algébrico de $\mathbb{Q}$, denotado por $\overline{\mathbb{Q}}$, denomina-se corpo dos números algébricos. Mais precisamente, qualquer extensão algébrica dos racionais é dito ser um corpo de números algébricos. A partir de agora, um corpo de números algébricos será qualquer extensão finita L de $\mathbb{Q}$. Nosso objetivo é mostrar que todo corpo de números algébricos da forma $L = \mathbb{Q}(\alpha)$ (isto é: toda extensão simples de $\mathbb{Q}$) possui um subanel I_L, cujo corpo de fração é L. Esse subanel é o anel dos elementos de L que são "inteiros"sobre $\mathbb{Z}$. A definição a seguir generaliza o conceito de inteiro algébrico.

Definição 3.1. *Sejam R um anel e S um subanel de R. Dizemos que um elemento $\alpha \in R$ é inteiro sobre S se existe um polinômio mônico $f \in S[x]$ tal que $f(\alpha) = 0$.*

Em particular, todo elemento de S é inteiro sobre S. Alguns autores costumam se referir a um elemento inteiro sobre S como sendo um elemento *integral* sobre S.

Exemplo 10. *No caso em que $S = \mathbb{Z}$ e $R = \mathbb{C}$, os inteiros sobre $\mathbb{Z}$ são chamados de inteiros algébricos. Por exemplo, os números $i = \sqrt{-1}, \sqrt{2}, \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$ são inteiros algébricos, pois são raízes dos polinômios mônicos $x^2+1, x^2-2, x^n-1 \in \mathbb{Z}[x]$, respectivamente.*

No caso em que $S = \mathbb{L}$ e $R = \mathbb{K}$ são corpos, um elemento $\alpha \in \mathbb{K}$ será inteiro sobre $\mathbb{L}$ se, e somente se, α for algébrico sobre $\mathbb{L}$. Uma importante motivação para a definição acima é a proposição a seguir, a qual caracteriza os elementos de $\mathbb{Z}$ como sendo exatamente os inteiros algébricos em $\mathbb{Q}$.

Proposição 3.1. *Se $\theta \in \mathbb{Q}$ é inteiro algébrico, então $\theta \in \mathbb{Z}$.*

Demonstração. Seja $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ polinômio mônico tal que $p(\theta) = 0$. Escreva $\theta = \dfrac{b}{c}$, com $b, c \in \mathbb{Z}$ coprimos e $c \neq 0$. Temos

$$p(\theta) = 0 \Leftrightarrow p\left(\frac{b}{c}\right) = 0 \Leftrightarrow \left(\frac{b}{c}\right)^n + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \cdots + a_1\left(\frac{b}{c}\right) + a_0 = 0$$

$$\Leftrightarrow b^n + a_{n-1}b^{n-1}c + a_{n-2}b^{n-2}c^2 + \cdots + a_1bc^{n-1} + a_0c^n = 0.$$

Com efeito, o número c divide todos os termos a partir do segundo. Logo c também divide o primeiro, isto é, $c|b^n$. Como b e c são coprimos, isto só pode ocorrer quando $c = \pm 1$, donde segue que $\theta = \pm b \in \mathbb{Z}$. **(c.q.d)**

Uma importante relação entre números algébricos e inteiros algébricos está descrita na proposição a seguir. Basicamente, ela nos diz que podemos "limpar os denominadores"de um dado número algébrico arbitrário.

Proposição 3.2. *Se θ é um número algébrico, então existe a inteiro não nulo tal que $a\theta$ é um inteiro algébrico.*

Demonstração. Tome $f \in \mathbb{Q}[x]$ tal que $f(\theta) = 0$. Escreva
$f(x) = a_n x^n + \cdots + a_1 x + a_0$. Se multiplicarmos ambos os lados da equação $f(\theta) = 0$ por $(a_n)^{n-1}$, obtemos que $(a_n\theta)^n + a_{n-1}(a_n\theta)^{n-1} + \cdots + a_1(a_n)^{n-2}(a_n\theta) + a_0(a_n)^{n-1} = 0$. Podemos, então, tomar $a = (a_n)^{n-1}$, percebendo que $a\theta$ é raiz do polinômio mônico $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1(a_n)^{n-2}x + a_0(a_n)^{n-1}x$ **(c.q.d)**

3.2 O anel I_L

O teorema a seguir busca mostrar que o conjunto dos elementos de R que são inteiros sobre S forma um subanel $I_S(R)$ de S. Antes dele, vamos enunciar, sem demonstração, a seguinte proposição:

Proposição 3.3. *Seja S um anel e seja $A = (a_{ij})$ uma matriz quadrada, com $a_{ij} \in S$. Se $a = \det(A)$, então existem $a_{ij}^* \in S$ tais que $\sum_{j=1}^{n} a_{ij}^* \cdot a_{jk} = a \cdot \delta_{ik}$ em que*

$$\delta_{ik} = \begin{cases} 1; \ sei = k \\ 0; \ sei \neq k \end{cases} \quad e \ 1 \leq i, k \leq n.$$

A demonstração dessa proposição pode ser encontrada em [2]. Passemos, agora, ao teorema citado anteriormente.

Teorema 3.1. *Seja R um anel, S subanel de R e α um elemento de R. São equivalentes as seguintes afirmações:*
(i) α é inteiro sobre S.
(ii) $S[\alpha]$ é um S-módulo finitamente gerado.
(iii) Existe um subanel R' de R que é um S - módulo finitamente gerado, com $\alpha \in R'$.
(iv) Existe um S-módulo finitamente gerado M tal que $\alpha \cdot M \subseteq M$ e que $y \cdot M \neq \{0\}$, para todo $y \in M \backslash \{0\}$.

Demonstração. (i)⇒(ii): Tome $p = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in S[x]$ tal que $\alpha \in R$ é raiz de p. Seja $M = S + S\alpha + S\alpha^2 + ... + S\alpha^{n-1}$. Evidentemente, $M \subseteq S[\alpha]$.
Afirmação: Para todo $k \in \mathbb{N}$, temos que $1, \alpha, \alpha^2, ..., \alpha^{n-1+k} \in M$.
Vamos usar indução em $k \in \mathbb{N}$ para demonstrar a afirmação acima, a qual é óbvia para o caso $k = 0$. Suponha que a afirmação seja verdadeira, para todo $k \leq m$. Como α é raiz de p, temos $\alpha^n = -a_0 - a_1\alpha - ... - a_{n-1}\alpha^{n-1}$. Tome $b_0, ..., b_{n-1} \in S$ tais que $\alpha^{n-1+m} = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}$. Agora, $\alpha^{n+m} = \alpha^{n-1+m} \cdot \alpha$, ou seja, $\alpha^{n+m} = (b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}) \cdot \alpha =$
$= b_0\alpha + ... + b_{n-1}\alpha^n = b_0\alpha + ... + b_{n-1}(-a_0 - a_1\alpha - ... - a_{n-1}\alpha^{n-1}) =$
$= b_0\alpha + ... - b_{n-1}a_0 - b_{n-1}a_1\alpha - ... - b_{n-1}a_{n-1}\alpha^{n-1} =$
$= -b_{n-1}a_0 + (b_0 - b_{n-1}a_1)\alpha + ... + (b_{n-2} - b_{n-1}a_{n-1})\alpha^{n-1} \in M$, o que mostra a afirmação. Segue que todas as potências de α são elementos de M, donde $S[\alpha] \subseteq M$.
(ii)⇒(iii) De fato, basta tomar $R' = S[\alpha]$.
(iii)⇒(iv) Tome $M = R'$. Então M é um S-módulo finitamente gerado, e como $\alpha \in M$, temos $\alpha \cdot M \subseteq M$. Também, qualquer $y \in M \backslash \{0\}$ é tal que $y = y \cdot 1 \in y \cdot S'$.
(iv)⇒(i) Seja $\beta_1, ..., \beta_r$ um conjunto de geradores de M. Como $\alpha \cdot M \subseteq M$, então, para cada $1 \leq j, k \leq r$, existe $a_{jk} \in S$ tais que $\alpha \cdot \beta_j = \sum_{k=1}^{r} a_{jk}\beta_k$. Segue que $\beta_1, ..., \beta_r$

é solução do sistema $\begin{pmatrix} -a_{11}+\alpha & -a_{12} & \cdots & -a_{1r} \\ -a_{21} & -a_{22}+\alpha & \cdots & -a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{r1} & -a_{r2} & \cdots & -a_{rr}+\alpha \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

Note que as entradas $e_{jk} = -a_{jk} + \alpha\delta_{jk}$ da matriz do sistema acima pertencem ao anel $S[\alpha]$. Seja $D = \det(e_{jk}) \in S[\alpha]$. Pela proposição anterior, existem $e^*_{ij} \in S[\alpha]$ tais que $\sum_{j=1}^{r} e^*_{ij} \cdot e_{jk} = D \cdot \delta_{ik}$, $(i, k = 1, ..., r)$. Daí, obtemos que

$$0 = \sum_{j,k=1}^{r} e^*_{ij} \cdot e_{jk} \cdot \beta_k = \sum_{k=1}^{r} D \cdot \delta_{ik} \cdot \beta_k = D \cdot \beta_k,$$

em que $1 \leq i \leq r$. Portanto $D \cdot M = \{0\}$, ou seja, $D = 0$. Com efeito, concluímos que α é raiz do polinômio mônico $\det(-a_{jk} + x \cdot \delta_{jk})$, **(c.q.d)**

Corolário 3.1. *Se $\alpha_1, ..., \alpha_n \in R$ forem tais que α_1 é inteiro sobre S e α_i é inteiro sobre $S[\alpha_1, \cdots, \alpha_{i-1}]$, para todo $i \in \{2, \cdots, n\}$, então $S[\alpha_1, ..., \alpha_n]$ é um S-módulo finitamente gerado.*

Demonstração. O teorema anterior demonstra o caso $n = 1$. Por hipótese de indução, entenderemos que $S_n = S[\alpha_1, ..., \alpha_n]$ é um S-módulo finitamente gerado, sempre que $n < k$, α_1 inteiro sobre S e α_i inteiro sobre $S[\alpha_1, \cdots, \alpha_{i-1}]$, para todo $2 \leq i \leq k-1$. Agora, suponha que $\alpha_1, ..., \alpha_k \in R$ são tais que α_1 é inteiro sobre S e α_j é inteiro sobre $S[\alpha_1, \cdots, \alpha_{j-1}]$, para cada $2 \leq j \leq k-1$. Da hipótese de indução, vem que $S[\alpha_1, ..., \alpha_{k-1}]$ possui sistema finito de geradores em S. Seja $\{x_1, ..., x_r\}$ conjunto de tais elementos. Como α_k é inteiro sobre $S_{k-1} = S[\alpha_1, \cdots, \alpha_{k-1}]$, temos, pelo teorema, que $S_{k-1}[\alpha_k] = S[\alpha_1, \cdots, \alpha_k]$ é um S_{k-1} módulo finitamente gerado. Tome $y_1, \cdots, y_m \in S_{k-1}$ sistema de geradores de S_{k-1}. Obtemos que $S_{k-1}[\alpha_k] = y_1S_{k-1} + \cdots + y_mS_{k-1} = y_1(x_1S + x_2S + \cdots + x_rS) + \cdots + y_m(x_1S + x_2S + \cdots + x_rS) = y_1x_1S + y_1x_2S + \cdots + y_1x_rS + \cdots + y_mx_1S + \cdots `+ y_mx_rS$. Portanto, o conjunto formado por todos os produtos da forma x_iy_j, com $1 \leq i \leq r$ e $1 \leq j \leq m$, é um conjunto de geradores de $S[\alpha_1, \cdots, \alpha_k]$, e este é um S-módulo finitamente gerado.**(c.q.d)**

Em particular, se $\alpha_1, \cdots, \alpha_n \in R$ são inteiros sobre S, o corolários nos dá que $S[\alpha_1, \cdots, \alpha_n]$ é um S-módulo finitamente gerado. A partir de agora, vamos denotar por $I_R(S)$ o conjunto dos elementos de R que são inteiros sobre S. O corolário que se segue mostra que, de fato, tal conjunto é um anel, conforme havíamos anunciado no início do capítulo.

Corolário 3.2. *$I_R(S)$ é um subanel de R que contém S.*

Demonstração. É claro que $S \subseteq I_R(S) \subseteq R$. Sejam $\alpha, \beta \in I_R(S)$. Do corolário anterior, temos que $S[\alpha, \beta]$ é um S-módulo finitamente gerado. Agora, note que $\alpha - \beta, \alpha\beta \in S[\alpha, \beta]$. Além disso, $S \subseteq S[\alpha, \beta] \subseteq R$. A equivalência entre os itens (i) e (iii) do teorema anterior nos mostra que $\alpha - \beta$ e $\alpha\beta$ são inteiros sobre S, donde segue o resultado.**(c.q.d)**

Corolário 3.3. *Se R' é subanel de R e R' é um S-módulo finitamente gerado, então $R' \subseteq I_R(S)$.*

Demonstração. Segue imediatamente do teorema. **(c.q.d)**

Definição 3.2. *Sejam R um anel e S subanel de R. O anel $I_R(S)$ chama-se o fecho inteiro de S em R.*

Definição 3.3. *Sejam R um anel e S subanel de R. Se $I_R(S) = S$, então S é dito ser integralmente fechado em R. Se $I_R(S) = R$, diremos que S é inteiro sobre R.*

No caso em que $S = \mathbb{K}$ e $R = \mathbb{L}$, temos que $I_{\mathbb{L}}(\mathbb{F})$ é um subcorpo de $\mathbb{L}$. Note que $I_{\mathbb{L}}(\mathbb{K}) = \mathbb{K}$ se, e somente se, $\mathbb{K}$ for algebricamente fechado em $\mathbb{L}$, e $I_{\mathbb{L}}(\mathbb{K}) = \mathbb{L}$ se, e somente se, $\mathbb{L}$ é extensão algébrica. No caso em que $R = \mathbb{L}$ é um corpo de números algébricos, o anel $I_{\mathbb{L}}(\mathbb{Z})$ é chamado o anel dos inteiros algébricos de $\mathbb{L}$ e vamos denotá-lo por I_L.

Exemplo 11. *Pela proposição (3.1), o anel $I_{\mathbb{Q}}(\mathbb{Z}) = I_{\mathbb{Q}}$ coincide com o anel dos números inteiros. Isto significa que $\mathbb{Z}$ é integralmente fechado em $\mathbb{Q}$.*

O exemplo anterior nos pode ser generalizado para o seguinte teorema, cuja demonstração é semelhante à demonstração da proposição (3.1).

Teorema 3.2. *Todo domínio de fatoração única é integralmente fechado no seu corpo de frações.*

Demonstração. Seja R um domínio fatorial e F = Fr(R) seu corpo de frações. Dado $x \in$ Fr(R), podemos tomar $a, b \in R$, com $b \neq 0$ e mdc$(a, b) = 1$ tais que $x = a \cdot b^{-1}$. Se $x \in I_F(R)$, então devem existir $c_1, ..., c_n \in R$ para os quais $x^n + c_1 x^{m-1} + ... + c_{n-1}x + c_n = 0$. Multiplicando esta igualdade por b^n, obtemos $a^n + c_1 \cdot b \cdot a^{n-1} + ... + c_n \cdot b^n = 0$. Portanto, b é um divisor de a^n. Como mdc$(a, b) = 1$, segue que $b \in R^X$, donde vem que $x \in R$, **(c.q.d)**

Podemos mostrar que a propriedade de ser inteiro é transitiva, por meio da:

Proposição 3.4. *Sejam S um subanel de T e T subanel de R. São equivalentes:*
(i) T é inteiro sobre S e R é inteiro sobre T.
(ii) R é inteiro sobre S.

Demonstração. Tome $\theta \in R$. Como R é inteiro sobre T, existem $t_0, ..., t_{n-1} \in T$ tais que $t_0 + t_1\theta + ... + t_{n-1}\theta^{n-1} + \theta^n = 0$. Agora, θ é inteiro sobre $S' = S[t_0, ..., t_{n-1}]$, ou seja, $S'[\theta] = (S[t_0, ..., t_{n-1}])[\theta] = S[t_0, ..., t_{n-1}, \theta]$ é S'-módulo finitamente gerado. Agora, como $t_0, ..., t_{n-1} \in T$ são inteiros sobre S, então, pelo corolário (3.1), temos que S' é S-módulo finitamente gerado. Isto significa que $S'[\theta]$ também o é, pois θ é inteiro sobre S'. Finalmente, o teorema (3.1) assegura que θ é inteiro sobre S, o que demonstra que R é inteiro sobre S. Reciprocamente, suponha R inteiro sobre S. Como $T \subseteq R$, então, em particular, todo elemento de T é inteiro sobre S, donde vem que T é inteiro sobre S. Todo polinômio de $S[x]$ pertence a $T[x]$. Logo, se um elemento de R for inteiro sobre S, também o será sobre T, isto é, R é inteiro sobre T. **(c.q.d)**

O teorema (3.1) nos dá, juntamente com a proposição acima, uma relação entre todos os subaneis de um anel R, a qual também justifica o fato de $I_R(\,)$ ser uma operação de fecho, conforme nos diz a:

Proposição 3.5. *Seja Ψ o conjunto dos subaneis de um anel R. Então a aplicação $\Phi : \Psi \to \Psi$, que associa cada subanel $S \in \Psi$ ao subanel $\Phi(S) = I_R(S)$ é tal que $S \subseteq I_R(S) = I_R(I_R(S))$ e, além disso, se $S \subseteq S'$, então $\Phi(S) \subseteq \Phi(S')$.*

Demonstração. É claro que $I_R(S) \subseteq I_R(I_R(S))$, qualquer que seja $S \in \Psi$. Temos $I_R(S)$ inteiro sobre S (por definição) e $I_R(I_R(S))$ inteiro sobre $I_R(S)$, donde segue, pela proposição acima, que $I_R(I_R(S))$ é subanel de T inteiro sobre S.

Portanto $I_R(I_R(S)) \subseteq I_R(S)$, ou seja, $I_R(I_R(S)) = I_R(S)$. A última afirmação é evidente. **(c.q.d)**

Podemos, agora, obter uma relação interessante entre extensões de corpos e os resultados obtidos até aqui, aplicados a domínios.

Teorema 3.3. *Sejam R e S domínios, com R inteiro sobre S. A fim de que S seja um corpo, é necessário e suficiente que R também o seja.*

Demonstração.($\Rightarrow$) Por hipótese, S é um corpo e R é um domínio, inteiro sobre S. Dado $\alpha \in R$, temos que $S[\alpha]$ é S-módulo finitamente gerado. Como S é um corpo, segue que $S[\alpha]$ é espaço vetorial sobre S. Defina uma aplicação $\phi : S[\alpha] \to S[\alpha]$ pondo $\phi(x) = x \cdot \alpha$. É evidente que ϕ é S-linear e que $x \in \ker(\phi) \Leftrightarrow x \cdot \alpha = 0 \Leftrightarrow x = 0$, pois R é um domínio de integridade e $\alpha \neq 0$. Segue que ϕ é injetiva. Como $\dim(S[\alpha]) < \infty$, temos que ϕ é sobrejetiva, isto é, ϕ define uma bijeção em $S[\alpha]$. Sendo $1 \in S[\alpha]$, deve existir $\beta \in S[\alpha]$ tal que $\phi(\beta) = 1$, ou ainda, $\beta\alpha = 1$. Daí, temos $\beta = \alpha^{-1}$. Portanto todo elemento de R possui inverso, donde vem que R é corpo.
($\Leftarrow$) Por hipótese, R é corpo inteiro sobre S. Se $\theta \in S \subseteq R$, então θ admite inverso em R. Logo, existem $a_0, ..., a_{n-1} \in S$ tais que $a_0 + a_1\theta^{-1} + ... + a_{n-1}(\theta^{-1})^{n-1} + (\theta^{-1})^n = 0$. Multiplicando esta igualdade por θ^{n-1}, obtemos
$\theta^{-1} = -(a_{n-1} + ... + a_1\theta^{n-2} + a_0\theta^{n-1}) \in S$, donde segue que S é corpo. **(c.q.d)**

Exemplo 12. *Seja F_n o n-ésimo número de Fibonacci. Sejam $m, n \in \mathbb{N}$ tais que $m \mid n$, isto é, $n = mk$, com $k \in \mathbb{N}$. Prova-se que uma fórmula explícita para esta sequência é dada por $F_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$, em que $\alpha = \dfrac{1+\sqrt{5}}{2}$ e $\beta = \dfrac{1-\sqrt{5}}{2}$ são as raízes de $x^2 - x - 1 = 0$. Temos*

$$\frac{F_n}{F_m} = \frac{F_{km}}{F_m} = \frac{\alpha^{km} - \beta^{km}}{\alpha^m - \beta^m} = (\alpha^m)^{k-1} + (\alpha^m)^{k-2}(\beta^m) + ... + (\beta^m)^{k-1}.$$

Como α, β são inteiros algébricos, segue que $\dfrac{F_n}{F_m}$ também o é, ou seja, $\dfrac{F_n}{F_m} \in \mathbb{Z}$, ou ainda: $F_m \mid F_n$. Concluímos, daí, a seguinte propriedade sobre a sequência de Fibonacci: $m \mid n \Rightarrow F_n \mid F_m$.

3.3 Traço, Norma e Discriminante

Sejam R e S aneis com $S \subseteq R$, sendo R um S-módulo finitamente gerado. Seja $\{e_1, ..., e_n\}$ base de R sobre S e seja $\phi : R \to R$ endomorfismo de S-módulos. Para cada $1 \leq i, j \leq n$, podemos tomar $a_{ij} \in S$ tais que

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} \phi(e_1) \\ \phi(e_2) \\ \vdots \\ \phi(e_n) \end{pmatrix}$$

Definição 3.4. *Sejam R e S aneis, e $\phi : R \to R$, como acima.*
(1) O traço de ϕ é definido por $Tr_{R|S}(\phi) = \sum_{i=1}^{n} a_{ii}$.
(2) Definimos a norma de ϕ como sendo $N_{R|S}(\phi) = \det(a_{ij})$.
(3) O polinômio característico de ϕ é o polinômio dado por $\det(xI_n - |a_{ij}|)$.

A teoria de álgebra linear assegura que as aplicações norma e traço são, respectivamente, aditivas e multiplicativas. Isto é: Dados $\phi, \psi : R \to R$ endomorfismo de S-módulos, temos:
1) $Tr_{R|S}(\phi + \psi) = Tr_{R|S}(\phi) + Tr_{R|S}(\psi)$.
2) $N_{R|S}(\phi \circ \psi) = N_{R|S}(\phi) \cdot N_{R|S}(\psi)$.

A seguir, vamos extender as definições acima para um elemento genérico de R, as quais são as definições mais usadas.

Definição 3.5. *Sejam R e S aneis com $S \subseteq R$ e $\alpha \in R$. Seja $\phi_\alpha : R \to R$ endomorfismo de S-módulos dado por $\phi_\alpha(x) = \alpha \cdot x$. Definimos:*
1) O traço de (α) como sendo o traço de ϕ_α.
2) A norma de α como sendo a norma de ϕ_α.
3) O polinômio característico de α como sendo o polinômio característico de ϕ_α.

Segue, diretamente das definições acima, e do fato de ϕ_α ser homomorfismo, a seguinte proposição:

Proposição 3.6. *Sejam R e S aneis com $S \subseteq R$, e sejam $\alpha, \beta \in R$ e $a \in S$. Suponha que a base de R sobre S é formada por n elemetos. Então, vale que:*
1) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
2) $Tr(a\alpha) = aTr(\alpha)$
3) $Tr(a) = na$
4) $N(\alpha\beta) = N(\alpha)N(\beta)$
5) $N(a) = a^n$
6) $N(a\alpha) = aN(\alpha)$

Temos, também, que a soma e o produto das raízes do polinômio característico são iguais, em módulo, ao traço e a norma, respectivamente. Na próxima seção, mostraremos exemplos de normas e traços em aneis quadráticos, os quais são os exemplos mais importantes de manipulação das definições acima. Prova-se, também, que o polinômio característico de qualquer elemento de um corpo $\mathbb{L}$ sobre um corpo $\mathbb{K}$ é igual a $I(\alpha, \mathbb{K})^m$, em que $m = [\mathbb{L} : \mathbb{K}[\alpha]]$. Para demonstração, ver, por exemplo, [6].

Definição 3.6. *Dizemos que um dominio R é integralmente fechado se for integralmente fechado em seu corpo de frações.*

Em particular, se $S = \mathbb{Z}$, e $\mathbb{L}$ é uma extensão de $\mathbb{Q}$, observamos que $\mathbb{Z}$ é integralmente fechado e está contido em qualquer subanel de I_L. Podemos estabelecer uma importante relação entre a norma de um elemento e as propriedadades desse elemento. Para tanto, vamos mostrar primeiramente que, para qualquer elemento de S, sua norma e seu polinômio característico pertencem a $\mathbb{Z}$, como nos informa a:

Proposição 3.7. *Seja L um corpo de números algébricos .*
1) Se $f, g \in \mathbb{Q}[x]$ são mônicos e $f \cdot g \in \mathbb{Z}[x]$, então $f, g \in \mathbb{Z}[x]$.
2) Para qualquer $\gamma \in I_L$, temos que $I(\gamma, \mathbb{Q}) \in \mathbb{Z}[x]$

Demonstração. 1) Sejam $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m \in \mathbb{C}$ tais que
$f = (x - \alpha_1) \cdots (x - \alpha_n)$ e $g = (x - \beta_1) \cdots (x - \beta_m)$. Como $f \cdot g \in \mathbb{Z}[x]$, segue que $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m \in I_{\mathbb{C}}$. Portanto, os coeficientes de f e g estão em
$I_{\mathbb{C}} \cap \mathbb{Q} = I_{\mathbb{Q}} = \mathbb{Z}$.
2) Com efeito, se $\gamma \in I_L$, então m é raiz de um polinômio f, mônico, com coeficientes

em $\mathbb{Z}$. Tal polinômio é, certamente, múltiplo do polinômio minimal de γ em $\mathbb{Q}$, donde segue que este também pertence a $\mathbb{Z}[x]$. **(c.q.d)**

Concluímos que o polinômio característico de γ também mora em $\mathbb{Z}[x]$, e por consequência, a norma e o traço de γ também (De fato, $N(m) = (-1)^n \cdot a_0$, em que $a_0 \in \mathbb{Z}$ é o coeficiente independente do polinômio característico de m, cujo grau é n). A partir disso, provemos o:

Teorema 3.4. *Sejam $\mathbb{L}$ um corpo de números algébricos e S um subanel de I_L. Para qualquer $\alpha \in S$, temos:*
1) $N_{\mathbb{L}|\mathbb{Q}}(\alpha)$ é um múltiplo de α em S.
2) $\alpha \in S^X$ se, e somente se, $|N_{\mathbb{L}|\mathbb{Q}}(\alpha)| = 1$.
3) Se $|N_{\mathbb{L}|\mathbb{Q}}(\alpha)|$ for primo, então α será irredutível em S.

Demonstração. 1) Seja $f = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ o polinômio característico de α sobre a extensão $\mathbb{Q} \subseteq \mathbb{L}$, do qual α é uma raiz. Já sabemos que $f \in \mathbb{Z}[x]$. Temos, também, que $N_{\mathbb{L}|\mathbb{Q}}(\alpha) = (-1)^n \cdot a_0$. Com efeito,

$$\begin{aligned}\alpha^{-1} \cdot N_{\mathbb{L}|\mathbb{Q}}(\alpha) = \alpha^{-1} \cdot (-1)^n \cdot a_0 = \alpha^{-1} \cdot (-1)^{n-1} \cdot (-a_0) = \\ = \alpha^{-1} \cdot (-1)^{n-1} \cdot (\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha) = \\ = (-1)^{n-1} \cdot (\alpha^{n-1} + a_{n-1}\alpha^{n-2} + ... + a_1) \in \mathbb{Z},\end{aligned}$$

donde segue o item 1.
2) Suponha $\alpha \in S^X$. Tome $\beta \in S$ tal que $\alpha\beta = 1$. Temos $N(\alpha\beta) = N(1) = 1$, e pela multiplicidade da norma, vem que $N(\alpha)N(\beta) = 1$. Portanto $|N_{\mathbb{L}|\mathbb{Q}}(\alpha) = 1|$. Reciprocamente, suponha que a norma de α seja um elemento invertível de $\mathbb{Z}$. Pelo item anterior, existe $\theta \in \mathbb{Z}$ tal que $\theta \cdot \alpha = N(\alpha)$, donde segue que $|\theta \cdot \alpha| = 1$, ou seja, $\alpha \in S^X$.
3) Com efeito, todo elemento primo em $\mathbb{Z}$ é irredutível. O resultado segue imediatamente de (b) e do fato da norma ser multiplicativa. **(c.q.d)**

O teorema acima, particularmente, nos mostra que, para decidir se um número algébrico é inteiro ou não, basta considerar seu polinômio minimal sobre $\mathbb{Q}$.

Exemplo 13. *Seja $\gamma = r \cdot \sqrt[q]{p}$, com $r \in \mathbb{Q} \setminus \{0\}$, e p,q números primos. Então $I(\gamma, \mathbb{Q}) = x^q - r^q \cdot p$. Portanto, γ será inteiro algébrico se, e somente se, $r \in \mathbb{Z}$. Certamente, γ não é invertível em $I_{\mathbb{Q}}(\gamma)$.*

Poderíamos ter escrito um teorema idêntico ao anterior para o caso mais geral em que R é um domínio integralmenete fechado, $\mathbb{L}$ é uma extensão do corpo de frações de R, e S é um subanel de $I_L(R)$ que contém R. A demonstração também seria análoga. Podemos, ainda, definir o discriminante de um polinômio, bem como o discriminante de uma upla de elementos pertencentes a um S-módulo finitamente gerado.

Definição 3.7. *Seja R um anel comutativo com unidade e $p = a_0 + a_1x + ... + x^n$ mônico. Sejam $\alpha_1, ..., \alpha_n$ as raízes de p. Definimos o discriminante de p como sendo o produto dos quadrados das diferenças entre raízes distintas de p,*

isto é, Disc(p) = $\displaystyle\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$.

Exemplo 14. *Seja $f = x^2 + bx + c \in \mathbb{C}[x]$ um polinômio de grau dois. Sejam $q, r \in \mathbb{C}$ suas raízes. Sem perda de generalidade, escreva $q = \dfrac{-b + \sqrt{b^2 - 4c}}{2}$ e $r = \dfrac{-b - \sqrt{b^2 - 4c}}{2}$. Temos $Disc(f) = (q - r)^2 = \left(\dfrac{-2\sqrt{b^2 - 4c}}{2}\right)^2 = b^2 - 4c$.*

Mais importante do que o discriminante de um polinômio é o conceito de discriminante $\text{Disc}(\alpha_1, ..., \alpha_n)$ de uma n-upla de elementos de uma extensão $\mathbb{K} \subseteq \mathbb{L}$, conforme:

Definição 3.8. *Seja $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n. Para quaisquer $\alpha_1, ..., \alpha_n \in \mathbb{L}$, definimos o discriminante da n-upla $(\alpha_1, ..., \alpha_n)$ como*

$$disc_{\mathbb{L}|\mathbb{K}}(\alpha_1, ..., \alpha_n) = \det(Tr_{\mathbb{L}|\mathbb{K}}(\alpha_i \cdot \alpha_j)) \in \mathbb{K},$$

com $1 \leq i, j \leq n$.

Podemos relacionar discriminantes de diferentes n-uplas. Mais especificamente, se os elementos dessa n-upla formam a base de uma extensão, então o discriminante é não nulo e, além disso, podemos relacionar os discriminantes de bases diferentes. É o que nos conta a:

Proposição 3.8. *Seja $\mathbb{Q} \subseteq \mathbb{K}$ extensão de corpos e sejam $W = \{w_1, \cdots, w_n\}$ e $U = \{u_1, \cdots, u_n\}$ bases dessa extensão. Se $C = (c_{ij})$ é a matriz de mudança da base W para base U, então $D(w_1, \cdots, x_n) = D(u_1, \cdots, u_n) \cdot (\det(C))^2$ e ambos os discriminantes são não nulos.*

Demonstração. Para a primeira afirmação, basta aplicar $Tr_{\mathbb{L}|\mathbb{K}}$ à igualdade $w_i w_j = \sum_{i,j=1}^{n} c_{ki} c_{mj} u_i u_j$ e considerar os determinantes das matrizes assim obtidas. Como C é invertível, temos $\det(C) \neq 0$. Finalmente, resta mostrar que os discriminantes são não nulos. Pela afirmação anterior, basta mostrarmos isto para uma base específica. Tome $\theta \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{Q}(\theta)$ (teorema do elemento primitivo). Então $\{1, \theta, \cdots, \theta^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{Q}$. Além disso, é fácil verificar que o discriminante dessa base é dado pelo determinante de Wandermonde

$$\begin{vmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \neq 0,$$

onde, para cada $i = 1, ..., n$, θ_i é um conjugado de θ, ou seja, θ_i é uma raiz do polinômio minimal de θ. Sendo os conjugados de θ dois a dois distintos (pois os polinômios minimais são separáveis), segue a afirmação.**(c.q.d)**

A proposição acima tem sua devida importância para demonstrar, que, dado um corpo $\mathbb{L}$ de números algébricos, o anel I_L é um $\mathbb{Z}$-módulo livre, ou seja, $\mathbb{L}$ possui base integral. Façamos isso a seguir.

3.4 I_L como Domínio de Dedekind

Nosso primeiro objetivo é demonstrar que o anel I_L admite uma base integral. Para tanto, demonstraremos a seguinte proposição, as vezes chamada de "Lema do Sanduíche", a qual fornece um "limitante"para os elementos de I_L.

Proposição 3.9. *Seja $\mathbb{L}$ corpo de números algébricos, com $[\mathbb{L} : \mathbb{Q}] = n$. Existe uma base $\{w_1, \cdots, w_n\}$ de $\mathbb{L}$ sobre $\mathbb{Q}$ e um inteiro $D \geq 0$ tal que*

$$\mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n \subseteq I_L \subseteq \mathbb{Z}\frac{w_1}{D} + \cdots + \mathbb{Z}\frac{w_n}{D}.$$

Demonstração. Seja $\{w_1, \cdots, w_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{Q}$. Evidentemente, cada w_i é número algébrico. A proposição (3.2) garante que podemos multiplicar tais elementos por um inteiro conveniente de modo a torná-los inteiros algébricos. Portanto, podemos considerar, sem perda de generalidade, que $w_i \in I_L$, para todo $i \in \{1, \cdots, n\}$. Sendo I_L um anel, tiramos a primeira inclusão.
Agora, para cada $a \in I_L$, escreva $a = b_1w_1 + \cdots + b_nw_n$, com $b_i \in \mathbb{Q}$. Multiplicando a equação anterior por w_j, para cada $j = 1, ..., n$, e tomando traços, obtemos

$$Tr_{\mathbb{L}|\mathbb{Q}}(aw_1) = b_1Tr_{\mathbb{L}|\mathbb{Q}}(w_1w_1) + \cdots + b_nTr_{\mathbb{L}|\mathbb{Q}}(w_1w_n)$$

$$\vdots$$

$$Tr_{\mathbb{L}|\mathbb{Q}}(aw_n) = b_1Tr_{\mathbb{L}|\mathbb{Q}}(w_1w_n) + \cdots + b_nTr_{\mathbb{L}|\mathbb{Q}}(w_nw_n).$$

Com efeito, o fato de aw_i e w_iw_j serem inteiros algébricos significa que os traços dados acima são inteiros. Portanto o discriminante $D(w_1, \cdots, w_n)$ pertence a $\mathbb{Z}$. Da proposição anterior, resulta que $D \neq 0$. A regra de Cramer nos dá que $b_i \in \dfrac{\mathbb{Z}}{D}$, donde segue a segunda continência. **(c.q.d)**

Com isso, podemos demonstrar o:

Teorema 3.5 (Base Integral)**.** *Se L é corpo de números algébricos e* $[L : \mathbb{Q}] = n$*, então existem* $u_1, \cdots, u_n \in I_L$ *tais que* $I_L = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n$*.*

Demonstração. Tome $w_1, \cdots, w_n \in I_L$ e D inteiro positivo tais que

$$\mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n \subseteq I_L \subseteq \mathbb{Z}\frac{w_1}{D} + \cdots + \mathbb{Z}\frac{w_n}{D}.$$

Para cada $i = 1, ..., n$, defina

$$N_i = \left\{ a_i\frac{w_i}{D} + \cdots + a_n\frac{w_n}{D} \in I_L : a_i, \cdots, a_n \in \mathbb{Z} \right\}.$$

Escolha $u_i \in N_i$ tal que o coeficiente $a_i > 0$ de $\dfrac{w_i}{D}$ seja mínimo. Se $\beta \in I_L$, então existem $b_1, \cdots, b_n \in \mathbb{Z}$ para os quais $\beta = b_1\dfrac{w_i}{D} + \cdots + b_n\dfrac{w_n}{D}$. Tome $q_1, r_1 \in \mathbb{Z}$ tais que $b_1 = a_1q_1 + r_1$, com $0 \leq r_1 < a_1$. Sendo I_L anel, temos $\beta - q_1u_1 \in I_L$. Sendo r_1 o coeficiente deste elemento, então, pela minimalidade de a_1, temos $r_1 = 0$. Portanto, $\beta - q_1a_1 \in N_2$. Prosseguindo assim, obtemos $q_2, \cdots, q_n \in \mathbb{Z}$ tais que $\beta - q_1u_1 - \cdots - q_nu_n = 0$, donde segue que β é combinação linear dos u_i. Daí, segue a igualdade. Agora, todo elemento de L é o quociente de um elemento de I_L e um inteiro, donde segue que os u_i geram L sobre $\mathbb{Q}$, ou ainda, $\{u_1, \cdots, u_n\}$ é base de L sobre $\mathbb{Q}$. **(c.q.d)**

Nosso próximo objetivo é mostrar que, de fato, o anel I_L é um anel noetheriano.

Definição 3.9. *Um anel comutativo R chama-se noetheriano se satisfaz qualquer uma das seguintes propriedades equivalentes:*
1) Todo ideal I de R é finitamente gerado.
2) Para toda cadeia $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$*, existe* $j \in \mathbb{N}$ *tal que* $I_n = I_j$*, sempre que* $n \geq j$*.*
3) Todo conjunto não vazio de ideais possui elemento maximal por inclusão.

Provemos as equivalências, bastante simples, da definição anterior:
(1)⇒(2) Considere o ideal $J = \bigcup_{i\geq 0} I_i$ de R. Dados $x_1, \cdots, x_n$ geradores de J, existe $j \in \mathbb{N}$ suficientemente grande tal que $x_1, \cdots, x_n \in I_j$, donde segue que $J = I_j$, isto é, $I_n = I_{n+1}$, para todo $n \geq j$.
(2)⇒(1) Seja I um ideal de R. Tome $x_1 \in I$. Se $(x_1) \neq I$, então tome $x_2 \in I \backslash (x_1)$. Se $\langle x_1, x_2\rangle \neq$, tome $x_3 \in I \backslash \langle x_1, x_2\rangle$, de modo que esse processo se repita indutivamente. Como a cadeia $(x_1) \subseteq \langle x_1, x_2\rangle \subseteq \langle x_1, x_2, x_3\rangle \subseteq \cdots$ se estabiliza, segue que existe $n \in \mathbb{N}$ tal que $I = \langle x_1, \cdots, x_n\rangle$.
(2)⇒(3) Seja K um conjunto de ideais de R. Suponha que K não possui elemento maximal. Tome $I_1 \in K$. Deve existir $I_2 \in K$ tal que $I_1 \subsetneq I_2$. Continuando esse processo indutivamente, teremos uma cadeia de ideiais $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ que não se estabiliza. Absurdo.
(3)⇒(2) Dada qualquer cadeia ascendente de ideais, podemos tomar, por hipótese, um elemento maximal. Todos os ideais que contém tal elemento devem ser iguais. Daí, segue o resultado. **(c.q.d)**

Já provamos que, para toda extensão finita $\mathbb{Q} \subseteq L$, existe uma base integral $\{w_1, \cdots, w_n\}$para I_L. Dado um ideal não nulo J e um elemento $a \in J$, temos $\mathbb{Z}aw_1 \subseteq \cdots \subseteq \mathbb{Z}aw_n \subseteq J \subseteq \mathbb{Z}w_1 \subseteq \cdots \subseteq \mathbb{Z}w_n$. Assim, podemos demonstrar, de um modo parecido ao que foi feito no teorema (3.5), que existe uma base integral para J. Portanto, todo ideal de I_L é finitamente gerado, ou seja, I_L é noetheriano.

O teorema a seguir finaliza esta seção, dando-nos 3 características importantes para o anel I_L:

Teorema 3.6. *Seja L um corpo de números algébricos. Então:*
1) I_L é integralmente fechado.
2) I_L é noetheriano
3) Todo ideal primo não nulo de I_L é maximal.

Demonstração. Os itens (1) e (2) já foram demonstrados anteriormente. Vamos demonstrar (3). Tome um ideal primo não nulo P. Como P é finitamente gerado, segue que $\frac{I_L}{P}$ é domínio finito, ou seja, $\frac{I_L}{P}$ é um corpo, ou ainda, P é ideal maximal. **(c.q.d)**

Definição 3.10. *Um domínio que satisfaz as três condições do teorema anterior é dito ser um domínio de Dedekind.*

Em qualquer domínio de Dedekind, prova-se que qualquer ideal pode ser escrito, de maneira única, como um produto de ideiais primos. Em particular, essa fatoração vale para qualquer anel I_L, pelo terorema acima.

4 Corpos Quadráticos

4.1 O anel $\mathbb{Z}[\sqrt{d}]$

Dedicamos esta curta seção ao estudo dos inteiros algébricos em corpos quadráticos, os quais exercem eficiente desempenho para resolver as chamadas Equações de Pell.

Definição 4.1. *Um corpo $\mathbb{L} \subseteq \mathbb{C}$ chama-se quadrático se, e somente se, $\mathbb{L}$ é extensão de $\mathbb{Q}$ tal que $[\mathbb{L} : \mathbb{Q}] = 2$.*

Observe que qualquer elemento $\alpha \in \mathbb{L}\backslash\mathbb{Q}$ é primitivo sobre a extensão $\mathbb{Q} \subseteq \mathbb{L}$, isto é, $\mathbb{L} = \mathbb{Q}(\alpha)$. Com efeito, temos $1 < [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2$, donde segue que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Logo, $\{1, \alpha\}$ é uma base dessa extensão, e o polinômio $I(\alpha, \mathbb{Q})$ é irredutível, mônico, e de grau 2. Denotaremos por $\mathbb{D}$ o conjunto dos números $d \in \mathbb{Z} \setminus \{0, 1\}$ que não são divisíveis por nenhum quadrado $c^2 \neq 1$, com $c \in \mathbb{Z}$. Com isso, vamos mostrar o seguinte:

Proposição 4.1. *A aplicação $d \mapsto \mathbb{Q}(\sqrt{d})$ é uma bijeção de $\mathbb{D}$ sobre o conjunto de todos os corpos quadráticos.*

Demonstração. Dado $d \in \mathbb{D}$, temos $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] \leq 2$, uma vez que $I(\sqrt{d}, \mathbb{Q})$ divide $x^2 - d \in \mathbb{Z}$. Se fosse $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 1$, então teríamos $\sqrt{d} \in \mathbb{Q}$ e $\sqrt{d}$ inteiro algébrico, donde viria que $\sqrt{d} \in \mathbb{Z}$. Logo $d = (\sqrt{d})^2 \notin \mathbb{D}$, o que é absurdo. Suponha que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$, para certos $d, d' \in \mathbb{D}$. Então, existem $r, s \in \mathbb{Q}$ tais que $\sqrt{d} = s\sqrt{d'} + r$, ou seja, $d = s^2 d' + r^2 + 2sr\sqrt{d'}$, ou ainda, $rs = 0$. Daí, concluímos que $r = 0$ ou $s = 0$. Se tivéssemos $s = 0$, então teríamos $\sqrt{d} = r \in I_L \cap \mathbb{Q} = \mathbb{Z}$, o que nos dá $d \in \mathbb{D}$. Absurdo. Portanto $r = 0$, e então $d = s^2 d'$. Como $d \in \mathbb{D}$, temos $s = 1$, isto é, $d = d'$. Daí, resulta que a aplicação é injetora. Agora, seja $\mathbb{L} = \mathbb{Q}(\alpha)$ corpo quadrático e $I(\alpha, \mathbb{Q}) = x^2 + ax + b$ polinômio minimal de α em $\mathbb{Q}$. Faça $\beta = \alpha + \dfrac{a}{2}$. Com efeito, $\mathbb{L} = \mathbb{Q}(\beta)$ e $I(\beta, \mathbb{Q}) = x^2 - \left(\dfrac{a^2}{4} - b\right)$. Finalmente, basta tomar $r \in \mathbb{Q} \setminus \{0\}$ e $d \in \mathbb{D}$ tais que $\dfrac{a^2}{4} - b = r^2 \cdot d$, o que nos dá $\mathbb{L} = \mathbb{Q}(\sqrt{d})$.

(c.q.d)

Tomando $1, \sqrt{d}$ como base de $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, o polinômio característico de qualquer elemento $\alpha = r + s \cdot \sqrt{d} \in \mathbb{L}$ é dado por $\det \begin{pmatrix} x - r & -s \\ -s \cdot d & x - r \end{pmatrix} = x^2 - 2rx + r^2 - s^2 d$.

De forma análoga ao que se faz em $\mathbb{Z}$, podemos definir uma relação de divisibilidade em corpos quadráticos, bem como a relação de congruência $\alpha \equiv \beta (mod \gamma) \Leftrightarrow \gamma \mid (\alpha - \beta)$. Podemos, com isso, obter a seguinte generalização do pequeno Teorema de Fermat:

Teorema 4.1. *Seja $p \in \mathbb{Z}$ um primo tal que $p \neq 2$ e $p \nmid d$. Para todo $\alpha \in \mathbb{Z}(\sqrt{d})$, vale que $\alpha^{p^2} \equiv \alpha (mod\ p)$.*

Demonstração. Escreva $\alpha = a + b\sqrt{d}$, para certos $a, b \in \mathbb{Z}$. Note que $\alpha^p = (a + b\sqrt{d})^p = \sum_{i=0}^{n} \binom{p}{i} a^i (b\sqrt{d})^{p-i} \equiv a^p + b^p (\sqrt{d})^p (\text{mod p})$, uma vez que $p \mid \binom{p}{i}$, para $1 \leq i \leq p - 1$. Pelo pequeno teorema de Fermat, temos que $a^p \equiv a (\text{mod p})$ e $b \equiv b^p (\text{mod p})$, donde segue que $\alpha^p \equiv a + b(\sqrt{d})^p (\text{mod p})$. Se elevarmos toda a equação a p, obteremos que $\alpha^{p^2} \equiv a + b(d^{p-1})^{(p+1)/2}\sqrt{d}$ (mod p). Como p é um primo que não divide 2,temos que p é ímpar, donde tiramos que $\dfrac{p+1}{2}$ é inteiro. O pequeno teorema de Fermat nos dá, novamente, que $(d^{p-1})^{(p+1)/2}\sqrt{d} \equiv \sqrt{d} (\text{mod p})$, o que resulta em $\alpha^{p^2} \equiv \alpha (\text{mod p})$. **(c.q.d)**

Demonstra-se o seguinte fato interessante sobre inteiros algébricos:

Proposição 4.2. *Seja $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{D}$, e seja $\gamma = \sqrt{d}$ (respectivamente $\dfrac{1 + \sqrt{d}}{2}$), no caso em que $d \equiv 2 (mod\ 4)$ ou $d \equiv 3 (mod\ 4)$ (respectivamente, $d \equiv 1 (mod\ 4)$). Então $\{1, \sqrt{d}\}$ formam uma base do $\mathbb{Z}$-módulo I_L.*

Para demonstração, veja [1]. Lembremos que todo domínio de fatoração única é integralmente fechado, pelo teorema (3.2). Podemos nos perguntar se vale a volta do teorema, ou seja, se todo domínio integralmente fechado é de fatoração única. A resposta para isto é negativa. Veja o contra-exemplo mais conhecido:

Exemplo 15. *Seja* $\mathbb{L} = \mathbb{Q}(\sqrt{-5})$. *Note que* $I_{\mathbb{L}} = \mathbb{Z}(\sqrt{-5})$, *o qual é, obviamente, integralemente fechado (por definição). Mostremos que* I_L *não é de fatoração única. Considere a norma* $N : \mathbb{Z}(\sqrt{-5}) \to \mathbb{Z}(\sqrt{-5})$, *dada por* $N(a + b\sqrt{-5}) = a^2 + 5b^2$. *Com efeito, note que* $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. *Basta mostrarmos que* $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ *são irredutíveis em* $\mathbb{Z}(\sqrt{-5})$. *Note que as normas desses elementos são, respectivamente,* $4, 9, 6$ *e* 6. *Pelo teorema* (3.4), *segue que esses elementos não são invertíveis. Se, por exemplo,* $1 - \sqrt{-5}$ *fosse redutível, então existiriam* $\alpha, \beta \in \mathbb{Z}(\sqrt{-5})$ *tais que* $1 - \sqrt{-5} = \alpha\beta$. *Logo* $6 = N(1 - \sqrt{-5}) = N(\alpha)N(\beta)$, *donde tiramos que* $N(\alpha) \in \{-2, 2, -3, 3\}$. *Isto é impossível, pois, para todo* $m, n \in \mathbb{Z}$, *temos* $m^2 + 5n^2 \notin \{-2, 2, 3, -3\}$. *Portanto* $1 - \sqrt{-5}$ *é irredutível. A irredutibilidade de* $2, 3$ *e* $1 + \sqrt{-5}$ *é provada de forma análoga.*

4.2 Os inteiros Gaussianos

Enquanto o matemático alemão Carl Friedrich Gauss tentava demonstrar a lei da reciprocidade quadrática (para enunciado, veja [1]) para graus maioes do que o quadrado, ele percebeu que as contas se tornavam mais fáceis se considerasse números imaginários juntos aos inteiros. Nasce, dessa idéia, o importante estudo do anel $\mathbb{Z}(i)$, conhecido como o anel dos Inteiros Gaussianos (ou inteiros de Gauss), onde $i = \sqrt{-1}$ denota a unidade imaginária. Estudaremos, para encerrar esta seção, as propriedades mais interessantes desse anel.

De fato, qualquer criança (que já fez um curso de álgebra na infância) sabe que este anel é euclidiano e, portanto, é principal e, consequentemente, de fatoração única. A função grau que o torna euclidiano concide com sua norma. Com base nos estudos gerais de normas feitos na seção anterior, podemos determinar a norma de um elemento genérico em $\mathbb{Z}(i)$. Para isso, considere a base $\{1, i\}$ de $\mathbb{Z}(i)$. Dado qualquer $\alpha \in \mathbb{Z}(i)$, escrevemos $\alpha = a+bi$, com $a, b \in \mathbb{Z}$. Então $\alpha = a+bi = a\cdot 1+b\cdot i$. Também, temos $\alpha \cdot i = -b + ai$. Portanto, temos

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha \cdot i \end{pmatrix},$$

donde segue que a norma de α, em relação a esta base, é dada por $N(\alpha) = a^2 + b^2$. Em relação às propriedades desta norma, podemos enunciar a:

Proposição 4.3. *1)* $\mathbb{Z}(i)^X = \{\pm 1, \pm i\}$.
2) Se $p \in \mathbb{Z}$ *é um primo congruente a* 3 *módulo* 4, *então* p *é irredutível em* $\mathbb{Z}(i)$.

Demonstração. 1) Pelo teorema (3.4), basta mostrar que estes são os únicos inteiros gaussianos cuja norma é igual a 1. De fato, seja $a+bi \in \mathbb{Z}(i)$ com $a^2+b^2 = 1$. Suponha, por absurdo, a e b inteiros não nulos. Então, temos que $a^2 = 1 - b^2 = (1 - b)(1 + b)$. Como $a^2 > 0$, então $(1 - b)(1 + b) > 0$, ou seja, $-1 < b < 1$, donde vem que $b = 0$. Absurdo, por hipótese. Logo, necessariamente teremos $a = 0$ ou $b = 0$, o que verifica o item 1.
2) Se p admitir fatoração não trivial, então existem $\alpha, \beta \in \mathbb{Z}(i)$ não invertíveis tais que $p = \alpha\beta$. Daí, vem que $p^2 = N(p) = N(\alpha)N(\beta)$. Como $N(\alpha) \neq 1$ e $N(\beta) \neq 1$, segue que $N(\alpha) = p = n(\beta)$. Escrevendo $\alpha = m + ni$, obtemos

$m^2 + n^2 = p \equiv 3(\text{mod } 4)$, o que é impossível, uma vez que um quadrado perfeito só é congruente a 0 ou a 1 módulo 4. Segue que p é irredutível em $\mathbb{Z}(i)$. **(c.q.d)**

Evidentemente, é possível definir uma relação de divisibilidade em $\mathbb{Z}(i)$, bem como a estabelecer a congruência $\alpha \equiv \beta(\text{mod } \gamma) \Leftrightarrow \gamma \mid (\alpha - \beta)$, a qual determina uma relação de equivalência no anel dos inteiros Gaussinaos.

Exemplo 16. *Vamos mostrar que* $(1+i)^{2009}+1$ *é divisível por* $2+i$ *em* $\mathbb{Z}(i)$*. Com efeito, temos* $i \equiv -2(mod\ 2+i) \Leftrightarrow 1+i \equiv -1(\ mod\ 2+i)$*. Daí,* $(1+i)^{2009} \equiv (-1)^{2009}(mod\ 2+i) \Leftrightarrow (1+i)^{2009}+1 \equiv 0(mod\ 2+i)$*.*

De modo análogo ao que se faz em $\mathbb{Z}$, demonstra-se o Teorema de Bézout para os inteiros Gaussianos. Prova-se que todo primo da forma $4k+1$ é redutível em $\mathbb{Z}(i)$. Podemos mostrar, com isso, que todo número primo da forma $4k+1$ é a soma de dois quadrados. Antes de mais nada, provemos a:

Proposição 4.4. *Seja p um número primo e sejam* $m, n \in \mathbb{Z}$*. As seguintes condições são equivalentes:*
(1) $p^2 = m^2 + n^2$
(2) $m + ni$ *é um divisor próprio de p, não invertível em* $\mathbb{Z}(i)$*.*

Demonstração. (1)⇒(2): Note que $m \neq 0 \neq n$, pois, caso contrário, p seria igual ao quadrado de um número interiro ($p = m^2$ ou $p = n^2$), isto é, p não seria primo. Além disso, como $p \neq 1$, temos $m^2 + n^2 \neq 1$, donde segue que $m + ni, m - ni \in \mathbb{Z}(i)$ não são invertíveis, e portanto são divisores próprios de p. Além disso, ambos são irredutíveis em $\mathbb{Z}(i)$, pelo teorema (3.4). Isso significa que ambos são elementos primos em $\mathbb{Z}(i)$.
(2)⇒(1): Tome $\alpha \in \mathbb{Z}(i)$ não invertível, tal que $p = (m + ni)\alpha$. Tomando normas, ficamos com $p^2 = (m^2 + n^2)N(\alpha)$, donde segue que $p = m^2 + n^2$. **(c.q.d)**

Passamos agora ao teroema, enunciado anteriormente:

Teorema 4.2. *Qualquer primo p que é congruente a* 1 *módulo* 4 *fatora-se como* $p = (a + bi)(a - bi)$*.*

Demonstração. Primeiro, vamos mostrar que p é redutível em $\mathbb{Z}(i)$. Lembre que o grupo multiplicativo $\mathbb{F}_p^*$ é cíclico de ordem $p-1$ (teorema do elemento primitivo para grupos). Seja a um gerador deste grupo. Seu único subgrupo de ordem 2 é gerado pelo elemento $-1 = a^{\frac{p-1}{2}}$, o qual é um quadrado em $\mathbb{F}_p^*$. Seja $h \in \mathbb{F}_p^*$ representante de $a^{\frac{p-1}{4}}$. Então $h^2 \equiv -1(\text{mod p})$, isto é, p divide $h^2 + 1 = (h + i)(h - i)$. Se p fosse irredutível em $\mathbb{Z}(i)$, então p seria primo, e portanto $p \mid (h + i)$ ou $p \mid (h - i)$. Isso é um absurdo, pois os múltiplos de p em $\mathbb{Z}(i)$ são da forma $px+pyi$, ou seja, com parte real e imaginária múltiplas de p, o que não é o caso de $h \pm i$. Portanto, p é redutível em $\mathbb{Z}(i)$. Tome $\alpha, \beta \in \mathbb{Z}(i)$ tais que $p = \alpha\beta$. Temos $p^2 = N(p) = N(\alpha)N(\beta)$, donde segue que $N(\alpha) = p = N(\beta)$. Escrevendo $\alpha = a + bi$, tiramos que $a^2 + b^2 = p$, ou seja, $p = (a + bi)(a - bi)$. Além disso, $a \pm bi$ são ambos irredutíveis, pois sua norma é um número primo, e portanto, irredutível. **(c.q.d)**

Corolário 4.1. *Todo número primo da forma* $4k + 1$*,* $k \in \mathbb{Z}$*, é a soma de dois quadrados.*

Demonstração. Seja p um primo dessa forma. Então $p \equiv 1(\text{mod } 4)$. Pelo teorema, existem $m, n \in \mathbb{Z}$ tais que $p = (m - ni)(m + ni) = m^2 + n^2$. **(c.q.d)**

5 Um exemplo de número transcedental

Fazendo uso de alguns critérios de irredutibilidade de polinômios, podemos determinar o grau de vários números algébricos, isto é: Dado um corpo $\mathbb{F}$ e um número α algébrico sobre $\mathbb{F}$, podemos determinar o grau da extensão $\mathbb{F} \subseteq \mathbb{F}(\alpha)$. Como um exemplo disso, provemos o teorema que se segue.

Teorema 5.1. *Se N é um número natural e $m > 1$ é um natural tal que não existe $k \in \mathbb{N}$ tal que $m = k^d$, para todo $d \neq 1$ divisor de N, então o número $m^{1/N}$ é um número algébrico de grau N.*

Demonstração. Seja $t = m^{1/N}$. Então t é raiz do polinômio $f = x^N - m$. O lema de Gauss garante que se este polinômio é irredutível em $\mathbb{Z}[x]$, também o será em $\mathbb{Q}[x]$. Suponha, por absurdo, que f é redutível em $\mathbb{Z}[x]$. Nesse caso, existem $p, q \in \mathbb{Z}[x]$, não constantes, tais que $x^n - m = pq$. Denotemos por z_N a raiz N-ésima da unidade igual a $e^{2\pi i/N}$. Temos $x^N - m = \prod_{j=0}^{N-1}(x - (z_N)^j t)$. Como p, q são não constantes, podemos tomar dois conjuntos A e B disjuntos tais que $A \cup B = \{0, 1, \cdots, N-1\}$. Além disso, podemos escrever

$$p = \prod_{j \in A}(x - (z_N)^j t), \quad q = \prod_{j \in B}(x - (z_N)^j t).$$

Sejam r o número de elementos de A e s número de elementos de B. Existem inteiros R, S para os quais

$$p(0) = (-1)^r t^r (z_N)^R, \quad q(0) = (-1)^s t^s (z_N)^S,$$

sendo t^r e r^s números naturais, pois tanto p(0) quanto q(0) são naturais, em virtude de que p e q são polinômios com coeficientes inteiros. Seja l o menor natural para o qual t^l é racional. É fácil ver que se j é um natural tal que t^j é racional, então $l|j$ (de fato, basta aplicar a divisão euclidiana de j por l e verificar que o resto r da divisão deve ser, obrigatoriamente, nulo). Daí, segue que l é um divisor de r, s e N. Como $(t^l)^{N/l} = m$ e $t^l = \dfrac{c}{d}$, com mdc$(c, d) = 1$, obtemos que $md^{N/l} = c^{N/l}$, ou seja, todo fator primo de d deve divir c. Mas c e d são coprimos. Logo d = 1. Assim, $m = (t^l)^{N/l}$, $t^l \in \mathbb{N}$ e $\dfrac{N}{l} \neq 1$. Em outras palavras, m é uma $\dfrac{N}{l}$-potência de $t^l \in \mathbb{N}$ e $\dfrac{N}{l} \neq 1$ é um divisor de N diferente de 1. Isto é um absurdo, pois contradiz a hipótese do teorema. Segue que f não possui fatoração não trivial, ou seja, f é irredutível. Portanto, a extensão $\mathbb{Q} \subseteq \mathbb{Q}(m^{1/N})$ possui grau N, donde conclui-se que N é o grau do número algébrico $m^{1/N}$. **(c.q.d)**

O objetivo deste capítulo é apresentar um exemplo de número transcedental, e demonstrar a transcedentalidade do mesmo utilizando apenas propriedades de números algébricos. Ora, é claro que se um certo número não possui uma propriedade que todos os números algébricos devem possuir, então este é transcendente. Isso mostra que o estudo de números algébricos permite também encontrarmos condições para que que um número não seja algébrico. Uma importante propriedade de números algébricos é, então, descrita pelo teorema abaixo, o qual é mérito do matemático francês Joseph Liouville.

Teorema 5.2. *Se $a \in \mathbb{R}$ é um número algébrico de grau $N \neq 1$, então existe uma constante $C = C(a)$ tal que para todos os inteiros A e B, com $B > 0$, vale que*

$$\left| a - \frac{A}{B} \right| \geq \frac{C}{B^N}$$

Demonstração. Seja $I(a, \mathbb{Q})(x) = x^N + ... + b_1 x + b_0 \in \mathbb{Q}[x]$ o polinômio minimal de a em $\mathbb{Q}$. Se multiplicarmos tal polinômio pelo valor do mínimo múltiplo comum entre os denominadores dos coeficientes de $I(a, \mathbb{Q})$, obteremos um polinômio irredutível $f(x) = a_N x^N + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ com as mesmas raízes de $I(a, \mathbb{Q})$. Em $\mathbb{R}[x]$, podemos tomar um polinômio g tal que $f(x) = (x - a)g(x)$. É claro que $g(a) \neq 0$, pois, caso contrário, a seria raiz dupla de f, que é irredutível em $\mathbb{Q}$, cuja característica é zero. Isso contradiria a proposição (2.7). Portanto, existem $\epsilon, \delta > 0$ tais que, para todo $x \in (a - \epsilon, a + \epsilon)$, tenhamos $0 < |g(x)| \leq \delta$ (De fato, o polinômio g define uma função contínua em $\mathbb{R}$, logo a imagem de qualquer intervalo é limitada. Em particular, podemos escolher um intervalo centrado em a que não contenha nenhuma outra raiz de g). Tome um número racional nesse intervalo. Tal número é da forma $\frac{A}{B}$, com $A, B \in \mathbb{Z}$ coprimos. Como $g\left(\frac{A}{B}\right) \neq 0$, então $f\left(\frac{A}{B}\right) \neq 0$, donde obtemos que

$$\left| a - \frac{A}{B} \right| = \left| \frac{f\left(\frac{A}{B}\right)}{g\left(\frac{A}{B}\right)} \right| = \left| \sum_{k=0}^{N} a_k A^k B^{N-k} \right| B^{-N} \left| g\left(\frac{A}{B}\right) \right|^{-1} \geq \frac{1}{\delta B^N},$$

uma vez que $\sum_{k=0}^{N} a_k A^k B^{N-k}$ é um inteiro não nulo. Por outro lado, se $\frac{A}{B} \notin (a - \epsilon, a + \epsilon)$, com A e B inteiros primos entre si, então claro que

$$\left| a - \frac{A}{B} \right| \geq \epsilon \geq \frac{\epsilon}{B^N}.$$

Portanto, basta tomarmos C = $\min\{\epsilon, \delta^{-1}\}$ para obter o resultado, **(c.q.d)**

Prontamente, qualquer número que não satisfaça o teorema acima não pode ser algébrico, e portanto será transcendental. O corolário abaixo nos dá o tão esperado exemplo de número transcendente, o que finaliza também este curtíssimo capítulo.

Corolário 5.1. *O número irracional $\sum_{n=1}^{\infty} 2^{-n!}$ é transcendente.*

Demosntração. É claro que a série $\sum_{n=1}^{\infty} 2^{-n!}$ converge, pois $2^{-n!} \leq 2^{-n}$, para todo $n \in \mathbb{N}$, e a série geométrica $\sum_{n=1}^{\infty} 2^{-n}$ converge. Se o número $a = \sum_{n=1}^{\infty} 2^{-n!}$ fosse algébrico de grau $N \in \mathbb{N}$, então, pelo teorema anterior, existiria uma constante C tal que, para todo $k \in \mathbb{N}$, teríamos

$$\sum_{n=n+1}^{\infty} 2^{-n!} = \left| a - \sum_{n=1}^{k} 2^{-n!} \right| \geq \frac{C}{2^{Nk!}},$$

pois o número racional $\sum_{n=1}^{k} 2^{-n!}$ possui denominador igual a $2^{k!}$. Por outro lado, note que

$$\sum_{n=k+1}^{\infty} 2^{-n!} \leq \sum_{m=0}^{\infty} 2^{-(k+1)!-m} = \frac{\frac{1}{2^{(1+k)!}}}{1-\frac{1}{2}} = \frac{\frac{1}{2^{(1+k)!}}}{\frac{1}{2}} = \frac{2}{2^{(1+k)!}},$$

ou seja, $\frac{C}{2^{Nk!}} \leq \frac{2}{2^{(1+k!)}}$, isto é, $2^{k!(1+k-N)} \leq \frac{2}{C}$, para todo $k \in \mathbb{N}$. Absurdo, pois $2^{k!(1+k-N)} \to +\infty$. Daí, segue o resultado. **(c.q.d)**

Finalmente, o teorema de Liouville nos mostra que os números algébricos não podem ser bem aproximados por números racionais. Embora os números transcendentes constituírem um conjunto muito "maior"do que o conjunto dos números algébricos, conforme visto no teorema de Cantor, é notória a dificuldade de se achar exemplos desses números. Claro que com a evolução da teoria dos números, a quantidade de exemplos existentes dessa espécie de números aumentou consideravelmente. Existem vários teoremas importantes (como o teorema acima) que nos dão condições suficientes para que um número seja transcendente. Como as propriedades entre números algébricos e transcendentes são complementares, concluímos, com entusiasmo, que o estudo de números algébricos permite aumentar, ainda mais, nosso conhecimento dos números reais, o qual ainda é "infinitamente pequeno"se comparado com nossa ignorância a respeito desses.

Referências

[1] Otto Endler. *Teoria dos Números Algébricos*. Imos Gráfica e Editora.

[2] W.H Greub. *Linear Algebra*. Springer Verlag.

[3] Israel Nathan Herstein. *Topics In Algebra*. Chapman and Hall.

[4] Paulo A. Martin. *Grupos, Corpos e Teoria de Galois*. Editora Livraria da Física.

[5] Luiz Henrique Jacy Monteiro. *Elementos de Álgebra*. Editora da Universidade de São Paulo.

[6] Luiz Henrique Jacy Monteiro. *Teoria de Galois*. Impa.

[7] Ian Stewart. *Galois Theory*. Chapman and Hall.