Anéis de Polinômios a Valores Inteiros

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pela Sra. *Ana Claudia Locateli Peruzzi* e aprovada pela Comissão Julgadora.

Campinas, 30 de setembro de 1993.

Prof. Dr. Paulo Roberto Brumatti

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

Universidade Estadual de Campinas
IMECC

Dissertação de Mestrado

Anéis de Polinômios a Valores Inteiros

Aluna: Ana Claudia Locateli Peruzzi
Orientador: Prof. Dr. Paulo Roberto Brumatti

Setembro de 1993

A meus pais, Domingos
e Sonia, e meus irmãos, Ana
Flavia e André.

Agradecimentos

- Ao professor Paulo R. Brumatti, pela orientação, atenção e amizade.
- Ao CNPq pelo auxílio financeiro.
- A meus pais, Domingos e Sonia, e a meus irmãos, Ana Flavia e André, pela compreensão, apoio e carinho.
- Ao professor Irineu Bicudo, que me apresentou à Álgebra, pelo incentivo e confiança.
- Aos meus professores de Rio Claro, especialmente à Solange, Nativi e João Ivo, pela força.
- A Túlio e Ana Márcia, pelo trabalho em latex.
- Aos meus amigos de graduação, em especial à Ana Paula, Flávia, Marcelo e Nelson.
- Aos amigos do "predinho", pelos bons momentos.
- Aos *irmãos* Ademir, Angela, Pedro e Jefferson, pela amizade, força, carinho e tudo que vivemos juntos.
- A Alancardek, que não é o Espírito de Luz, mas que me deu o apoio, o incentivo e principalmente muito carinho para que tudo desse certo.

Valeu!

Ana Claudia

Conteúdo

Introdução

Consideremos K um corpo numérico e A o anel de inteiros de K. Seja

$$Int(A) = \{f(\mathsf{x}) \in K[\mathsf{x}]; f(A) \subset A\}$$

o subconjunto de $K[\mathsf{x}]$ dos polinômios a valores inteiros sobre K. Surgem então algumas perguntas naturais: "Qual a estrutura algébrica do conjunto $Int(A)$?" ou "Como determinar os elementos de $Int(A)$?".

Buscando respostas a essas perguntas, vemos que claramente $Int(A)$ é um anel e logo um A-módulo. Vamos mostrar nesse trabalho que $Int(A)$, visto como um anel, possui características especiais; mostramos, por exemplo, que $Int(A)$ é um domínio de Prüfer. Agora, vendo $Int(A)$ como um A-módulo, vamos mostrar que impondo algumas condições sobre A e K, o A-módulo $Int(A)$ é livre. Sob esse último ponto de vista buscamos ainda determinar uma A-base livre de $Int(A)$. No caso particular em que K é o corpo dos números racionais $\mathbf{Q}$ e A é o anel dos números inteiros $\mathbf{Z}$, é possível obter-se explicitamente uma $\mathbf{Z}$-base livre para $Int(\mathbf{Z})$, porém no caso geral verificamos que nem sempre isso é possível. Trabalharemos então no sentido de determinar sob quais condições $Int(A)$ é um A-módulo livre, e nesse caso mostrar uma A-base livre, e estudar suas características como anel.

Apresentamos em apêndice a notação que é utilizada e recordamos alguns resultados gerais que são necessários no decorrer do trabalho. Achamos por

bem colocar esses resultados no trabalho destacadamente para que por um lado este seja auto-contido e por outro lado não se perca a unidade dos capítulos.

O estudo sobre o anel $Int(A)$ teve início em artigos de G. Polya[14] e A. Ostrowski[13], no começo deste século, mais especificamente em 1919. No capítulo 1, baseado no artigo de G. Polya, determinamos condições para que $Int(A)$ seja um A-módulo livre e, no caso em que essas condições são satisfeitas, determinamos ainda características que devem possuir os polinômios de uma A-base livre de $Int(A)$. As respostas mais objetivas nesse sentido são dadas no caso em que K é um corpo quadrático.

No capítulo 2 consideramos A um domínio de Dedekind e K o corpo de frações de A e definimos o anel

$$\mathcal{I}(A) = \{f(\mathsf{x}) \in K[\mathsf{x}]; f(A) \subset A\} .$$

Temos então que $\mathcal{I}(A)$ é uma generalização do anel $Int(A)$ que foi estudado no capítulo 1. A partir daí estudamos as características de $\mathcal{I}(A)$ como anel. Mostramos que se A satisfaz determinadas condições, $\mathcal{I}(A)$ é um domínio de Prüfer. Além disso, motivados por um resultado de T. Skolem[16], mostramos ainda que sob essas mesmas condições o anel $\mathcal{I}(A)$ possui uma propriedade muito interessante, chamada propriedade forte de Skolem, que afirma que se I e J são ideais finitamente gerados de $\mathcal{I}(A)$ tais que

$$I(a) = \{f(a); f(\mathsf{x}) \in I\} = J(a) = \{g(a); g(\mathsf{x}) \in J\}$$

para todo $a \in A$, então $I = J$. Em particular, se A é o anel de inteiros de um corpo numérico então A satisfaz as condições exigidas e portanto podemos concluir que $Int(A)$ é um domínio de Prüfer e possui a propriedade forte de Skolem. Os resultados apresentados nesse capítulo são devidos a D. Brizolis[2,3,4].

O terceiro e último capítulo é dedicado à exibição de exemplos e contra-exemplos sobre o que foi apresentado nos capítulos precedentes. O objetivo é ilustrar teoremas e mostrar a importância de hipóteses exigidas dando exemplos onde os resultados obtidos falham na ausência destas.

Chamamos a atenção para o fato de que existem outras linhas de estudo sobre os polinômios a valores inteiros. Por exemplo, D. Brizolis em [3,4] trabalha com polinômios a valores inteiros a várias variáveis, ou seja, com o anel

$$Int(A,n) = \{f(\mathrm{x}_1,\cdots,\mathrm{x}_n) \in K[\mathrm{x}_1,\cdots,\mathrm{x}_n]; f(A^n) \subset A\}$$

onde $n \in \mathbf{Z}$, A é um domínio e K é o corpo de frações de A. Outra abordagem interessante é a realizada por R. Gilmer[8], que busca subconjuntos S de $\mathbf{Z}$ que determinam $Int(\mathbf{Z})$, isto é, subconjuntos minimais $S \subset \mathbf{Z}$ tais que

$$Int(\mathbf{Z}) = \{f(\mathrm{x}) \in K[\mathrm{x}]; f(S) \subset \mathbf{Z}\} .$$

D.L.McQuillan[11] também trabalhou nessa linha, em artigo de 1991.

Vale destacar ainda a publicação recente de um artigo por R. Gilmer, W. Heinzer e D. Lantz[9] sobre o anel $Int(D)$, onde D é um domínio Noetheriano, ser ou não Noetheriano. O assunto aqui tratado tem portanto um caráter bem atual.

Capítulo 1

O A-módulo $Int(A)$

Introdução

Neste capítulo estaremos sempre considerando K um corpo de números algébricos e A o anel de inteiros de K.

Considerando o anel $K[\mathsf{x}]$ de polinômios a uma variável sobre K, nos interessa o subconjunto de $K[\mathsf{x}]$, que denotaremos por $Int(A)$, dos polinômios $P(\mathsf{x})$ sobre K tais que

$$P(A) \subseteq A$$

onde $P(A) = \{P(a)\ ;\ a \in A\}$.

Aqui vamos dar condições necessárias e suficientes para que $Int(A)$ seja um A-módulo livre e, no caso em que essas condições são satisfeitas, dar uma descrição dos elementos da base livre sobre A, que chamaremos de base regular de polinômios a valores inteiros sobre K. O resultado mais objetivo a esse respeito é obtido no caso em que K é um corpo quadrático, mas, no caso geral, mesmo quando não existe uma tal base livre, ainda é possível encontrar um conjunto de geradores para $Int(A)$ sobre A.

Esse capítulo é baseado no trabalho de George Pólya [14], que serviu de fonte para uma série de outros estudos sobre o anel $Int(A)$.

1.1 Bases regulares

Seja K um corpo de números algébricos e A o anel de inteiros de K.

Definição 1.1.1: Um polinômio $P(\mathsf{x}) \in K[\mathsf{x}]$ é dito *inteiro sobre* K se todos os seus coeficientes são inteiros de K.

Mas estamos interessados em polinômios satisfazendo uma propriedade especial.

Definição 1.1.2: Um polinômio $P(\mathsf{x}) \in K[\mathsf{x}]$ é dito *a valores inteiros sobre* K se satisfaz

$$P(A) \subset A \ .$$

Desde que o conjunto dos inteiros de K é um anel, vemos claramente que todo polinômio inteiro sobre K é a valores inteiros sobre K. A recíproca é falsa, isto é, existem polinômios a valores inteiros sobre K que não são inteiros sobre K. Exemplos de polinômios desse tipo podem ser vistos no capítulo 3, exemplos 3.1 e 3.2.

Considere agora o conjunto

$$Int(A) = \{P(\mathsf{x}) \in K[\mathsf{x}] \ ; \ P(A) \subset A\} \ .$$

Então é claro que $Int(A)$ é um subanel do anel de polinômios $K[\mathsf{x}]$, que chamaremos o *anel dos polinômios a valores inteiros sobre* K.

Mas será possível encontrar um subconjunto de polinômios de $Int(A)$ que gera esse anel como um A-módulo? Primeiramente vamos especificar o que queremos desse subconjunto.

Definição 1.1.3: Uma *base regular de polinômios a valores inteiros sobre*

K é uma seqüência de polinômios

$$\{F_i(\mathsf{x})\}_{i=0}^{\infty}$$

em $Int(A)$ que satisfaz as propriedades:

1. $\partial F_m(\mathsf{x}) = m$, onde ∂ denota o grau do polinômio;
2. para todo polinômio $P(\mathsf{x}) \in Int(A)$ com $\partial P(\mathsf{x}) = m$, existem $\beta_0, \beta_1, \cdots, \beta_m \in A$ tais que

$$P(\mathsf{x}) = \beta_m F_m(\mathsf{x}) + \cdots + \beta_1 F_1(\mathsf{x}) + \beta_0 F_0(\mathsf{x}) \ .$$

No exemplo 3.3 do capítulo 3 podemos ver que se K é o corpo dos números racionais $\mathbf{Q}$ então o anel de polinômios a valores inteiros $Int(\mathbf{Z})$ possui uma base regular de polinômios a valores inteiros sobre $\mathbf{Q}$ dada por:

$$F_0(\mathsf{x}) = 1$$

e para cada $m \in \mathbf{N}, m \geq 1$,

$$F_m(\mathsf{x}) = \binom{\mathsf{x}}{m} = \frac{\mathsf{x}(\mathsf{x}-1)\cdots(\mathsf{x}-m+1)}{m!} \ .$$

Observação :

(1) É simples provar que a propriedade 1 nos garante que o conjunto

$$\{F_i(x)\}_{i=0}^{\infty}$$

é K-linearmente independente, logo os β_i na propriedade 2 são únicos.

(2) Observe que $Int(A)$ pode ser considerado como um A-módulo. Então, no caso em que K possui uma base regular de polinômios a valores inteiros, essa base constitui uma A-base livre do A-módulo $Int(A)$.

Nos parágrafos seguintes deste capítulo estaremos interessados em encontrar condições sobre o corpo K e seu anel de inteiros que garantam a existência de uma base regular de polinômios a valores inteiros e, no caso em que ela existir, tentar descrever o melhor possível os polinômios desta base.

1.2 Primeiros Resultados

Nesse parágrafo apresentaremos os primeiros resultados acerca da existência de bases regulares de polinômios a valores inteiros sobre um corpo numérico. Colocaremos uma condição necessária e suficiente para a existência de uma tal base e, no caso em que ela exista, obteremos informações sobre os coeficientes dos polinômios desta base. No caso em que não exista tal base, ainda assim garantiremos a existência de um conjunto gerador de $Int(A)$ como A-módulo.

Proposição 1.2.1: Seja K um corpo de números algébricos e seja x uma variável sobre K. Então a seqüência

$$\left\{ \binom{\mathsf{x}}{n} \right\}_{n \in \mathbf{N}}$$

onde para cada $n > 0$,

$$\binom{\mathsf{x}}{n} = \frac{\mathsf{x}(\mathsf{x}-1)\cdots(\mathsf{x}-n+1)}{n!} \quad \text{e} \quad \binom{\mathsf{x}}{0} = 1$$

é uma K-base do K-espaço vetorial $K[\mathsf{x}]$.

Demonstração:

(1) Como já observamos, o fato de que $\partial\left(\begin{pmatrix} x \\ n \end{pmatrix}\right) = n$ para todo $n \in \mathbf{N}$ já implica que o conjunto $\left\{\begin{pmatrix} x \\ n \end{pmatrix}\right\}_{n\in\mathbf{N}}$ é K-linearmente independente.

(2) Agora vamos mostrar que $\left\{\begin{pmatrix} \mathsf{x} \\ n \end{pmatrix}\right\}_{n\in\mathbf{N}}$ gera $K[\mathsf{x}]$ como K-espaço vetorial.

Seja $P(\mathsf{x}) \in K[\mathsf{x}]$ um polinômio qualquer. Queremos mostrar que $P(\mathsf{x})$ pode ser escrito como combinação linear com coeficientes em K de polinômios em $\left\{\begin{pmatrix} \mathsf{x} \\ n \end{pmatrix}\right\}_{n\in\mathbf{N}}$. Faremos isso por indução sobre o grau de $P(\mathsf{x})$.

Se $\partial P(\mathsf{x}) = 0$, então $P(\mathsf{x}) = a \in K$ e daí podemos escrever

$$P(\mathsf{x}) = a\begin{pmatrix} \mathsf{x} \\ 0 \end{pmatrix}.$$

Suponhamos então $\partial P(\mathsf{x}) = m > 0$ e suponhamos como hipótese de indução que o resultado é válido para todo polinômio com grau menor que m. Então temos

$$P(\mathsf{x}) = Q(\mathsf{x})\begin{pmatrix} \mathsf{x} \\ m \end{pmatrix} + R(\mathsf{x})$$

onde $Q(\mathsf{x}), R(\mathsf{x}) \in K[\mathsf{x}]$ e $\partial R(\mathsf{x}) < \partial\begin{pmatrix} \mathsf{x} \\ m \end{pmatrix} = m$. Mas como $\partial P(\mathsf{x}) = \partial\begin{pmatrix} \mathsf{x} \\ m \end{pmatrix}$, temos que

$$Q(\mathsf{x}) = a \in K,$$

e, por hipótese de indução ,

$$R(\mathrm{x}) = a_{m-1}\binom{\mathrm{x}}{m-1} + \cdots + a_1\binom{\mathrm{x}}{1} + a_0\binom{\mathrm{x}}{0}$$

onde $a_i \in K$ para todo $0 \leq i \leq m-1$. Assim

$$P(\mathrm{x}) = a\binom{\mathrm{x}}{m} + a_{m-1}\binom{\mathrm{x}}{m-1} + \cdots + a_1\binom{\mathrm{x}}{1} + a_0\binom{\mathrm{x}}{0}$$

como queríamos mostrar. ■

Pela proposição 1.2.1, sabemos que todo polinômio $P(\mathrm{x}) \in K[\mathrm{x}]$ de grau m pode ser escrito na forma

$$P(\mathrm{x}) = a_m\binom{\mathrm{x}}{m} + \cdots + a_1\binom{\mathrm{x}}{1} + a_0\binom{\mathrm{x}}{0}$$

onde $a_i \in K$ para todo $0 \leq i \leq m$. Vamos então determinar quem são esses coeficientes.

Considere o operador Δ de Gregory-Newton dado por

$$\begin{aligned} \Delta : \quad & K[\mathrm{x}] \to K[\mathrm{x}] \\ & P(\mathrm{x}) \mapsto \Delta P(\mathrm{x}) = P(\mathrm{x}+1) - P(\mathrm{x}) \, . \end{aligned}$$

Escrevemos indutivamente, para $i \in \mathbf{N}$,

$$\Delta^i P(\mathrm{x}) = (\underbrace{\Delta \circ \cdots \circ \Delta}_{i \text{ vezes}})P(\mathrm{x}) \, .$$

Esse operador possui as seguintes propriedades imediatas:

i. Para todo $a \in K$, $\Delta(a) = 0$;

ii. $\Delta\binom{\mathrm{x}}{n} = \binom{\mathrm{x}}{n-1}$ para todo $n \in \mathbf{N}$, $n \geq 1$;

3. $\Delta aP(\mathsf{x}) = a\Delta P(\mathsf{x})$, para todo $a \in K$ e todo $P(\mathsf{x}) \in K[\mathsf{x}]$;

4. $\Delta(P+Q)(\mathsf{x}) = \Delta P(\mathsf{x}) + \Delta Q(\mathsf{x})$, quaisquer que sejam $P(\mathsf{x}), Q(\mathsf{x}) \in K[\mathsf{x}]$.

Vamos mostrar apenas a propriedade (2). As demais seguem diretamente da definição do operador Δ.

Demonstração: (propriedade 2)

Temos que, dado $n \in \mathbb{N}$, $n \geq 1$

$$\Delta\binom{\mathsf{x}}{n} = \binom{\mathsf{x}+1}{n} - \binom{\mathsf{x}}{n}$$

e queremos então mostrar que

$$\binom{\mathsf{x}+1}{n} - \binom{\mathsf{x}}{n} = \binom{\mathsf{x}}{n-1}.$$

De fato, temos

$$\begin{aligned}
&\binom{\mathsf{x}}{n-1} + \binom{\mathsf{x}}{n} = \\
&= \frac{\mathsf{x}(\mathsf{x}-1)\cdots(\mathsf{x}-(n-2))}{(n-1)!} + \frac{\mathsf{x}(\mathsf{x}-1)\cdots(\mathsf{x}-(n-1))}{n!} = \\
&= \frac{\mathsf{x}(\mathsf{x}-1)\cdots(\mathsf{x}-(n-2))[n! + (\mathsf{x}-(n-1))(n-1)!]}{(n-1)!n!}
\end{aligned}$$

mas

$$\frac{n! + (\mathsf{x}-(n-1))(n-1)!}{(n-1)!} = n + \mathsf{x} - n + 1 = \mathsf{x} + 1$$

e daí segue que

$$\binom{\mathsf{x}}{n-1} + \binom{\mathsf{x}}{n} = \frac{(\mathsf{x}+1)\mathsf{x}(\mathsf{x}-1)\cdots(\mathsf{x}-(n-2))}{n!} = \binom{\mathsf{x}+1}{n}.$$

Portanto

$$\Delta\binom{\mathsf{x}}{n} = \binom{\mathsf{x}+1}{n} - \binom{\mathsf{x}}{n} = \binom{\mathsf{x}}{n-1}$$

como queríamos demonstrar. ■

Observação : As propriedades (3) e (4) nos dizem que o operador Δ é K-linear. Observe ainda que podemos generalizar a propriedade (2) escrevendo

$$\Delta^i\binom{\mathsf{x}}{n} = \binom{\mathsf{x}}{n-i}$$

para quaisquer $n, i \in \mathbb{N}$, $n \geq i$, o que pode ser facilmente demonstrado por indução.

Seja então

$$P(\mathsf{x}) = \sum_{i=0}^{m} a_i \binom{\mathsf{x}}{i}$$

onde $m = \partial P(\mathsf{x})$ e $a_i \in K$ para todo $0 \leq i \leq m$. Usando as propriedades do operador Δ temos

$$a_0 = P(0) = \Delta^0 P(0) \ ;$$

$$\text{e} \qquad \Delta P(\mathsf{x}) = \sum_{i=0}^{m} a_i \Delta\binom{\mathsf{x}}{i} = \sum_{i=1}^{m} a_i \binom{\mathsf{x}}{i-1}$$

donde

$$a_1 = \Delta P(0) \ .$$

Assim recursivamente temos

$$a_i = \Delta^i P(0)$$

para todo $0 \leq i \leq m$.

Agora seja $P(\mathsf{x}) \in K[\mathsf{x}]$ um polinômio qualquer. De acordo com o que vimos acima, podemos escrever $P(\mathsf{x})$ de modo único na forma

$$P(\mathsf{x}) = \Delta^m P(0)\binom{\mathsf{x}}{m} + \cdots + \Delta P(0)\binom{\mathsf{x}}{1} + P(0)$$

onde $m = \partial P(\mathsf{x})$. Assim podemos escrever

$$P(\mathsf{x}) = \frac{\Delta^m P(0)}{m!}\mathsf{x}^m + \cdots \tag{1.2.2}$$

Se A é o anel de inteiros de K, observe que se $P(\mathsf{x}) \in Int(A)$ então

$$\Delta^i P(0) \in A \quad \text{para} \quad 0 \leq i \leq m \ .$$

Em particular, o coeficiente líder de $P(\mathsf{x})$ deve ser o quociente de um inteiro de K por $m!$.

Considere então para cada $m \in \mathrm{N}$ o seguinte conjunto:

$$\mathcal{A}_m = \left\{ \alpha \in A; \begin{array}{l} \alpha \neq 0 \ \text{ e existe } \ P(\mathsf{x}) \in Int(A) \ \text{ com } \ \partial P(\mathsf{x}) = m \\ \text{e tal que } \ \frac{\alpha}{m!} \ \text{ é coeficiente líder de } \ P(\mathsf{x}) \end{array} \right\} \cup \{0\} \ .$$

Proposição 1.2.3: Para cada $m \in \mathrm{N}$, $\mathcal{A}_m$ é um ideal do anel de inteiros de K.

Demonstração:

Sejam $\alpha_1, \alpha_2 \in \mathcal{A}_m$ para $m \in \mathrm{N}$ dado e $\lambda_1, \lambda_2 \in A$. Então se $\lambda_1\alpha_1 + \lambda_2\alpha_2 = 0$, temos imediatamente que $\lambda_1\alpha_1 + \lambda_2\alpha_2 \in \mathcal{A}_m$. Agora, se $\lambda_1\alpha_1 + \lambda_2\alpha_2 \neq 0$ e temos

$$\begin{aligned} P_1(\mathsf{x}) &= \frac{\alpha_1}{m!}\mathsf{x}^m + \cdots \\ \text{e } \ P_2(\mathsf{x}) &= \frac{\alpha_2}{m!}\mathsf{x}^m + \cdots \end{aligned}$$

polinômios em $Int(A)$, então o polinômio

$$\lambda_1 P_1(\mathsf{x}) + \lambda_2 P_2(\mathsf{x}) = \frac{\lambda_1\alpha_1 + \lambda_2\alpha_2}{m!}\mathsf{x}^m + \cdots$$

ainda é um polinômio em $Int(A)$, uma vez que $Int(A)$ é anel e $A \subset Int(A)$. Portanto $\lambda_1\alpha_1 + \lambda_2\alpha_2 \in \mathcal{A}_m$, donde segue que $\mathcal{A}_m$ é ideal. ■

Vamos agora ao primeiro teorema sobre a existência de bases regulares de polinômios a valores inteiros sobre corpos numéricos.

Teorema 1.2.4: Seja K um corpo numérico. K possui uma base regular de polinômios a valores inteiros se, e somente se, para todo $m \in \mathbf{N}$, $\mathcal{A}_m$ é ideal principal de A.

Demonstração:

Suponha primeiramente que K possui uma base regular de polinômios a valores inteiros, digamos

$$\{F_i(\mathsf{x})\}_{i\in\mathbf{N}} .$$

Desde que os polinômios

$$P(\mathsf{x}) = 1 = \frac{1}{0!}\mathsf{x}^0 \quad \text{e} \quad G(\mathsf{x}) = \mathsf{x} = \frac{1}{1!}\mathsf{x}$$

são a valores inteiros sobre K, temos que $1 \in \mathcal{A}_0$ e $1 \in \mathcal{A}_1$ donde segue que

$$\mathcal{A}_0 = \mathcal{A}_1 = (1) .$$

Logo $\mathcal{A}_0$ e $\mathcal{A}_1$ são ideais principais.

Agora seja $m \in \mathbf{N}$, $m > 1$. O polinômio a valores inteiros sobre K de grau m que faz parte da base regular, $F_m(\mathsf{x})$, pode ser escrito na forma

$$F_m(\mathsf{x}) = \frac{\alpha}{m!}\mathsf{x}^m + \cdots$$

como foi visto em 1.2.3, onde $\alpha \in A$. Então pela definição de $\mathcal{A}_m$ devemos ter

$$\alpha \in \mathcal{A}_m .$$

Tome então $a \in \mathcal{A}_m$ qualquer. Existe um polinômio $P(\mathsf{x}) \in Int(A)$ de grau m tal que

$$P(\mathsf{x}) = \frac{a}{m!}\mathsf{x}^m + \cdots \quad .$$

Mas por outro lado podemos escrever

$$P(\mathsf{x}) = \beta_m F_m(\mathsf{x}) + \cdots + \beta_0 F_0(\mathsf{x})$$

onde $\beta_i \in A$ para $0 \leq i \leq n$. Comparando os coeficientes líderes temos então que

$$a = \beta_m . \alpha$$

donde segue que $\mathcal{A}_m = (\alpha)$ e portanto é ideal principal de A.

Reciprocamente, suponha que $\mathcal{A}_m$ é ideal principal para todo $m \in \mathbf{N}$. Vamos construir indutivamente uma base regular de polinômios a valores inteiros sobre K. Tome

$$F_0(\mathsf{x}) = 1 \ .$$

Então todo polinômio $P(\mathsf{x}) \in Int(A)$ de grau 0 claramente é escrito na forma

$$P(\mathsf{x}) = \beta F_0(\mathsf{x})$$

onde $\beta \in A$.

Agora seja $m \in \mathbf{N}$, $m \geq 1$, e suponhamos por hipótese de indução que existam m polinômios em $Int(A)$,

$$F_0(\mathsf{x}), \cdots, F_{m-1}(\mathsf{x})$$

onde $\partial F_i(\mathsf{x}) = i$ para $0 \leq i \leq m-1$, tais que todo polinômio em $Int(A)$ de grau menor ou igual a $m-1$ se escreva como combinação linear desse F_i's com coeficientes em A. Vamos então encontrar um polinômio em $Int(A)$, $F_m(\mathsf{x})$, de grau m e tal que todo polinômio em $Int(A)$ de grau m se escreva como combinação linear com coeficientes em A dos polinômios

$$F_0(\mathsf{x}), \cdots, F_{m-1}(\mathsf{x}), F_m(\mathsf{x}) \ .$$

Por hipótese, $\mathcal{A}_m$ é ideal principal, digamos

$$\mathcal{A}_m = (\alpha)$$

onde $\alpha \in \mathcal{A}_m$. Mas pela definição de $\mathcal{A}_m$, temos que $\alpha \neq 0$ e existe um polinômio em $Int(A)$ de grau m tal que seu coeficiente líder é $\frac{\alpha}{m!}$. Chamando esse polinômio de $F_m(\mathsf{x})$ temos

$$F_m(\mathsf{x}) = \frac{\alpha}{m!}\mathsf{x}^m + \cdots .$$

Seja agora $P(\mathsf{x})$ um polinômio em $Int(A)$ qualquer de grau m. Então podemos escrever

$$P(\mathsf{x}) = \frac{\gamma}{m!}\mathsf{x}^m + \cdots$$

com $\gamma \in A$, e daí $\gamma \in \mathcal{A}_m = (\alpha)$, donde

$$\gamma = \beta.\alpha$$

com $\beta \in A$. Desse modo o polinômio

$$P(\mathsf{x}) - \beta F_m(\mathsf{x})$$

ainda é um polinômio a valores inteiros sobre K e tem grau menor ou igual a $m-1$. Logo, por hipótese de indução , temos

$$P(\mathsf{x}) - \beta F_m(\mathsf{x}) = \beta_0 F_0(\mathsf{x}) + \cdots + \beta_{m-1} F_{m-1}(\mathsf{x})$$

onde $\beta_i \in A$ para todo $0 \leq i \leq m-1$, e portanto

$$P(\mathsf{x}) = \beta_0 F_0(\mathsf{x}) + \cdots + \beta_{m-1} F_{m-1}(\mathsf{x}) + \beta F_m(\mathsf{x})$$

onde $\beta_i \in A$ para todo $0 \leq i \leq m-1$ e $\beta \in A$.

Desse modo construímos em K uma base regular de polinômios a valores inteiros sobre K. ■

Corolário 1.2.5: Todo corpo numérico K com anel de inteiros A principal possui uma base regular de polinômios a valores inteiros.

Demonstração:

Segue diretamente do teorema 1.2.4. ■

Supondo K um corpo de números algébricos que possui uma base regular de polinômios a valores inteiros, surge o interesse em conhecer quem são os polinômios da base. O próximo teorema nos fornece uma informação sobre o coeficiente líder dos polinômios da base.

Teorema 1.2.6: Seja K um corpo de números algébricos que possui uma base regular de polinômios a valores inteiros sobre K. Então existe uma seqüência

$$\{\mu_n\}_{n\in\mathbf{N}}$$

de inteiros de K, tal que o coeficiente líder do polinômio de grau m da base, $m \in \mathbf{N}$, é igual a

$$\frac{1}{\mu_0\mu_1\cdots\mu_m}.$$

Demonstração:

Seja

$$\{F_i\}_{i\in\mathbf{N}}$$

uma base regular de polinômios a valores inteiros sobre K. Pelo teorema

1.2.4, temos que para todo $m \in \mathbf{N}$, o ideal $\mathcal{A}_m$ é principal, e se

$$F_m(\mathsf{x}) = \frac{\alpha}{m!}\mathsf{x}^m + \cdots$$

então $\mathcal{A}_m = (\alpha)$.

Para cada $m \in \mathbf{N}$ temos que o polinômio

$$\mathsf{x}^m = \frac{m!}{m!}\mathsf{x}^m$$

pertence a $Int(A)$. Assim, para cada $m \in \mathbf{N}$,

$$m! \in \mathcal{A}_m = (\alpha) \ .$$

Logo para cada $m \in \mathbf{N}$ existe $M_m \in A$ tal que

$$m! = M_m.\alpha$$

e então podemos escrever para todo $m \in \mathbf{N}$,

$$F_m(\mathsf{x}) = \frac{\alpha}{m!}\mathsf{x}^m + \cdots = \frac{1}{M_m}\mathsf{x}^m + \cdots \ .$$

Agora dado $m \in \mathbf{N}$, o polinômio

$$\mathsf{x}F_{m-1}(\mathsf{x}) = \frac{1}{M_{m-1}}\mathsf{x}^m + \cdots$$

pertence a $Int(A)$, logo pode ser escrito na forma

$$\mathsf{x}F_{m-1}(\mathsf{x}) = \beta_m F_m(\mathsf{x}) + \cdots + \beta_0 F_0(\mathsf{x})$$

onde $\beta_i \in A$ para todo $0 \leq i \leq m$. Tome então

$$\begin{aligned} \mu_0 &= M_0 \\ \text{e} \quad \mu_m &= \beta_m \quad \text{para} \quad m \geq 1 \end{aligned}$$

e considere a seqüência

$$\{\mu_n\}_{n \in \mathbf{N}} \ .$$

Vamos mostrar que para cada $m \in \mathbf{N}$ temos

$$F_m(\mathsf{x}) = \frac{1}{\mu_0\mu_1\cdots\mu_m}\mathsf{x}^m + \cdots .$$

De fato, para todo $m \in \mathbf{N}$ temos

$$\frac{1}{M_{m-1}}\mathsf{x}^m + \cdots = \mathsf{x}F_{m-1}(\mathsf{x}) = \mu_m F_m(\mathsf{x}) + \cdots + \beta_0 F_0(\mathsf{x})$$

e comparando os coeficientes líderes,

$$M_m = \mu_m M_{m-1} .$$

Daí segue que

$$F_m(\mathsf{x}) = \frac{1}{M_m}\mathsf{x}^m + \cdots = \frac{1}{\mu_m M_{m-1}}\mathsf{x}^m + \cdots$$

donde

$$F_m(\mathsf{x}) = \frac{1}{\mu_m\mu_{m-1}M_{m-2}}\mathsf{x}^m + \cdots$$

e assim recursivamente concluímos que

$$F_m(\mathsf{x}) = \frac{1}{\mu_m\cdots\mu_1\mu_0}\mathsf{x}^m + \cdots$$

onde μ_0 deve ser uma unidade já que $\mathcal{A}_0 = (1)$. ■

Observe que a seqüência $\{\mu_n\}_{n\in\mathbf{N}}$ construída na demonstração é única, a menos de unidade. Mudando a base e construindo então uma nova seqüência

$$\{\mu'_n\}_{n\in\mathbf{N}}$$

a partir dessa outra base, vemos que para todo $i \in \mathbf{N}$. μ_i difere de μ'_i por uma unidade. Isso se deve ao fato da determinação dos μ_i's depender apenas do gerador de $\mathcal{A}_i$.

Observe ainda que na demonstração do teorema 1.2.4, se temos que $\mathcal{A}_m$ é ideal principal de A para todo $m \in \mathbf{N}$, digamos $\mathcal{A}_m = (\alpha_m)$, então tomamos para polinômio da base de grau m um polinômio a valores inteiros do tipo

$$F_m(\mathsf{x}) = \frac{\alpha_m}{m!}\mathsf{x}^m + \cdots$$

Mas de acordo com o que foi feito na demonstração do teorema 1.2.6, existe uma seqüência $\{\mu_n\}_{n\in\mathbf{N}}$ de inteiros de K tal que

$$\frac{\alpha_m}{m!} = \frac{1}{\mu_0\mu_1\cdots\mu_m}\,.$$

Desse modo vemos que se o corpo K possui uma base de polinômios a valores inteiros sobre K e conhecemos a seqüência $\{\mu_i\}_{i\in\mathbf{N}}$, então para construir uma tal base basta tomarmos como m-ésimo polinômio da base um polinômio a valores inteiros sobre K da forma

$$F_m(\mathsf{x}) = \frac{1}{\mu_0\mu_1\cdots\mu_m}\mathsf{x}^m + \cdots$$

onde $\mu_0, \mu_1, \cdots, \mu_m$ são elementos da seqüência construída conforme a demonstração do teorema 1.2.6.

Vamos mostrar agora que mesmo no caso em que o corpo de números algébricos K não possui uma base regular de polinômios a valores inteiros, ainda é possível encontrar um conjunto de polinômios um pouco mais fraco que gera $Int(A)$.

Definição 1.2.7: Uma *base irregular de polinômios a valores inteiros* sobre K consiste em uma seqüência de polinômios

$$\{G_n(\mathsf{x})\}_{n\in\mathbf{N}}$$

em $Int(A)$ e um conjunto χ formado por determinadas potências de x,

$$\mathsf{x}^{m_1}, \mathsf{x}^{m_2}, \cdots$$

onde $m_1, m_2, \cdots \in \mathbf{N}$, que satisfazem as seguintes propriedades

1. $\partial G_n(\mathsf{x}) = n$ para todo $n \in \mathrm{N}$;

2. todo polinômio em $Int(A)$ pode ser escrito como combinação linear com coeficientes inteiros de K, de polinômios da seqüência $\{G_n(\mathsf{x})\}_{n\in\mathbf{N}}$ e potências de x do conjunto χ.

Teorema 1.2.8: Todo corpo de números algébricos K possui uma base regular ou uma base irregular de polinômios a valores inteiros sobre K.

Demonstração:

Seja K um corpo de números algébricos. Se para todo $m \in \mathrm{N}$ o ideal $\mathcal{A}_m$ de A é principal então K possui uma base regular de polinômios a valores inteiros sobre K, pelo teorema 1.2.4. Suponhamos então que existe $k \in \mathrm{N}$ tal que $\mathcal{A}_k$ não é ideal principal de A. Vamos construir uma base irregular de polinômios a valores inteiros sobre K. Para isso, dado $m \in \mathrm{N}$, vamos considerar dois casos:

1. Se $\mathcal{A}_m$ é ideal principal. Digamos $\mathcal{A}_m = (\alpha_m)$; nesse caso tome

$$G_m(\mathsf{x}) = \frac{\alpha_m}{m!}\mathsf{x}^m + \cdots$$

um polinômio a valores inteiros sobre K como no teorema 1.2.4.

2. Se $\mathcal{A}_m$ não é principal. Nesse caso, como $m! \in \mathcal{A}_m$, pelo teorema A.1.13, temos que

$$\mathcal{A}_m = (m!, \alpha_m)$$

onde $\alpha_m \in A$. Tome então

$$G_m(\mathsf{x}) = \frac{\alpha_m}{m!}\mathsf{x}^m + \cdots$$

um polinômio a valores inteiros, e a potência de x

$$\mathsf{x}^m \ .$$

Assim, considere a seqüência

$$S = \{G_n(\mathrm{x})\}_{n\in\mathbf{N}}$$

construída acima e o conjunto

$$\chi = \{\mathrm{x}^{m_1}, \mathrm{x}^{m_2}, \cdots\}$$

onde $m_1, m_2, \cdots \in \mathrm{N}$ são tais que $\mathcal{A}_{m_1}, \mathcal{A}_{m_2}, \cdots$ são todos os ideais do tipo $\mathcal{A}_m$ com $m \in \mathrm{N}$ que não são principais. Vamos mostrar que a seqüência S e o conjunto χ constituem uma base irregular de polinômios a valores inteiros sobre K.

Seja $P(\mathrm{x})$ um polinômio qualquer em $Int(A)$. Como $\mathcal{A}_0 = \mathcal{A}_1 = (1)$ temos que, se $\partial P(\mathrm{x}) = 0$ então $P(\mathrm{x}) = \beta \in A$ e assim

$$P(\mathrm{x}) = \beta G_0(\mathrm{x}) \ ;$$

se $\partial P(\mathrm{x}) = 1$, então $P(\mathrm{x}) = \beta\mathrm{x} + \gamma$ com $\beta, \gamma \in A$ e assim

$$P(\mathrm{x}) = \beta G_1(\mathrm{x}) + \gamma G_0(\mathrm{x}) \ .$$

Seja agora $m \in \mathrm{N}$, $m \geq 2$, e suponhamos que $\partial P(\mathrm{x}) = m$. Suponhamos também, por hipótese de indução, que todo polinômio em $Int(A)$ de grau menor que m pode ser escrito na forma desejada. Então novamente temos dois casos:

(a) Se $\mathcal{A}_m$ é principal, procedemos de modo análogo à demonstração do teorema 1.2.4 e obtemos a combinação linear desejada.

(b) Se $\mathcal{A}_m$ não é ideal principal, sabemos que $P(\mathrm{x})$ pode ser escrito na forma

$$P(\mathrm{x}) = \frac{\beta}{m!}\mathrm{x}^m + \cdots$$

com $\beta \in A$. Assim $\beta \in \mathcal{A}_m = (m!, \alpha_m)$, como vimos em (1), logo

$$\beta = a.m! + b.\alpha_m$$

onde $a, b \in A$. Usando a hipótese de indução temos então que

$$P(\mathsf{x}) - bG_m(\mathsf{x}) - a\mathsf{x}^m = \sum_{i=1}^{m-1} \gamma_i G_i(\mathsf{x}) + \sum_{\mathsf{x}^k \in \chi} \gamma_k \mathsf{x}^k$$

uma vez que esse polinômio tem grau menor que m. Daí segue que $P(\mathsf{x})$ pode ser escrito na forma desejada.

Dessa forma temos que a seqüência $\{G_n(\mathsf{x})\}_{n\in\mathbf{N}}$ e o conjunto χ constituem uma base irregular de polinômios a valores inteiros sobre K, como queríamos demonstrar. ■

Observação : Note que os números naturais $m_1, m_2, \cdots$ são aqueles para os quais os ideais $\mathcal{A}_{m_1}, \mathcal{A}_{m_2}, \cdots$ não são ideais principais de A.

1.3 Sobre Congruências

Nesse parágrafo vamos apresentar alguns resultados sobre congruências do tipo

$$P(\mathsf{x}) \equiv 0 \ (I)$$

onde $P(\mathsf{x})$ é um polinômio inteiro sobre K e I é um ideal de A. Esses resultados nos auxiliarão nos parágrafos seguintes a demonstrar outros teoremas sobre bases regulares de polinômios a valores inteiros sobre um corpo numérico.

Durante esse parágrafo estaremos sempre considerando $P(\mathsf{x})$ um polinômio inteiro sobre K.

Definição 1.3.1: Dado um polinômio $P(\mathsf{x})$ inteiro sobre K e um ideal I de

A, dizemos que a congruência

$$P(\mathrm{x}) \equiv 0\ (I)$$

é *sempre satisfeita* se esta é satisfeita para todo inteiro x de K.

Teorema 1.3.2: Seja $P(\mathrm{x}) \in K[\mathrm{x}]$ um polinômio inteiro sobre K de grau m e seja $\mathcal{P}$ um ideal primo de A. Se existe um coeficiente de $P(\mathrm{x})$ que não pertence a $\mathcal{P}$ e se a congruência

$$P(\mathrm{x}) \equiv 0\ (\mathcal{P}^a)$$

é sempre satisfeita, onde $a \in \mathbf{N}$, então

$$a \leq \left[\frac{m}{N}\right] + \left[\frac{m}{N^2}\right] + \cdots = \sum_{i=1}^{\infty} \left[\frac{m}{N^i}\right] \tag{1.3.3}$$

onde $N = N(\mathcal{P})$ indica a norma do ideal $\mathcal{P}$ e $\left[\frac{m}{N^i}\right] = \max\{n \in \mathbf{N}, n \leq \frac{m}{N^i}\}$ para todo $i \in \mathbf{N}$.

Antes de demonstrar o teorema 1.3.2, vamos mostrar que a série à direita na desigualdade 1.3.3 converge. Vamos ainda mostrar alguns fatos que nos serão úteis na demonstração.

Primeiramente vamos mostrar que a série de termos inteiros à direita na desigualdade 1.3.3 converge. Na verdade vamos mostrar que essa série tem apenas h termos não nulos, onde

$$h = \left[\frac{\log m}{\log N}\right],$$

isto é, o maior inteiro menor ou igual a $\frac{\log m}{\log N}$. De fato, o termo $\left[\frac{m}{N^k}\right]$ se anula quando $N^k > m$. Assim se para todo $i \in \mathbf{N}$ temos $m < N^i$, então a série é

nula. Suponhamos que existe $h \in \mathrm{N}$ tal que $m \geq N^h$. Podemos tomar esse h máximo, ou seja, tomar h de forma que

$$N^h \leq m < N^{h+1} .$$

Nesse caso, para $i \leq h$ temos $m \geq N^i$ e daí todos os termos da série com $i \leq h$ não são nulos. Por outro lado, para $i > h$ temos $m < N^i$ e consequentemente os termos da série com $i > h$ são nulos. Logo a série em questão possui apenas h termos não nulos, onde h é o único inteiro tal que

$$N^h \leq m \leq N^{h+1}$$

ou seja

$$h = \left[\frac{\log m}{\log N}\right] .$$

Agora vamos construir uma seqüência de polinômios que satisfazem as hipóteses do teorema 1.3.2 e tais que a igualdade ocorre em 1.3.3. Com isso estaremos mostrando que o limite superior dado por 1.3.3 não pode ser reduzido. Além disso esses polinômios possuem propriedades, que aqui serão demonstradas, que nos auxiliarão na prova do teorema 1.3.2.

Seja $\mathcal{P}$ um ideal primo de A e seja

$$\{\rho_0, \rho_1, \cdots, \rho_{N-1}\}$$

um sistema completo de resíduos módulo $\mathcal{P}$, onde $N = N(\mathcal{P})$ é a norma do ideal $\mathcal{P}$. A é anel de Dedekind, então tome

$$\pi \in \mathcal{P} \quad \text{tal que} \quad \pi \notin \mathcal{P}^2$$

Para cada $n \in \mathrm{N}$, podemos escrever o número n no sistema numérico com base N na forma

$$n = c_0 + c_1 N + \cdots + c_h N^h$$

onde $0 \leq c_i \leq N-1$ para $0 \leq i \leq h$. Definimos então uma seqüência de inteiros de A

$$\{\alpha_n\}_{n \in \mathbf{N}} \tag{1.3.4}$$

onde para cada $n \in \mathrm{N}$, α_n é dado por

$$\alpha_n = \rho_{c_0} + \rho_{c_1}\pi + \rho_{c_2}\pi^2 + \cdots + \rho_{c_h}\pi^h \ .$$

Daremos agora três propriedades úteis que essa seqüência possui.

Propriedade 1: Se $m, n \in \mathrm{N}$ e $m \neq n$, então a maior potência do ideal primo $\mathcal{P}$ à qual $\alpha_m - \alpha_n$ pertence é igual à maior potência de N que divide $m-n$.

Demonstração:

Em outras palavras, a propriedade 1 afirma que

$$(1) \qquad \alpha_m - \alpha_n \equiv 0 \ (\mathcal{P}^a) \quad \text{e} \quad \alpha_m - \alpha_n \not\equiv 0 \ (\mathcal{P}^{a+1})$$

se e somente se

$$(2) \qquad m - n \equiv 0 \ (N^a) \quad \text{e } m - n \not\equiv 0 \ (N^{a+1}) \ .$$

onde $a \in \mathrm{N}$.

De fato, temos que m e n podem ser escritos no sistema numérico de base N na forma

$$\begin{aligned} m &= c_0 + c_1 N + \cdots + c_{a-1}N^{a-1} + c_a N^a + \cdots \\ n &= c_0' + c_1' N + \cdots + c_{a-1}'N^{a-1} + c_a' N^a + \cdots \end{aligned}$$

Supondo que (2) ocorre, temos que

$$c_i = c_i' \quad \text{para} \quad 0 \leq i \leq a-1 \quad \text{e} \quad c_a \neq c_a' \ .$$

Desse modo,

$$\alpha_m - \alpha_n = (\rho_{c_a} - \rho_{c_a'})\pi^a + \cdots$$

donde segue que (1) ocorre. Reciprocamente, como

$$\begin{aligned} \alpha_m &= \rho_{c_0} + \rho_{c_1}\pi + \cdots + \rho_{c_a}\pi^a + \cdots \\ \alpha_n &= \rho_{c'_0} + \rho_{c'_1}\pi + \cdots + \rho_{c'_a}\pi^a + \cdots , \end{aligned}$$

então supondo que (1) ocorre temos que

$$\rho_{c_i} = \rho_{c'_i} \quad \text{para} \quad 0 \leq i \leq a-1 \quad \text{e} \quad \rho_{c_a} \neq \rho_{c'_a} .$$

Assim, como $\{\rho_0, \cdots, \rho_{N-1}\}$ é um sistema completo de resíduos módulo $\mathcal{P}$ temos que

$$c_i = c'_i \quad \text{para} \quad 0 \leq i \leq a-1 \quad \text{e} \quad c_a \neq c'_a .$$

Logo (2) ocorre. ■

Propriedade 2: A maior potência de $\mathcal{P}$ à qual pertence o produto

$$(\alpha_{m_1} - \alpha_{n_1})(\alpha_{m_2} - \alpha_{n_2}) \cdots (\alpha_{m_k} - \alpha_{n_k})$$

onde $m_1, \cdots, m_k, n_1, \cdots, n_k \in \mathbf{N}$, pode ser obtida pelo estudo das diferenças

$$m_1 - n_1,\ m_2 - n_2,\ \cdots,\ m_k - n_k .$$

De fato, se para cada i, $1 \leq i \leq k$, temos

$$\begin{aligned} m_i - n_i &\equiv (N^{a_i}) \\ \text{e} \quad m_i - n_i &\not\equiv (N^{a_i+1}) \end{aligned}$$

onde $a_i \in \mathbf{N}$ para todo $0 \leq i \leq k$, então

$$\begin{aligned} (m_1 - n_1) \cdots (m_k - n_k) &\equiv 0\,(N^{a_1+\cdots+a_k}) \\ \text{e} \quad (m_1 - n_1) \cdots (m_k - n_k) &\not\equiv 0\,(N^{a_1+\cdots+a_k+1}) \end{aligned}$$

donde segue pela propriedade 1 que

$$\begin{aligned} (\alpha_{m_1} - \alpha_{n_1}) \cdots (\alpha_{m_k} - \alpha_{n_k}) &\equiv 0\,(\mathcal{P}^{a_1+\cdots+a_k}) \\ \text{e} \quad (\alpha_{m_1} - \alpha_{n_1}) \cdots (\alpha_{m_k} - \alpha_{n_k}) &\not\equiv 0\,(\mathcal{P}^{a_1+\cdots+a_k+1}) . \end{aligned}$$

Propriedade 3: Se $a \in A$ então o conjunto

$$\{\alpha_0, \alpha_1, \cdots, \alpha_{N^a-1}\}$$

é um sistema completo de resíduos módulo o ideal $\mathcal{P}^a$.

Demonstração:

A cardinalidade desse conjunto é

$$N^a = N(\mathcal{P}^a) .$$

Basta então mostrarmos que se

$$0 \leq m < N^a \quad \text{e} \quad 0 \leq n < N^a$$

então

$$\alpha_m - \alpha_n \not\equiv 0 \ (\mathcal{P}^a) .$$

Mas isso segue imediatamente da propriedade 1, uma vez que $0 \leq m < N^a$ e $0 \leq n < N^a$ implicam que

$$m - n \not\equiv 0 \ (N^a) .$$

■

A partir da seqüência $\{\alpha_n\}_{n\in\mathbf{N}}$, construiremos agora a seqüência de polinômios mencionada anteriormente e com a ajuda das propriedades 1, 2 e 3 mostraremos algumas propriedades satisfeitas pelos polinômios dessa seqüência.

Se $\{\alpha_n\}_{n\in\mathbf{N}}$ é a seqüência definida em 1.3.4, então defina uma seqüência

$$\{f_n(x)\}_{n\in\mathbf{N}} \tag{1.3.5}$$

de polinômios inteiros sobre K da seguinte maneira:

$$f_0(x) = 1$$

e para cada $n \in \mathbf{N}$, $n \geq 1$,

$$f_n(\mathsf{x}) = (\mathsf{x} - \alpha_0)(\mathsf{x} - \alpha_1) \cdots (\mathsf{x} - \alpha_{n-1}) \, .$$

No que se segue, mostraremos duas propriedades da seqüência 1.3.5. Para isso vamos fixar a notação

$$\psi(m) = \sum_{i=1}^{\infty} \left[\frac{m}{N^i} \right]$$

onde $m \in \mathbf{N}$ é um natural qualquer.

Propriedade 4: Dado $m \in \mathbf{N}$ temos

$$\begin{aligned} f_m(\alpha_m) &\equiv 0 \, (\mathcal{P}^{\psi(m)}) \\ \text{e} \quad f_m(\alpha_m) &\not\equiv 0 \, (\mathcal{P}^{\psi(m)+1}) \, . \end{aligned}$$

Demonstração:

Temos que, dado $m \in \mathbf{N}$,

$$f_m(\alpha_m) = (\alpha_m - \alpha_0)(\alpha_m - \alpha_1) \cdots (\alpha_m - \alpha_{m-1}) \, ,$$

logo para provar a propriedade 4 basta usar a propriedade 2 e observar as diferenças

$$m - 0, \, m - 1, \, \cdots \, m - (m-1) \, .$$

Para cada $i \in \mathbf{N}$ temos entre essas diferenças, $\left[\frac{m}{N^i} \right]$ elementos divisíveis por N^i e $\left[\frac{m}{N^{i+1}} \right]$ elementos divisíveis por N^{i+1}. Então temos

$$\left[\frac{m}{N^i} \right] - \left[\frac{m}{N^{i+1}} \right]$$

elementos que são divisíveis por N^i mas que não são divisíveis por N^{i+1}. Desse modo, a maior potência de N que divide o produto

$$(m-0)(m-1) \cdots (m-(m-1))$$

tem expoente

$$1\left(\left[\frac{m}{N}\right]-\left[\frac{m}{N^2}\right]\right)+2\left(\left[\frac{m}{N^2}\right]-\left[\frac{m}{N^3}\right]\right)+\cdots+i\left(\left[\frac{m}{N^i}\right]-\left[\frac{m}{N^{i+1}}\right]\right)+\cdots$$

ou seja

$$\left[\frac{m}{N}\right]+\left[\frac{m}{N^2}\right]+\left[\frac{m}{N^3}\right]+\cdots+\left[\frac{m}{N^i}\right]+\cdots=\psi(m)$$

Portanto pela propriedade 2 temos o resultado desejado. ■

Propriedade 5: Para cada $m \in \mathbf{N}$, a congruência

$$f_m(\mathsf{x}) \equiv 0 \ (\mathcal{P}^{\psi(m)})$$

é sempre satisfeita.

Demonstração:

Seja $a \in A$ um inteiro de K. Pela proriedade 3, existe $k \in \mathbf{N}$ com $0 \leq k \leq N^{\psi(m)}$, tal que

$$a \equiv \alpha_k \ (\mathcal{P}^{\psi(m)}) \ .$$

Assim temos

$$f_m(a) \equiv f_m(\alpha_k) = (\alpha_k-\alpha_0)(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_{m-1}) \ \ (\mathcal{P}^{\psi(m)}) \ .$$

Se $k < m$ então claramente o resultado é válido. Suponhamos então $k \geq m$.

Observando as diferenças

$$k-0,\ k-1,\ \cdots,\ k-(m-1)$$

vemos que entre elas temos

$$\left[\frac{k}{N^i}\right]-\left[\frac{k-m}{N^i}\right]$$

são divisíveis por N^i. Logo temos entre essas diferenças

$$\left(\left[\frac{k}{N^i}\right]-\left[\frac{k-m}{N^i}\right]\right)-\left(\left[\frac{k}{N^{i+1}}\right]-\left[\frac{k-m}{N^{i+1}}\right]\right)$$

que são divisíveis por N^i mas não são divisíveis por nenhuma potência maior de N. Assim, como na propriedade 2, a maior potência de $\mathcal{P}$ à qual $f_m(\alpha_k)$ pertence tem expoente

$$\sum_{i=1}^{\infty} i\left\{\left(\left[\frac{k}{N^i}\right]-\left[\frac{k-m}{N^i}\right]\right)-\left(\left[\frac{k}{N^{i+1}}\right]-\left[\frac{k-m}{N^{i+1}}\right]\right)\right\}=$$
$$=\sum_{i=1}^{\infty}\left(\left[\frac{k}{N^i}\right]-\left[\frac{k-m}{N^i}\right]\right)$$

Desse modo basta provarmos que

$$\sum_{i=1}^{\infty}\left(\left[\frac{k}{N^i}\right]-\left[\frac{k-m}{N^i}\right]\right)\geq\psi(m)\ .$$

Mas essa desigualdade equivale à desigualdade

$$\sum_{i=1}^{\infty}\left[\frac{k}{N^i}\right]\geq\sum_{i=1}^{\infty}\left(\left[\frac{m}{N^i}\right]+\left[\frac{k-m}{N^i}\right]\right)$$

que é claramente válida. Portanto temos provado a propriedade 5. ■

Observe agora que pelas propriedades 3 e 5 temos que, para cada $m \in$ N, o polinômio $f_m(\mathsf{x})$ satisfaz as hipóteses do teorema 1.3.2 e nos fornece a igualdade em 1.3.3. Por outro lado a propriedade 4 nos garante que a congruência

$$f_m(\mathsf{x}) \equiv 0\ (\mathcal{P}^{\psi(m)+1})$$

não é sempre satisfeita. Em resumo, mostramos que para cada $m \in$ N o teorema 1.3.2 é válido para o polinômio $f_m(\mathsf{x})$ e mais. que o limite superior $\psi(m)$ não pode ser reduzido, uma vez que $f_m(\mathsf{x})$ nos fornece a igualdade em 1.3.3.

Agora vamos mostrar um último lema sobre os polinômios de 1.3.5 antes de realizar a demonstração do teorema 1.3.2.

Lema 1.3.6: Todo polinômio inteiro sobre K, $P(\mathsf{x})$ de grau $m \in$ N pode

ser escrito na forma

$$P(\mathsf{x}) = \gamma_0 f_0(\mathsf{x}) + \gamma_1 f_1(\mathsf{x}) + \cdots + \gamma_m f_m(\mathsf{x})$$

onde $\gamma_0, \gamma_1, \cdots, \gamma_m \in A$. Além disso, se $\mathcal{P}$ é um ideal primo de A e existe algum coeficiente de $P(\mathsf{x})$ que não pertence a $\mathcal{P}$, então existe γ_i, com $0 \leq i \leq m$, que não pertence a $\mathcal{P}$.

Demonstração:

Seja $P(\mathsf{x})$ um polinômio inteiro sobre K. A primeira afirmação será mostrada por indução sobre o grau de $P(\mathsf{x})$.

Se $\partial P(\mathsf{x}) = 0$ então $P(\mathsf{x}) = \gamma \in A$, donde segue que

$$P(\mathsf{x}) = \gamma f_0(\mathsf{x})$$

Suponha agora que $\partial P(\mathsf{x}) = m \geq 1$, e suponha ainda por hipótese de indução que a afirmação é válida para todo polinômio inteiro sobre K de grau menor que m. Seja

$$P(\mathsf{x}) = \beta_0 + \beta_1 \mathsf{x} + \cdots + \beta_m \mathsf{x}^m$$

onde $\beta_i \in A$ para todo $0 \leq i \leq m$. Então o polinômio $P(\mathsf{x}) - \beta_m f_m(\mathsf{x})$ tem grau menor que m, logo por hipótese de indução pode ser escrito na forma

$$P(\mathsf{x}) - \beta_m f_m(\mathsf{x}) = \gamma_0 f_0(\mathsf{x}) + \cdots + \gamma_{m-1} f_{m-1}(\mathsf{x})$$

onde $\gamma_i \in A$ para todo $0 \leq i \leq m-1$. Portanto tomando $\gamma_m = \beta_m$ temos

$$P(\mathsf{x}) = \gamma_0 f_0(\mathsf{x}) + \cdots + \gamma_{m-1} f_{m-1}(\mathsf{x}) + \gamma_m f_m(\mathsf{x})$$

donde $P(\mathsf{x})$ pode ser escrito na forma desejada. Assim está provada a primeira afirmação do lema.

Para provar a segunda afirmação basta notar que se $\mathcal{P}$ é ideal primo de A e $\gamma_i \in \mathcal{P}$ para todo $0 \leq i \leq m$, então é claro que temos um coeficiente de $P(\mathsf{x})$ pertencendo a $\mathcal{P}$. ■

Finalmente vamos à demonstração do teorema 1.3.2.

Demonstração do Teorema 1.3.2:

Seja $P(\mathsf{x}) \in K[\mathsf{x}]$ um polinômio inteiro sobre K de grau m. Pelo lema 1.3.6 sabemos que $P(\mathsf{x})$ pode ser escrito na forma

$$P(\mathsf{x}) = \gamma_0 f_0(\mathsf{x}) + \cdots + \gamma_s f_s(\mathsf{x}) + \cdots + \gamma_m f_m(\mathsf{x})$$

onde para todo $0 \leq i \leq m$ temos $\gamma_i \in A$ e f_i é elemento da seqüência dada em 1.3.5. Suponhamos então por absurdo que $\mathcal{P}$ é um ideal primo de A tal que

$$P(\mathsf{x}) \equiv 0 \ (\mathcal{P}^a) \tag{1.3.7}$$

é sempre satisfeita, onde $a \in \mathbf{N}$, existe

$$\gamma_s \not\equiv 0 \ (\mathcal{P}) \tag{1.3.8}$$

onde $0 \leq s \leq m$, e ainda

$$a > \psi(m) \ . \tag{1.3.9}$$

Então temos que

$$\gamma_s \not\equiv 0 \ (\mathcal{P}^{a-\psi(s)}) \ .$$

De fato, como $s \leq m$ temos

$$a - \psi(s) = a - \psi(m) + \psi(m) - \psi(s) \geq a - \psi(m) > 0$$

por 1.3.9; logo se

$$\gamma_s \equiv 0 \ (\mathcal{P}^{a-\psi(s)})$$

então

$$\gamma_s \equiv 0 \ (\mathcal{P}) \ ,$$

o que contraria 1.3.8.

Escolha então $t \in \mathbb{N}$, $0 \leq t \leq m$, tal que

$$\gamma_t \not\equiv 0 \ (\mathcal{P}^{a-\psi(t)}) \tag{1.3.10}$$

$$\text{e} \quad \gamma_i \equiv 0 \ (\mathcal{P}^{a-\psi(i)})$$

para todo $0 \leq i < t$, isto é, t é o menor inteiro entre 0 e m com a propriedade 1.3.10. Considere o elemento α_t da seqüência 1.3.4. Então pelo fato da congruência 1.3.7 ser sempre satisfeita temos que

$$\gamma_0 f_0(\alpha_t) + \cdots + \gamma_t f_t(\alpha_t) + \cdots + \gamma_m f_m(\alpha_t) \equiv 0 \ (\mathcal{P}^a)$$

donde pela definição 1.3.5 segue que

$$\gamma_0 f_0(\alpha_t) + \cdots + \gamma_{t-1} f_{t-1}(\alpha_t) + \gamma_t f_t(\alpha_t) + \equiv 0 \ (\mathcal{P}^a) \ .$$

Agora, pela propriedade 5 temos que

$$f_i(\alpha_t) \equiv 0 \ (\mathcal{P}^{\psi(i)})$$

para todo $0 \leq i \leq m$, e pela escolha de t temos ainda que

$$\gamma_i \equiv 0 \ (\mathcal{P}^{a-\psi(i)})$$

para todo $0 \leq i < t$. Logo segue que

$$\gamma_i f_i(\alpha_t) \equiv 0 \ (\mathcal{P}^a)$$

para todo $0 \leq i < t$. Desse modo,

$$\gamma_t f_t(\alpha_t) \equiv 0 \ (\mathcal{P}^a)$$

donde segue pela propriedade 4 que

$$\gamma_t \equiv 0 \ (\mathcal{P}^{a-\psi(t)})$$

o que contraria 1.3.10.

Portanto devemos ter

$$a \leq \psi(m)$$

como queríamos demonstrar. ■

Agora vamos considerar $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \cdots$ todos os ideais primos de A indicados por ordem crescente da norma, e $N_1, N_2, N_3, \cdots$ suas respectivas normas.

Teorema 1.3.11: Sejam $P(\mathrm{x}) \in K[\mathrm{x}]$ um polinômio inteiro sobre K de grau m, e I um ideal de A. Considere para cada $i \in \mathrm{N}$ o número inteiro

$$a_i = \left[\frac{m}{N_i}\right] + \left[\frac{m}{N_i^2}\right] + \left[\frac{m}{N_i^3}\right] + \cdots .$$

Nessa condições, se a congruência

$$P(\mathrm{x}) \equiv 0 \ (I)$$

é sempre satisfeita então I divide o ideal

$$\prod_{i=1}^{\infty} \mathcal{P}_i^{a_i} .$$

Demonstração:

Sabemos que A é anel de Dedekind, logo o ideal I pode ser escrito na forma

$$I = \mathcal{P}_{i_1}^{\alpha_1} . \mathcal{P}_{i_2}^{\alpha_2} \cdots \mathcal{P}_{i_n}^{\alpha_n}$$

onde para todo $j \in \mathrm{N}$ temos $i_j, \alpha_j \in \mathrm{N}$. Por hipótese, a congruência

$$P(\mathrm{x}) \equiv 0 \ (I)$$

é sempre satisfeita, logo para todo $a \in A$ temos

$$P(a) \in I = \mathcal{P}_{i_1}^{\alpha_1} . \mathcal{P}_{i_2}^{\alpha_2} \cdots \mathcal{P}_{i_n}^{\alpha_n} \subset \mathcal{P}_{i_j}^{\alpha_j}$$

para todo $j \in \mathrm{N}$. Assim a congruência

$$P(\mathrm{x}) \equiv 0 \ (\mathcal{P}_{i_j}^{\alpha_j})$$

é sempre satisfeita para todo $1 \leq j \leq n$. Segue então do teorema 1.3.2 que

$$\alpha_j \leq a_j$$

para todo $1 \leq j \leq n$, e portanto o ideal I divide o ideal

$$\prod_{i=1}^{\infty} \mathcal{P}_i^{a_i} \ ,$$

como queríamos mostrar. ■

Por outro lado, se a_i, $i \in \mathrm{N}$, são os números naturais definidos no teorema 1.3.11, então dado $m \in \mathrm{N}$ podemos determinar um polinômio primitivo $P(\mathrm{x}) \in K[\mathrm{x}]$ de grau m e inteiro sobre K, e um ideal I de A que divide o ideal $\prod_{i=1}^{\infty} \mathcal{P}_i^{a_i}$, tais que a congruência

$$P(\mathrm{x}) \equiv 0 \ (I)$$

é sempre satisfeita. De fato:

Sejam $\mathcal{P}_1, \cdots, \mathcal{P}_l$ todos os ideais primos de A cuja norma é menor ou igual a m. Do mesmo modo que definimos 1.3.5 e pela propriedade 5, podemos determinar l polinômios inteiros de grau m

$$\begin{aligned} H_1(\mathrm{x}) &= (\mathrm{x} - \alpha_{01})(\mathrm{x} - \alpha_{11}) \cdots (\mathrm{x} - \alpha_{m-1\,1}) \\ H_2(\mathrm{x}) &= (\mathrm{x} - \alpha_{02})(\mathrm{x} - \alpha_{12}) \cdots (\mathrm{x} - \alpha_{m-1\,2}) \\ &\vdots \\ H_l(\mathrm{x}) &= (\mathrm{x} - \alpha_{0l})(\mathrm{x} - \alpha_{1l}) \cdots (\mathrm{x} - \alpha_{m-1\,l}) \end{aligned}$$

todos com coeficiente líder 1, e portanto primitivos, e tais que as congruências

$$H_i(\mathsf{x}) \equiv 0 \ (\mathcal{P}_i^{a_i})$$

são sempre satisfeitas para todo $1 \leq i \leq l$. Agora resolvendo o sistema de congruências

$$\begin{cases} \beta_j & \equiv & \alpha_{j_1} & (\mathcal{P}_1^{a_1}) \\ \beta_j & \equiv & \alpha_{j_2} & (\mathcal{P}_2^{a_2}) \\ & \vdots & & \vdots \\ \beta_j & \equiv & \alpha_{j_l} & (\mathcal{P}_l^{a_l}) \end{cases}$$

em A para cada $0 \leq j \leq m-1$, determinamos o polinômio

$$H(\mathsf{x}) = (\mathsf{x} - \beta_0)(\mathsf{x} - \beta_1) \cdots (\mathsf{x} - \beta_{m-1})$$

inteiro sobre K, primitivo, e tal que

$$H(\mathsf{x}) \equiv H_i(\mathsf{x}) \ (\mathcal{P}_i^{a_i})$$

identicamente em x para todo $1 \leq i \leq l$. Isto é, para cada $1 \leq i \leq l$ passando os polinômios $H(\mathsf{x})$ e $H_i(\mathsf{x})$ ao quociente $\frac{A}{\mathcal{P}_i^{a_i}}$ temos que os polinômios

$$\overline{H}(\mathsf{x}) = (\mathsf{x} - \overline{\beta_0})(\mathsf{x} - \overline{\beta_1}) \cdots (\mathsf{x} - \overline{\beta_{m-1}})$$

e

$$\overline{H}_i(\mathsf{x}) = (\mathsf{x} - \overline{\alpha_{0i}})(\mathsf{x} - \overline{\alpha_{1i}}) \cdots (\mathsf{x} - \overline{\alpha_{m-1\,i}})$$

são iguais, uma vez que são mônicos, de mesmo grau m e possuem m raízes iguais. Assim, para todo $a \in A$ temos que

$$H(a) \equiv H_i(a) \equiv 0 \ (\mathcal{P}_i^{a_i})$$

para todo $1 \leq i \leq l$, donde segue que

$$H(a) \equiv 0 \ (\cap_{i=1}^{l} \mathcal{P}_i^{a_i}) \ .$$

Mas como A é anel de Dedekind,

$$\mathcal{P}_i^{a_i} + \mathcal{P}_j^{a_j} = A$$

quaisquer que sejam $i, j \in \mathrm{N}$, $i \neq j$, e então

$$\cap_{i=1}^{l} \mathcal{P}_i^{a_i} = \prod_{i=1}^{l} \mathcal{P}_i^{a_i} .$$

Portanto temos que a congruência

$$H(\mathrm{x}) \equiv 0 \, (\prod_{i=1}^{l} \mathcal{P}_i^{a_i})$$

é sempre satisfeita. Logo tomando

$$P(\mathrm{x}) = H(\mathrm{x}) \quad \mathrm{e} \quad I = \prod_{i=1}^{l} \mathcal{P}_i^{a_i}$$

temos provada a afirmação feita.

1.4 Corpos numéricos principais

Chamamos de corpo numérico principal a todo corpo numérico cujo anel de inteiros é principal.

Sabemos pelo corolário 1.2.5 que todo corpo numérico principal K possui uma base regular de polinômios a valores inteiros. Nesse parágrafo vamos utilizar os resultados obtidos no parágrafo 3 para dar continuidade ao estudo dessa base. Explicitaremos nesse caso o produto

$$\mu_0 \mu_1 \cdots \mu_m$$

onde $m \in \mathrm{N}$ e $\{\mu_n\}_{n \in \mathbf{N}}$ é a seqüência definida no teorema 1.2.6, e daremos mais detalhes sobre a escolha dos polinômios da base.

Durante esse parágrafo estaremos sempre considerando K um corpo numérico principal. Nesse caso A é um domínio de ideais prinicipais e portanto um domínio fatorial.

Proposição 1.4.1: Considere o polinômio

$$P(\mathsf{x}) = \frac{\alpha_m}{\beta_m}\mathsf{x}^m + \cdots + \frac{\alpha_1}{\beta_1}\mathsf{x} + \frac{\alpha_0}{\beta_0} \in K[\mathsf{x}]$$

onde $\alpha_0, \cdots, \alpha_m, \beta_0, \cdots, \beta_m \in A$ e são tais que

$$\mathrm{mdc}(\alpha_i, \beta_i) = 1$$

para todo $0 \leq i \leq m$. Então $P(\mathsf{x})$ pode ser escrito na forma

$$P(\mathsf{x}) = \frac{\alpha}{\beta}(\gamma_m\mathsf{x}^m + \cdots + \gamma_1\mathsf{x} + \gamma_0)$$

onde o polinômio $\gamma_m\mathsf{x}^m + \cdots + \gamma_1\mathsf{x} + \gamma_0 \in A[\mathsf{x}]$ é primitivo, $\alpha, \beta \in A$ com $\mathrm{mdc}(\alpha, \beta) = 1$, e β é divisível por β_i para todo $0 \leq i \leq m$.

Demonstração:

Podemos escrever

$$P(\mathsf{x}) = \frac{\gamma'_m\mathsf{x}^m + \cdots + \gamma'_1\mathsf{x} + \gamma'_0}{\beta'}$$

onde $\beta' \in A$ e $\gamma'_i \in A$ para todo $0 \leq i \leq m$. Tomando

$$\alpha' = \mathrm{mdc}(\{\gamma'_i \,; 0 \leq i \leq m\}) \tag{1.4.2}$$

temos então que

$$P(\mathsf{x}) = \frac{\alpha'}{\beta'}(\gamma_m\mathsf{x}^m + \cdots + \gamma_1\mathsf{x} + \gamma_0)$$

e é claro que podemos substituir α' e β' por α e β respectivamente, tais que $\mathrm{mdc}(\alpha, \beta) = 1$. Resta então mostrar que o polinômio

$$G(\mathsf{x}) = \gamma_m\mathsf{x}^m + \cdots + \gamma_1\mathsf{x} + \gamma_0 \in A[\mathsf{x}]$$

é primitivo.

Suponhamos por absurdo que existe um ideal primo $\mathcal{P} = (\pi)$ de A, onde $\pi \in A$ é irredutível, tal que

$$\gamma_i \in \mathcal{P}$$

para todo $0 \leq i \leq m$. Então para cada $0 \leq i \leq m$ existe $a_i \in A$ tal que

$$\gamma_i = a_i \pi \ .$$

Agora para cada $0 \leq i \leq m$ temos

$$\alpha' \gamma_i = \gamma_i'$$

donde segue que

$$\alpha' \pi a_i = \gamma_i' \ .$$

Desse modo, $(\alpha'\pi)/\gamma_i'$ para todo $0 \leq i \leq m$ e $(\alpha'\pi)$ não divide α', o que contraria 1.4.2.

Logo não existe ideal primo de A que contém γ_i para todo $0 \leq i \leq m$ e portanto o polinômio $G(\mathrm{x})$ é primitivo.

O fato de β ser divisível por β_i para todo $0 \leq i \leq m$ segue diretamente de que para todo $0 \leq i \leq m$,

$$\beta \alpha_i = \alpha \gamma_i \beta_i \ . \qquad \blacksquare$$

Observação : Note que se existe $s \in \mathrm{N}$, com $0 \leq s \leq m$, tal que α_s é unidade de A, então α ainda é unidade de A. De fato, temos que

$$\beta \alpha_s = \alpha \gamma_s \beta_s \equiv 0 \ (\alpha)$$

donde $\beta \equiv 0 \ (\alpha)$; mas $\mathrm{mdc}(\alpha, \beta) = 1$, logo α é unidade.

Ainda considerando K um corpo numérico principal, sejam

$$(\pi_1), (\pi_2), (\pi_3), \cdots$$

onde $\pi_i \in A$ é irredutível para todo $i \in \mathbf{N}$, todos os ideais primos de A, colocados em ordem crescente das normas. Sejam também

$$N_1, N_2, N_3, \cdots$$

suas respectivas normas. Dado $m \in \mathbf{N}$, considere para cada $i \in \mathbf{N}$

$$a_i = \left[\frac{m}{N_i}\right] + \left[\frac{m}{N_i^2}\right] + \left[\frac{m}{N_i^3}\right] + \cdots \in \mathbf{N} ,$$

e escolha $l \in \mathbf{N}$ tal que

$$N_1 \leq N_2 \leq \cdots \leq N_l \leq m < N_{l+1} .$$

Então temos o seguinte teorema:

Teorema 1.4.3: Nas condições acima, se $\{\mu_n\}_{n\in\mathbf{N}}$ é a seqüência definida na demonstração do teorema 1.2.6, então

$$\mu_0\mu_1 \cdots \mu_m = \epsilon.\pi_1^{a_1}.\pi_2^{a_2} \cdots \pi_l^{a_l}$$

onde $\epsilon \in A$ é uma unidade.

Demonstração:

Seja $\{F_n\}_{n\in\mathbf{N}}$ uma base regular de polinômios a valores inteiros sobre K. Como vimos no parágrafo 2, dado $m \in \mathbf{N}$ podemos tomar o polinômio de grau m da base na forma

$$F_m(\mathsf{x}) = \frac{1}{\mu_0\mu_1 \cdots \mu_m}\mathsf{x}^m + \cdots$$

Pela proposição 1.4.1 podemos escrever esse polinômio na forma

$$F_m(\mathsf{x}) = \frac{\gamma_m\mathsf{x}^m + \cdots + \gamma_1\mathsf{x} + \gamma_0}{\beta}$$

onde $G(\mathsf{x}) = \gamma_m \mathsf{x}^m + \cdots + \gamma_1 \mathsf{x} + \gamma_0 \in A[\mathsf{x}]$ é um polinômio primitivo e β é múltiplo de $\mu_0\mu_1\cdots\mu_m$. Assim, como $F_m(\mathsf{x})$ é a valores inteiros sobre K, temos que a congruência

$$G(\mathsf{x}) \equiv 0\ (\beta)$$

é sempre satisfeita, donde

$$G(\mathsf{x}) \equiv 0\ (\mu_0\mu_1\cdots\mu_m)$$

também é sempre satisfeita. Mas $G(\mathsf{x})$ é inteiro sobre K, logo pelo teorema 1.3.11 temos que

$$\mu_0\mu_1\cdots\mu_m \quad \text{divide} \quad \pi_1^{a_1}.\pi_2^{a_2}\cdots\pi_l^{a_l}\ . \tag{1.4.4}$$

Por outro lado, como foi feito no parágrafo 3, podemos construir um polinômio

$$H(\mathsf{x}) = (\mathsf{x}-\alpha_0)(\mathsf{x}-\alpha_1)\cdots(\mathsf{x}-\alpha_{m-1})$$

inteiro, mônico e de grau m tal que a congruência

$$H(\mathsf{x}) \equiv 0\ (\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_l^{a_l})$$

é sempre satisfeita, ou seja, tal que o polinômio

$$\frac{H(\mathsf{x})}{\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_l^{a_l}}$$

é a valores inteiros sobre K. Desse modo podemos escrever

$$\frac{H(\mathsf{x})}{\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_l^{a_l}} = \beta_m F_m(\mathsf{x}) + \cdots + \beta_0 F_0(\mathsf{x})$$

onde $\beta_i \in A$ para todo $0 \leq i \leq m$, e comparando os coeficientes líderes temos

$$\frac{1}{\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_l^{a_l}} = \frac{\beta_m}{\mu_0\mu_1\cdots\mu_m}\ .$$

Ou seja, também temos que

$$\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_l^{a_l} \quad \text{divide} \quad \mu_0\mu_1\cdots\mu_m \ . \tag{1.4.5}$$

Assim, por 1.4.4 e 1.4.5 segue que

$$\mu_0\mu_1\cdots\mu_m = \epsilon\pi_1^{a_1}\pi_2^{a_2}\cdots\pi_l^{a_l}$$

onde ϵ é unidade de A. ■

Vimos no parágrafo 2 que se K possui uma base regular de polinômios a valores inteiros sobre K, então podemos tomar como polinômio da base de grau m um polinômio em $Int(A)$ de grau m cujo coeficiente líder é

$$\frac{1}{\mu_0\mu_1\cdots\mu_m} \ .$$

Agora, pelo que foi apresentado nesse parágrafo, concluímos que se K é um corpo numérico principal então podemos tomar como polinômio de grau m da base um polinômio em $Int(A)$ da forma

$$\frac{H(\mathsf{x})}{\mu_0\mu_1\cdots\mu_m}$$

onde $H(\mathsf{x})$ é inteiro sobre K, tem grau m e é mônico.

Daí segue ainda que um polinômio $P(\mathsf{x})$ em $Int(A)$ de grau m, devido à sua representação através dos polinômios da base, pode ser escrito na forma

$$P(\mathsf{x}) = \frac{G(\mathsf{x})}{\beta}$$

onde $G(\mathsf{x})$ é um polinômio inteiro sobre K e $\beta \in A$ é um divisor de $\mu_0\mu_1\cdots\mu_m$.

1.5 Corpos Quadráticos

Vamos considerar agora K um corpo quadrático. Nesse parágrafo apresentamos o último teorema desse capítulo, onde damos uma condição necessária e suficiente para que o corpo quadrático K possua uma base regular de polinômios a valores inteiros.

Teorema 1.5.1: Seja K um corpo quadrático. K possui uma base regular de polinômios a valores inteiros se e somente se todos os ideais primos de A que provêm de números inteiros ramificados são principais.

Demonstração:

Seja d o discriminante absoluto de K. Suponhamos inicialmente que todos os ideais primos de A que contêm d são principais. Assim, todo ideal primo de A que não é principal não contém d, e nesse caso esses ideais são da forma $\mathcal{P}\overline{\mathcal{P}}$, onde $\mathcal{P}$ é um ideal primo de K e $\overline{\mathcal{P}}$ é o seu ideal conjugado.

Dado $m \in \mathrm{N}$, tome a decomposição de $m!$ em fatores primos

$$m! = p_1^{a_1} \cdots p_k^{a_k} . p_{k+1}^{a_{k+1}} \cdots p_l^{a_l}$$

onde $a_i, p_i \in \mathrm{N}$ e p_i é primo para todo $1 \leq i \leq l$. Passando ao anel de inteiros de K, temos então que

$$(m!) = (p_1)^{a_1} \cdots (p_k)^{a_k} (\mathcal{P}_{k+1}\overline{\mathcal{P}}_{k+1})^{a_{k+1}} \cdots (\mathcal{P}_l\overline{\mathcal{P}}_l)^{a_l}$$

onde $(p_1), \cdots, (p_k)$ são todos os ideais primos principais de A que contêm $m!$, e $\mathcal{P}_{k+1}, \overline{\mathcal{P}}_{k+1}, \cdots, \mathcal{P}_l, \overline{\mathcal{P}}_l$ são os ideais primos de A que contêm $m!$ e que não são principais. Agora como vimos no parágrafo 3, existe um polinômio interio sobre K, $P(\mathrm{x})$, mônico e de grau m, tal que a congruência

$$P(\mathrm{x}) \equiv 0 \ (\mathcal{P}_{k+1}^{a_{k+1}} \overline{\mathcal{P}}_{k+1}^{a_{k+1}} \cdots \mathcal{P}_l^{a_l} \overline{\mathcal{P}}_l^{a_l})$$

é sempre satisfeita. Daí segue que o polinômio

$$\frac{P(\mathrm{x})}{p_{k+1}^{a_{k+1}} \cdots p_l^{a_l}} = \frac{p_1^{a_1} \cdots p_k^{a_k}}{m!}\mathrm{x}^m + \cdots$$

é a valores inteiros sobre K, e portanto

$$p_1^{a_1} \cdots p_k^{a_k} \in \mathcal{A}_m$$

onde $\mathcal{A}_m$ é o ideal de A definido no parágrafo 2. Mas então temos

$$(p_1^{a_1} \cdots p_k^{a_k}) \subset \mathcal{A}_m$$

ou seja

$$(p_1)^{a_1} \cdots (p_k)^{a_k} \subset \mathcal{A}_m = Q_1^{b_1} \cdots Q_r^{b_r}$$

onde Q_i é ideal primo de A e $b_i \in \mathrm{N}$ para todo $1 \leq i \leq r$. Segue então que

$$\mathcal{A}_m = (p_1)^{c_1} \cdots (p_k)^{c_k} = (p_1^{c_1} \cdots p_k^{c_k})$$

onde $c_i \in \mathrm{N}$ e $c_i \leq a_i$ para todo $1 \leq i \leq k$, e portanto $\mathcal{A}_m$ é um ideal principal.

Com isso verificamos que para todo $m \in \mathrm{N}$, o ideal $\mathcal{A}_m$ é principal. Logo pelo teorema 1.2.4 concluímos que K possui uma base regular de polinômios a valores inteiros sobre K.

Reciprocamente, suponhamos agora que K possui uma base regular de polinômios a valores inteiros. Tome $p \in \mathrm{N}$ o menor número primo que divide d e tal que (p) em A é o produto de ideais não principais. Então, como p/d, temos

$$(p) = \mathcal{P}^2$$

onde $\mathcal{P}$ é um ideal primo não principal de A. Escrevendo ainda

$$(p!) = \mathcal{P}^2(\pi_1)^{a_1} \cdots (\pi_r)^{a_r}(\mathcal{P}_1\overline{\mathcal{P}}_1)^{b_1} \cdots (\mathcal{P}_l\overline{\mathcal{P}}_l)^{b_l}$$

onde $(\pi_1), \cdots, (\pi_r)$ são ideais primos principais de A e $\mathcal{P}_1, \overline{\mathcal{P}}_1, \cdots, \mathcal{P}_l, \overline{\mathcal{P}}_l$ são ideais primos de A que não são principais (observe que os ideais primos de A que não são principais e têm norma menor que p, e portanto não divide d, podem ser decompostos em um par de ideais primos conjugados). De acordo com o que foi feito no parágrafo 2, existe um polinômio $P(\mathsf{x})$ mônico, inteiro sobre K e de grau p tal que a congruência

$$P(\mathsf{x}) \equiv 0 \ (\mathcal{P}\, \mathcal{P}_1^{b_1}\, \overline{\mathcal{P}}_1^{b_1} \cdots \mathcal{P}_l^{b_l}\, \overline{\mathcal{P}}_l^{b_l})$$

é sempre satisfeita. Então se

$$\mathcal{P} = (\alpha, \beta)$$

onde $\alpha, \beta \in A$, temos que os polinômios

$$\frac{\alpha\, P(\mathsf{x})}{pN_1^{b_1} \cdots N_l^{b_l}} = \frac{\alpha \pi_1^{a_1} \cdots \pi_r^{a_r}}{p!} \mathsf{x}^p + \cdots$$

e

$$\frac{\beta\, P(\mathsf{x})}{pN_1^{b_1} \cdots N_l^{b_l}} = \frac{\beta \pi_1^{a_1} \cdots \pi_r^{a_r}}{p!} \mathsf{x}^p + \cdots$$

onde $N_i = N(\mathcal{P}_i)$ para todo $1 \leq i \leq l$, são polinômios a valores inteiros sobre K. Daí segue que

$$\mathcal{P}(\pi_1^{a_1} \cdots \pi_r^{a_r}) \subset \mathcal{A}_p$$

ou seja,

$$\mathcal{P}(\pi_1)^{a_1} \cdots (\pi_r)^{a_r} \subset \mathcal{A}_p \ .$$

Vamos então dividir em dois casos: se $\mathcal{A}_p$ não é múltiplo de $\mathcal{P}$ ou se $\mathcal{A}_p$ é múltiplo de $\mathcal{P}$.

Se $\mathcal{A}_p$ não é múltiplo de $\mathcal{P}$ então $(p-1)! \in \mathcal{A}_p$. Logo existe um polinômio em $Int(A)$ cujo coeficiente líder é

$$\frac{(p-1)!}{p!} \ .$$

Mas todo polinômio em $Int(A)$ de grau p pode ser escrito como o quociente de um polinômio inteiro sobre K de grau p por $p!$. logo devemos ter um polinômio em $Int(A)$ da forma

$$\frac{(p-1)!x^p + \alpha_{p-1}x^{p-1} + \cdots + \alpha_1 x + \alpha_0}{p!}$$

onde $\alpha_i \in A$ para $0 \leq i \leq p-1$. Desse modo a congruência

$$(p-1)!x^p + \alpha_{p-1}x^{p-1} + \cdots + \alpha_1 x + \alpha_0 \equiv 0\ (\mathcal{P}^2)$$

é sempre satisfeita. Mas isso contraria o teorema 1.3.2. uma vez que $(p-1)! \notin \mathcal{P}$ e

$$\left[\frac{p}{N(\mathcal{P})}\right] + \left[\frac{p}{N(\mathcal{P})^2}\right] + \cdots = \frac{p}{N(\mathcal{P})} = 1 < 2\ .$$

Resta então o caso em que $\mathcal{A}_p$ é múltiplo de $\mathcal{P}$. Nesse caso,

$$\mathcal{A}_p = \mathcal{P}.I$$

onde I é um divisor de $(\pi_1^{a_1} \cdots \pi_r^{a_r})$, logo é um ideal principal. Dessa forma, como $\mathcal{P}$ não é um ideal principal, temos que $\mathcal{A}_p$ não é principal, o que contraria o teorema 1.2.4.

Assim, em ambos os casos, chegamos a uma contradição , logo os ideais primos que contêm d são ideais principais. ■

Capítulo 2

O Anel $Int(A)$

Introdução

Neste capítulo vamos considerar A um domínio qualquer e K seu corpo de frações. Vamos estudar um subconjunto do anel de polinômios $K[\mathsf{x}]$, que denotaremos por $\mathcal{I}(A)$ e que é dado por

$$\mathcal{I}(A) = \{P(\mathsf{x}) \in K[\mathsf{x}] \, ; P(A) \subset A\} \, .$$

Claramente $\mathcal{I}(A)$ é um anel. Mais que isso, impondo algumas restrições ao domínio A, mostraremos que $\mathcal{I}(A)$ é um domínio de Prüfer.

Além disso, generalizando um resultado provado por T. Skolem para $\mathcal{I}(\mathbf{Z})$, mostraremos que sob essas mesmas imposições feitas ao domínio A, o domínio de Prüfer $\mathcal{I}(A)$ possui a seguinte propriedade:

Se I e J são ideais finitamente gerados de $\mathcal{I}(A)$ tais que $I(a) = J(a)$ para todo $a \in A$, então $I = J$.

É importante notar que se K é um corpo numérico e A é o anel de inteiros de K então $\mathcal{I}(A) = Int(A)$. Nesse caso em particular as condições impostas sobre A são satisfeitas e portanto todos os resultados aqui apresentados são válidos para o anel $Int(A)$ estudado no primeiro capítulo.

2.1 Definições e Motivação

Neste capítulo estaremos sempre considerando A um domínio e K o corpo de frações de A. Neste parágrafo daremos algumas definições e enunciaremos um teorema provado por T. Skolem em [16] que é o ponto de partida para o estudo realizado neste capítulo.

Definição 2.1.1: Dado um domínio A com corpo de frações K, definimos

$$\mathcal{I}(A) = \{f(\mathsf{x}) \in K[\mathsf{x}] \; ; f(A) \subset A\}$$

o anel de polinômios *a valores inteiros sobre* K.

É claro que $\mathcal{I}(A)$ é anel, uma vez que A é anel.

Observação : Note que se K é um corpo numérico e A é o anel de inteiros de K, então $\mathcal{I}(A)$ nada mais é que o anel de polinômios a valores inteiros sobre K, $Int(A)$. Nesse caso podemos usar qualquer uma dessas notações .

Teorema 2.1.2 (Teorema de Skolem): Seja $\mathbf{Z}$ o anel dos números inteiros. Se I é um ideal finitamente gerado em $\mathcal{I}(\mathbf{Z})$ tal que

$$I(a) = \{f(a) \; ; f(\mathsf{x}) \in I\} = \mathbf{Z}$$

para todo $a \in \mathbf{Z}$, então $I = \mathcal{I}(A)$.

Surge então o interesse em generalizar esse resultado. Mas como podemos ver no exemplo 3.5 do capítulo 3; isso não é possível para um domínio A em geral. Porém, em [3], Demétrios Brizolis obteve uma generalização desse teorema impondo algumas restrições ao anel A, que apresentaremos no próximo parágrafo.

A fim de simplificar a linguagem utilizada, temos as seguintes definições:

Definição 2.1.3: Sejam A um domínio com corpo de frações K e R um

subanel de $\mathcal{I}(A)$ que contém $A[\mathsf{x}]$. Dizemos que R é um *anel de Skolem* se para todo ideal I finitamente gerado de R tal que

$$I(a) = \{f(a)\ ; f(\mathsf{x}) \in I\} = A$$

para todo $a \in A$, temos $I = R$.

Observação : $I(a) \subset A$ é ideal de A para todo $a \in A$.

Definição 2.1.4: Seja A um domínio. Dizemos que A é um *D^*-domínio* se satisfaz as condições:

1. A é um domínio de Dedekind;
2. $\mathrm{ch}(K) = 0$;
3. o anel quociente $\frac{A}{\mathcal{P}}$ é finito para todo ideal primo $\mathcal{P}$ de A;
4. se $f(\mathsf{x})$ é um polinômio não constante em $A[\mathsf{x}]$, então a equação

$$f(\mathsf{x}) \equiv 0\ (\mathcal{P})$$

possui solução em A para infinitos ideais primos $\mathcal{P}$ de A.

Observação : Note que a condição (iv) elimina a possibilidade de A ser um corpo.

2.2 A Generalização do Teorema de Skolem

Considere A um domínio com corpo de frações K. Neste parágrafo vamos apresentar a generalização do teorema de Skolem, visto no parágrafo 1, e sua demonstração . Observe que foi necessário impor restrições sobre o domínio

A.

Teorema 2.2.1 (Teorema de Skolem Generalizado): Seja A um D^*-domínio. Então $\mathcal{I}(A)$ é um anel de Skolem.

Para demonstrar este teorema precisamos de um resultado preliminar.

Lema 2.2.2: Seja A um domínio de Dedekind tal que para todo polinômio não constante $f(\mathsf{x})$ em $A[\mathsf{x}]$ existem infinitos ideais primos $\mathcal{P}'$ de A para os quais a equação

$$f(\mathsf{x}) \equiv 0 \ (\mathcal{P}')$$

tem solução em A, e com corpo de frações K tal que $ch(K) = 0$. Sejam ainda L uma extensão finita de K e B o fecho integral de A em L. Então existem infinitos ideais primos $\mathcal{P}$ de B tais que

$$\left[\frac{B}{\mathcal{P}} : \frac{A}{\mathcal{P} \cap A}\right] = 1$$

Demonstração:

Como a extensão $L|K$ é finita e $ch(K) = 0$, existe $\alpha' \in L$ tal que $K(\alpha') = L$. Mas α' pode ser escrito na forma

$$\alpha' = \frac{\alpha}{a}$$

onde $\alpha \in B$ e $a \in A$. Logo podemos tomar $L = K(\alpha)$, onde $\alpha \in B$.

Como α é inteiro sobre A, existe um polinômio $f(\mathsf{x})$ em $A[\mathsf{x}]$, mônico e com grau mínimo tal que $f(\alpha) = 0$. Então por hipótese existem infinitos ideais primos $\mathcal{P}'$ de A tais que

$$f(\mathsf{x}) \equiv 0 \ (\mathcal{P}')$$

tem solução em A.

Por outro lado, pelo teorema A.2.6, temos que $B_{\mathcal{P}} = A_{\mathcal{P}}[\alpha]$ exceto para um número finito de ideais primos $\mathcal{P}$ de A.

Desse modo existem infinitos ideais primos $\mathcal{P}'$ de A que satisfazem ambas as condições:

1. $f(\mathsf{x}) \equiv 0\ (\mathcal{P}')$ tem solução em A;

2. $B_{\mathcal{P}'} = A_{\mathcal{P}'}[\alpha]$.

Tome então $\mathcal{P}'$ um tal ideal primo de A e escolha $a \in A$ tal que $f(a) \equiv 0\ (\mathcal{P}')$. Passando ao quociente $\frac{A}{\mathcal{P}'}$ temos que

$$\overline{f}(\mathsf{x}) = (\mathsf{x} - \overline{a})^e . \overline{G}(\mathsf{x})$$

onde $\overline{a} \in \frac{A}{\mathcal{P}'}$ e $G(a) \not\equiv 0\ (\mathcal{P}')$.

Agora, se $\mathcal{M}_{\mathcal{P}'}$ é o ideal maximal de $A_{\mathcal{P}'}$, então $\mathcal{M}_{\mathcal{P}'} \cap A = \mathcal{P}'$, e como temos $f(\mathsf{x}) \in A[\mathsf{x}] \subset A_{\mathcal{P}'}[\mathsf{x}]$, segue que

$$f(a) \equiv 0\ (\mathcal{M}_{\mathcal{P}'})$$

Logo passando ao quociente $\frac{A_{\mathcal{P}'}}{\mathcal{M}_{\mathcal{P}'}}$, podemos escrever

$$\overline{\overline{f}}(\mathsf{x}) = (\mathsf{x} - \overline{\overline{a}})^e . \overline{\overline{Q}}(\mathsf{x})$$

onde $\overline{\overline{a}} \in \frac{A_{\mathcal{P}'}}{\mathcal{M}_{\mathcal{P}'}}$ e $Q(a) \not\equiv 0\ (\mathcal{M}_{\mathcal{P}'})$.

Assim, tomando no teorema A.1.12 $A = A_{\mathcal{P}'}$, $B = B_{\mathcal{P}'}$ e $\mathcal{P} = \mathcal{M}_{\mathcal{P}'}$, temos que

$$\mathcal{M}_{\mathcal{P}'} B_{\mathcal{P}'} = \mathcal{P}_1^{e_1} . \mathcal{P}_2^{e_2} \cdots \mathcal{P}_r^{e_r}$$

onde

$$\mathcal{P}_1 = \mathcal{M}_{\mathcal{P}'} B_{\mathcal{P}'} + (\alpha - a) B_{\mathcal{P}'}$$

é ideal primo de $B_{\mathcal{P}'}$ tal que $\mathcal{P}_1 \cap A_{\mathcal{P}'} = \mathcal{M}_{\mathcal{P}'}$ e ainda que

$$\left[\frac{B_{\mathcal{P}'}}{\mathcal{P}_1} : \frac{A_{\mathcal{P}'}}{\mathcal{M}_{\mathcal{P}'}}\right] = 1 .$$

Assim, como

$$\frac{A_{\mathcal{P}'}}{\mathcal{M}_{\mathcal{P}'}} \simeq \frac{A}{\mathcal{M}_{\mathcal{P}'} \cap A} = \frac{A}{\mathcal{P}'}$$

e

$$\frac{B_{\mathcal{P}'}}{\mathcal{P}_1} \simeq \frac{B}{\mathcal{P}_1 \cap B}$$

temos que

$$\left[\frac{B}{\mathcal{P}_1 \cap B} : \frac{A}{\mathcal{P}'}\right] = 1 .$$

Então se tomamos $\mathcal{P} = \mathcal{P}_1 \cap B$ temos que $\mathcal{P}$ é ideal primo de B e

$$\begin{aligned} \mathcal{P} \cap A &= (\mathcal{P}_1 \cap B) \cap A = \mathcal{P}_1 \cap A = \mathcal{P}_1 \cap A_{\mathcal{P}'} \cap A = \\ &= \mathcal{M}_{\mathcal{P}'} \cap A = \mathcal{P}' . \end{aligned}$$

Logo temos demonstrado o lema. ■

Estamos prontos agora para demonstrar o teorema.

Demonstração do Teorema 2.2.1:

Seja $I = (f_1(\mathsf{x}), \cdots, f_n(\mathsf{x}))$ um ideal finitamente gerado de $\mathcal{I}(A)$ tal que

$$I(a) = (f_1(a), \cdots, f_n(a)) = A$$

para todo $a \in A$. Vamos mostrar que $I = \mathcal{I}(A)$, e portanto, que $\mathcal{I}(A)$ é um anel de Skolem.

Primeiramente vamos mostrar que $f_1(\mathsf{x}), \cdots, f_n(\mathsf{x})$ não possuem raiz comum em qualquer extensão de K. De fato, suponhamos que exista α tal que

$$f_1(\alpha) = \cdots = f_n(\alpha) = 0$$

e tome então $L = K(\alpha)$. Então existe $c \in A$ tal que $c\alpha$ é inteiro sobre A em L, uma vez que α é algébrico sobre K. Também, como os coeficientes dos f_i's estão em K, podemos escrevê-los na forma

$$\frac{e_{ij}}{d}$$

onde $e_{ij} \in A$ para todo $1 \leq i \leq n$ e todo $0 \leq j \leq \partial f_i$ e $d \in A$. Agora como A é D^*-domínio, temos que $ch(K) = 0$; logo pelo lema 2.2.2 existem infinitos ideais primos $\mathcal{P}$ no fecho integral de A em L, que chamaremos B, tais que

$$\left[\frac{B}{\mathcal{P}} : \frac{A}{\mathcal{P} \cap A}\right] = 1 \ . \tag{2.2.3}$$

Podemos então tomar $\mathcal{P}$ um desses ideais, tal que

$$c \not\equiv 0 \ (\mathcal{P}) \quad \text{e} \quad d \not\equiv 0 \ (\mathcal{P}) \ ,$$

pois B é Dedekind e portanto o conjunto dos ideais primos de B que contêm c e d é finito. Como $\mathcal{P}$ é ideal primo de B, $\mathcal{P} \cap A$ deve ser ainda um ideal primo de A. Segue então por hipótese que $\frac{A}{\mathcal{P} \cap A}$ deve ser finito; suponhamos $\#\left(\frac{A}{\mathcal{P} \cap A}\right) = N$ e seja

$$S = \{r_1, \cdots, r_N\} \subset A$$

um sistema completo de resíduos em A módulo $\mathcal{P} \cap A$. Agora por 2.2.3 e como $S \subset A \subset B$, temos que S é também um sistema completo de resíduos em B módulo $\mathcal{P}$. Desse modo,

$$c\alpha \equiv r_{j_0} \ (\mathcal{P})$$

para algum $1 \leq j_0 \leq N$. Mas como $c \in A$, $c \notin \mathcal{P}$ e $\frac{A}{\mathcal{P} \cap A}$ é corpo, temos que c é inversível em $\frac{A}{\mathcal{P} \cap A}$, logo existe j, com $1 \leq j \leq N$. tal que

$$\alpha \equiv r_j \ (\mathcal{P}) \ .$$

Assim, como $d f_i(\mathsf{x}) \in A[\mathsf{x}]$ para todo $1 \leq i \leq n$, temos que

$$d f_i(\alpha) \equiv d f_i(r_j) \ (\mathcal{P})$$

para todo $1 \leq i \leq n$. Mas $d \notin \mathcal{P}$, logo é inversível em $\frac{A}{\mathcal{P} \cap A}$, e daí segue que

$$0 = f_i(\alpha) \equiv f_i(r_j) \ (\mathcal{P})$$

para todo $1 \leq i \leq n$. Então como $f_i(\mathsf{x}) \in \mathcal{I}(A)$ e $r_j \in A$. temos que

$$f_i(r_j) \equiv 0 \ (\mathcal{P} \cap A)$$

para todo $1 \leq i \leq n$. Mas isso é uma contradição , pois $r_j \in A$ e no entanto

$$(f_1(r_j), \cdots, f_n(r_j)) \subset \mathcal{P} \cap A \subset A \quad \text{e} \quad \mathcal{P} \cap A \neq A \ .$$

Portanto $f_1(\mathsf{x}), \cdots, f_n(\mathsf{x})$ não possuem raiz comum.

Com isso provado, temos então que $f_1(\mathsf{x}), \cdots, f_n(\mathsf{x})$ são relativamente primos como elementos de $K[\mathsf{x}]$, isto é,

$$\text{mdc}(f_1(\mathsf{x}), \cdots, f_n(\mathsf{x})) = 1 \ .$$

Como $K[\mathsf{x}]$ é Euclideano, existem polinômios $g_1(\mathsf{x}), \cdots, g_n(\mathsf{x}) \in K[\mathsf{x}]$ tais que

$$f_1(\mathsf{x})\, g_1(\mathsf{x}) + \cdots + f_n(\mathsf{x})\, g_n(\mathsf{x}) = 1 \ .$$

Eliminando então os denominadores dos coeficientes de cada g_j, podemos escrever

$$f_1(\mathsf{x})\, h_1(\mathsf{x}) + \cdots + f_n(\mathsf{x})\, h_n(\mathsf{x}) = M \ .$$

onde $M \in A$ e $h_j(\mathsf{x}) \in A[\mathsf{x}]$ para $1 \leq j \leq n$.

Considere agora em A o ideal gerado por M, $I = (M)$. Como A é anel de Dedekind, temos

$$I = (M) = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}$$

onde cada $\mathcal{P}_s$, $1 \leq s \leq k$, é ideal primo de A, $\mathcal{P}_i \neq \mathcal{P}_j$ se $i \neq j$, e cada e_s, $1 \leq s \leq k$, é um número inteiro. Também, se para cada s, $1 \leq s \leq k$, o corpo $\frac{A}{\mathcal{P}_s}$ tem λ_s elementos, então se $b \in A$ é tal que $b \not\equiv 0\ (\mathcal{P}_s)$ temos

$$b^{\lambda_s - 1} \equiv 1\ (\mathcal{P}_s)\ . \tag{2.2.4}$$

Agora defina para cada s, $1 \leq s \leq k$, os seguintes polinômios em $\mathcal{I}(A)$:

$$\begin{aligned}
&A_{s1}(\mathsf{x}) = 1\ , \\
&A_{s2}(\mathsf{x}) = f_2^{\lambda_s - 1}(\mathsf{x}) - f_1^{\lambda_s - 1}(\mathsf{x})\ , \\
&\vdots \\
&A_{sn}(\mathsf{x}) = (f_n^{\lambda_s - 1}(\mathsf{x}) - f_1^{\lambda_s - 1}(\mathsf{x})) \cdots (f_n^{\lambda_s - 1}(\mathsf{x}) - f_{n-1}^{\lambda_s - 1}(\mathsf{x}))
\end{aligned}$$

e seja, para $1 \leq s \leq k$,

$$A_s(\mathsf{x}) = A_{s1}(\mathsf{x}) f_1(\mathsf{x}) + \cdots + A_{sn}(\mathsf{x}) f_n(\mathsf{x})$$

que ainda é um polinômio em $\mathcal{I}(A)$.

Afirmamos que para todo $a \in A$,

$$A_s(a) \not\equiv 0\ (\mathcal{P}_s)$$

De fato:
Se $a \in A$ então por hipótese,

$$(f_1(a), \cdots, f_n(a)) = (1)\ .$$

Logo existe um menor inteiro j, $1 \leq j \leq n$, tal que $f_j(a) \not\equiv 0\ (\mathcal{P}_s)$, pois caso contrário teríamos $(f_1(a), \cdots, f_n(a)) \subset \mathcal{P}_s \subset A$ e $\mathcal{P}_s \neq A$.

Assim, se l é um inteiro tal que $1 \leq l \leq j$ então

$$f_l(a) \equiv 0\ (\mathcal{P}_s)\ . \tag{2.2.5}$$

e daí

$$\begin{aligned} A_{sj}(a) &= (f_j^{\lambda_s-1}(a) - f_1^{\lambda_s-1}(a)) \cdots (f_j^{\lambda_s-1}(a) - f_{j-1}^{\lambda_s-1}(a)) \equiv \\ &\equiv (1-0)(1-0)\cdots(1-0)\ (\mathcal{P}_s)\ , \quad \text{por (2.2.4) e (2.2.5)} \\ &\equiv 1\ (\mathcal{P}_s)\ , \end{aligned}$$

ou seja, $A_{sj}(a) \equiv 1\ (\mathcal{P}_s)$.

Agora, se t é um inteiro tal que $j \leq t \leq n$ então ou $f_t(a) \equiv 0\ (\mathcal{P}_s)$ ou $f_t(a) \not\equiv 0\ (\mathcal{P}_s)$. Vamos estudar ambos os casos.

1) $f_t(a) \equiv 0\ (\mathcal{P}_s)$

Nesse caso, $A_{st}(a)$ contém $(f_t^{\lambda_s-1}(a) - f_l^{\lambda_s-1}(a))$ como fator, onde $1 \leq l < j$; ou seja,

$$\begin{aligned} A_{st}(a) &= (f_t^{\lambda_s-1}(a) - f_1^{\lambda_s-1}(a)) \cdots (f_t^{\lambda_s-1}(a) - f_l^{\lambda_s-1}(a)) \cdots \\ &\quad (f_t^{\lambda_s-1}(a) - f_{t-1}^{\lambda_s-1}(a))\ . \end{aligned}$$

Assim, pela escolha de j e como $f_t^{\lambda_i-1}(a) \equiv 0\ (\mathcal{P}_s)$ devemos ter

$$(f_t^{\lambda_s-1}(a) - f_l^{\lambda_s-1}(a)) \equiv (0-0)\ (\mathcal{P}_s)$$

ou seja,

$$(f_t^{\lambda_s-1}(a) - f_l^{\lambda_s-1}(a)) \equiv 0\ (\mathcal{P}_s)$$

e daí

$$A_{st}(a) \equiv 0\ (\mathcal{P}_s)\ .$$

2) $f_t(a) \not\equiv 0\ (\mathcal{P}_s)$

Nesse caso, $A_{st}(a)$ contém $(f_t^{\lambda_s-1}(a) - f_j^{\lambda_s-1}(a))$ como fator e então , desde que

$$(f_t^{\lambda_s-1}(a) - f_j^{\lambda_s-1}(a)) \equiv (1-1)\ (\mathcal{P}_s) \quad \text{(por 2.2.3)}$$

ou seja,

$$(f_t^{\lambda_s-1}(a) - f_j^{\lambda_s-1}(a)) \equiv 0\ (\mathcal{P}_s)$$

temos ainda que

$$A_{st}(a) \equiv 0\ (\mathcal{P}_s)\ .$$

Desse modo,

$$\begin{aligned} A_s(a) &= A_{s1}(a)f_1(a) + \cdots + A_{sj-1}(a)f_{j-1}(a) + \\ &+ A_{sj}(a)f_j(a) + A_{sj+1}(a)f_{j+1}(a) + \cdots + A_{sn}(a)f_n(a) \end{aligned}$$

donde

$$A_s(a) \equiv 0 + \cdots + 0 + 1.f_j(a) + 0 + \cdots + 0\ (\mathcal{P}_s)$$

e portanto pela escolha de j,

$$A_s(a) \not\equiv 0\ (\mathcal{P}_s)\ ,$$

como havíamos afirmado.

Prosseguindo a demonstração do teorema, usando o conhecido Teorema do Resto Chinês, para cada s, $1 \leq s \leq k$, podemos escolher $\pi_s \in A$ tal que

$$\pi_s \equiv 0\ (\mathcal{P}_s) \quad \text{e} \quad \pi_s \equiv 1\ (\mathcal{P}_i) \quad \text{para} \quad i \neq s\ .$$

Defina então

$$\pi = \pi_1 \cdots \pi_k\ .$$

Assim, se $a \in A$,

$$\frac{\pi}{\pi_i} A_i(a) = \frac{\pi_1 \cdots \pi_s \cdots \pi_k}{\pi_i} A_i(a) \equiv 0\ (\mathcal{P}_s)$$

para $i \neq s$, e

$$\frac{\pi}{\pi_s} A_s(a) \not\equiv 0\ (\mathcal{P}_s)$$

pela afirmação provada anteriormente.

Desse modo, se definimos

$$g(\mathsf{x}) = \frac{\pi}{\pi_1} A_1(\mathsf{x}) + \cdots + \frac{\pi}{\pi_k} A_k(\mathsf{x})$$

então temos que para todo $a \in A$

$$g(a) \not\equiv 0 \ (\mathcal{P}_s) \ , \ \text{para} \ 1 \leq s \leq k$$

e daí

$$g(a) \not\equiv 0 \ (M) \ , \ \text{para todo} \ a \in A \ .$$

Desde que $\frac{A}{\mathcal{P}_s}$ é finito para todo s, $1 \leq s \leq k$, temos que $\frac{A}{\mathcal{P}_s^{e_s}}$ também é finito e portanto $\frac{A}{(M)}$ deve ser finito. Seja T a ordem do grupo das unidades de $\frac{A}{(M)}$. Assim, se $b \in A$ é unidade módulo (M), isto é, $\text{mdc}(b, M) = 1$, então

$$b^T \equiv 1 \ (M) \ .$$

Como $g(\mathsf{x}) \in \mathcal{I}(A)$ pela sua construção e $g(a) \not\equiv 0 \ (\mathcal{P}_s)$ para todo $1 \leq s \leq k$, temos que $g(a)A + (M) = A$, donde segue que $g(a)$ é unidade módulo (M) e daí

$$g(a)^T \equiv 1 \ (M) \quad \text{para todo} \ a \in A \ .$$

Considere agora

$$\hat{g}(\mathsf{x}) = \frac{(g(\mathsf{x})^T - 1)}{M} \ .$$

que é um polinômio em $\mathcal{I}(A)$, pois $g(a)^T - 1 \in (M)$ para todo $a \in A$.

Considerando o polinômio

$$F_j(\mathsf{x}) = \left(\sum_{i=1}^{k} \frac{\pi}{\pi_i} A_{ij}(\mathsf{x}) \right) g^{T-1}(\mathsf{x}) - \hat{g}(\mathsf{x}) \, h_j(\mathsf{x})$$

que pertence a $\mathcal{I}(A)$ para cada $1 \leq j \leq n$, temos finalmente que

$$\sum_{j=1}^{n} F_j(\mathsf{x}) f_j(\mathsf{x}) = 1$$

pois

$$\sum_{j=1}^{n} F_j \, f_j = \sum_{j=1}^{n} \left[\left(\sum_{i=1}^{k} \frac{\pi}{\pi_i} A_{ij} \, f_j \right) g^{T-1} - \hat{g} \, h_j \, f_j \right] =$$

$$= \left[\sum_{i=1}^{k} \frac{\pi}{\pi_i} \underbrace{\left(\sum_{j=1}^{n} A_{ij} f_j\right)}_{A_i}\right] g^{T-1} - \hat{g} \underbrace{\left[\sum_{j=1}^{n} h_j f_j\right]}_{M} =$$

$$= \left[\sum_{i=1}^{k} \frac{\pi}{\pi_i} A_i\right] g^{T-1} - \hat{g}.M =$$

$$= g^T - \hat{g}.M = g^T - g^T + 1 = 1 .$$

Logo $(f_1(\mathsf{x}), \cdots, f_n(\mathsf{x})) = \mathcal{I}(A)$, o que encerra a demonstração do teorema de Skolem generalizado. ■

A partir daí surge uma nova questão : se A é um D^*-domínio e I , J são ideais finitamente gerados em $Int(A)$ tais que $I(a) = J(a)$ para todo $a \in A$, então $I = J$? A resposta a esta pergunta é sim, e este é o resultado principal desse capítulo, que será demonstrado nos próximos parágrafos. Para isso vamos antes mostrar alguns resultados adicionais sobre o anel $\mathcal{I}(A)$, no caso em A é D^*-domínio. Vale notar que o teorema 2.2.1 é um caso particular do que vamos mostrar, onde $J = \mathcal{I}(A)$.

2.3 O Domínio de Prüfer $\mathcal{I}(A)$

Neste parágrafo vamos mostrar que o anel $\mathcal{I}(A)$ é um domínio de Prüfer, quando A é um D^*-domínio. Esse fato nos será muito útil no próximo parágrafo onde provaremos uma outra versão do teorema 2.2.1.

Considere A um domínio de Dedekind e $\mathcal{P}$ um ideal primo de A. Denotaremos por $|\ |_{\mathcal{P}}$ o valor absoluto $\mathcal{P}$-ádico de A com respeito a $\mathcal{P}$, e por $\overline{A}_{\mathcal{P}}$ o completamento $\mathcal{P}$-ádico de A.

Vale a pena observar antes de mais nada que, se $f(\mathsf{x}) \in \mathcal{I}(A)$ então temos, por continuidade da função polinomial determinada por $f(\mathsf{x})$, que $f(\alpha) \in \overline{A}_{\mathcal{P}}$

para todo $\alpha \in \overline{A}_{\mathcal{P}}$.

Teorema 2.3.1 (Caracterização dos ideais maximais de $\mathcal{I}(A)$): Seja A um D^*-domínio. Então todo ideal maximal M de $\mathcal{I}(A)$ é da forma

$$M = M_{\alpha\ ,\mathcal{P}} = \{f(\mathsf{x}) \in \mathcal{I}(A)\ ;\ |f(\alpha)|_{\mathcal{P}} < 1\}$$

onde $\mathcal{P} = M \cap A$ é ideal primo de A, e $\alpha \in \overline{A}_{\mathcal{P}}$.

Antes de demonstrar este teorema, vamos provar um lema auxiliar.

Lema 2.3.2: Seja A um D^*-domínio e $f(\mathsf{x}) \in A[\mathsf{x}]$ não constante. Então existe $a \in A$ e um ideal primo $\mathcal{P}$ de A tal que, reduzindo ao corpo $\frac{A}{\mathcal{P}}$, $\partial\overline{f}(\mathsf{x}) = \partial f(\mathsf{x})$ e $\overline{a}$ é raiz simples de $\overline{f}(\mathsf{x})$.

Demonstração:

Seja α uma raiz de $f(\mathsf{x})$ em algum fecho algébrico de $K = \mathrm{Cfr}(A)$. Sejam ainda $L = K(\alpha)$ e B o fecho integral de A em L. Considere então os seguintes ideais de A:

$$I_1 = c.A\ ,\ \text{ onde } c \text{ é o coeficiente líder de } f(\mathsf{x})\ ,$$

$$I_2 = D_{L/K}\ ,\ \text{onde } D_{L/K} \text{ é o ideal discriminante de } L/K\ ,$$

$$I_3 = \{b \in A[\alpha];\ b.B \subset A[\alpha]\} \cap A\ .$$

Agora desde que A é domínio de Dedekind , existe apenas um número finito de ideais primos de A que contêm I_1, I_2 e I_3. Por outro lado, existem infinitos ideais primos de A tais que a congruência $f(\mathsf{x}) \equiv 0\ (\mathcal{P})$ tem solução, logo é possível escolher um ideal primo $\mathcal{P}$ de A tal que

$$f(\mathsf{x}) \equiv 0\ (\mathcal{P}) \quad \text{e} \quad I_1, I_2, I_3 \not\subseteq \mathcal{P}\ .$$

Desse modo, como $I_1 \not\subseteq \mathcal{P}$, temos que $\partial f(\mathsf{x}) = \partial \overline{f}(\mathsf{x})$. Além disso, como $I_2 \not\subseteq \mathcal{P}$, segue que

$$\mathcal{P}.B = Q_1 \cdots Q_s$$

onde $Q_1, \cdots, Q_s$ são ideais primos de B tais que $Q_i \neq Q_j$ se $i \neq j$. Também temos que

$$B_{\mathcal{P}} = A_{\mathcal{P}}[\xi]$$

pelo teorema A.2.6, uma vez que $I_3 \not\subseteq \mathcal{P}$.

Tomemos agora $a \in A$ tal que

$$f(a) \equiv 0 \ (\mathcal{P}) \ .$$

Então temos, passando ao quociente $\frac{A}{\mathcal{P}}$, que

$$\overline{f}(\mathsf{x}) = (\mathsf{x} - \overline{a})^{e}.\overline{g}(\mathsf{x})$$

onde $g(\mathsf{x}) \in A[\mathsf{x}]$ e $g(a) \not\equiv 0 \ (\mathcal{P})$. e como

$$\mathcal{P}\, B_{\mathcal{P}} = Q_1\, B_{\mathcal{P}} \cdots Q_s\, B_{\mathcal{P}} \ ,$$

segue pelo teorema A.1.12 que

$$e = 1$$

donde concluímos que $\overline{a}$ é raiz simples de $\overline{f}(\mathsf{x})$. ■

Demonstração do Teorema 2.3.1:

Primeiramente vamos mostrar que $M_{\alpha,\mathcal{P}} = \{f(\mathsf{x}) \in \mathcal{I}(A) \ ; |f(\alpha)|_{\mathcal{P}} < 1\}$ é um ideal de $\mathcal{I}(A)$, onde $\mathcal{P}$ é um ideal primo de A e $\alpha \in \overline{A}_{\mathcal{P}}$. De fato, sejam $f(\mathsf{x}) \ , g(\mathsf{x}) \in M_{\alpha,\mathcal{P}}$ e $h(\mathsf{x}) \in \mathcal{I}(A)$. Então

$$|f(\alpha) + g(\alpha)|_{\mathcal{P}} \leq \max\{|f(\alpha)|_{\mathcal{P}} \ , |g(\alpha)|_{\mathcal{P}}\} < 1 \ ,$$

donde $f(\mathsf{x}) + h(\mathsf{x}) \in M_{\alpha,\mathcal{P}}$; também,

$$|h(\alpha)f(\alpha)|_{\mathcal{P}} = |h(\alpha)|_{\mathcal{P}}|f(\alpha)|_{\mathcal{P}} \leq |f(\alpha)|_{\mathcal{P}} < 1$$

Agora, pelo lema 2.3.2, existe $a \in A$ e $\mathcal{P}'$ ideal primo de A tais que, reduzindo ao quociente $\frac{A}{\mathcal{P}'}$,

$$\overline{a} \text{ é raiz simples de } \overline{f}(\mathsf{x}) \quad \text{e}$$
$$\text{o coeficiente líder de } f(\mathsf{x}) \text{ não pertence a } \mathcal{P}' .$$

Tomando então $K_{\mathcal{P}'}$ o completamento $\mathcal{P}'$-ádico do corpo de frações de A, $V = \overline{A}_{\mathcal{P}'}$ o seu anel de valorização, e $\alpha_1 = a$ segue pelo teorema A.3.16 que existe $\alpha \in \overline{A}_{\mathcal{P}'}$ tal que

$$f(\alpha) = 0 .$$

Daí segue então que

$$(f(\mathsf{x})).K[\mathsf{x}] \cap \mathcal{I}(A) \subset M_{\alpha,\mathcal{P}'} .$$

De fato, se $h(\mathsf{x}).f(\mathsf{x}) \in \mathcal{I}(A)$, onde $h(\mathsf{x}) \in K[\mathsf{x}]$, então temos

$$|h(\alpha).f(\alpha)|_{\mathcal{P}'} = |0|_{\mathcal{P}'} < 1$$

donde segue que $h(\mathsf{x}).f(\mathsf{x}) \in M_{\alpha,\mathcal{P}'}$. Ou seja,

$$M \subset M_{\alpha,\mathcal{P}'} .$$

Observando que $M_{\alpha,\mathcal{P}'} \cap A = \mathcal{P}'$, que é um ideal não nulo de A, vemos que existe $a \in A - \{0\}$ tal que $a \in M_{\alpha,\mathcal{P}'}$. Portanto

$$M \subset M_{\alpha,\mathcal{P}'} \quad \text{e} \quad M \neq M_{\alpha,\mathcal{P}'}$$

uma vez que $M \cap A = (0)$. Mas isso é um absurdo pois M é ideal maximal de $\mathcal{I}(A)$.

Portanto devemos ter

$$\mathcal{P} = M \cap A \neq (0) .$$

Ou seja, $\mathcal{P}$ é ideal primo não nulo de A.

Agora, para cada $f(\mathsf{x}) \in M$ defina

$$M_f = \{\alpha \in \overline{A}_{\mathcal{P}} \; ; |f(\alpha)|_{\mathcal{P}} < 1\}$$

Afirmamos que se $f_1(\mathsf{x}), \cdots, f_n(\mathsf{x}) \in M$ então

$$M_{f_1} \cap \cdots \cap M_{f_n} \neq \phi \; .$$

De fato, tome $\pi \in \mathcal{P}$ tal que $\pi \notin \mathcal{P}^2$. Então pelo teorema A.1.13, existe $\gamma \in A$ tal que

$$\mathcal{P} = (\pi, \gamma)$$

em A. Assim temos que

$$(f_1(\mathsf{x}), \cdots, f_n(\mathsf{x}), \pi, \gamma) \subseteq M \subset \mathcal{I}(A) \; , \text{ mas } \; M \neq \mathcal{I}(A) \; ,$$

e como $\mathcal{I}(A)$ é um anel de Skolem pelo teorema 2.2.1, existe então $a \in A$ tal que

$$(f_1(a), \cdots, f_n(a), \pi, \gamma) \subset A \; , \text{ estritamente.}$$

Segue daí que

$$\mathcal{P} \subseteq (f_1(a), \cdots, f_n(a), \pi, \gamma) \subset A \text{ estritamente.}$$

Mas A é um anel de Dedekind, donde todo ideal primo não nulo é maximal; logo temos

$$\mathcal{P} = (f_1(a), \cdots, f_n(a), \mathcal{P}) \; .$$

Desse modo temos que, para todo $1 \leq i \leq n$, ocorre

$$|f_i(a)|_{\mathcal{P}} < 1$$

e portanto

$$M_{f_1} \cap \cdots \cap M_{f_n} \neq \phi$$

como havíamos afirmado.

Para cada $f(\mathrm{x}) \in M$, temos que M_f é um subconjunto fechado de $\overline{A}_{\mathcal{P}}$. De fato, se $\beta = \lim_{n\to\infty} \alpha_n$, onde $\alpha_n \in M_f$ para todo $n \in \mathrm{N}$, então

$$f(\beta) = \lim_{n\to\infty} f(\alpha_n)$$

por continuidade. Assim dado $k \in \mathrm{N}$, $k \geq 2$, existe $n_0 \in \mathrm{N}$ tal que para $n \geq n_0$ temos

$$|f(\beta) - f(\alpha_n)|_{\mathcal{P}} < \frac{1}{k}$$

e daí tomando $n \geq n_0$,

$$\begin{aligned} |f(\beta)|_{\mathcal{P}} &= |f(\beta) - f(\alpha_n) + f(\alpha_n)|_{\mathcal{P}} \leq \\ &\leq \max\{|f(\beta) - f(\alpha_n)|_{\mathcal{P}}, |f(\alpha_n)|_{\mathcal{P}}\} < \\ &< 1 \end{aligned}$$

e portanto $\beta \in M_f$, e M_f é fechado em $\overline{A}_{\mathcal{P}}$. Desse modo, pelo que provamos acima, a família

$$\{M_f \,; f(\mathrm{x}) \in M\}$$

satisfaz a propriedade da intersecção finita e então como $\overline{A}_{\mathcal{P}}$ é compacto, pelo teorema A.3.15, devemos ter

$$\cap_{f\in M} M_f \neq \phi \,.$$

Segue daí que existe $\alpha \in \overline{A}_{\mathcal{P}}$ tal que

$$|f(\alpha)|_{\mathcal{P}} < 1$$

para todo $f(\mathrm{x}) \in M$. Logo temos

$$M \subseteq M_{\alpha,\mathcal{P}} \,.$$

Desde que $\mathcal{P}$ é ideal primo de A, existe $a \in A$ tal que $a \notin \mathcal{P}$, e como $h(\mathsf{x}) = a \in \mathcal{I}(A)$ e $h(\mathsf{x}) \notin M_{\alpha,\mathcal{P}}$, temos

$$M \subseteq M_{\alpha,\mathcal{P}} \neq \mathcal{I}(A) .$$

Mas M é ideal maximal de $\mathcal{I}(A)$ e portanto

$$M = M_{\alpha,\mathcal{P}}$$

onde $\mathcal{P} = M \cap A$ e $\alpha \in \overline{A}_{\mathcal{P}}$, como queríamos mostrar. ■

Lema 2.3.3: Seja A um domínio de Dedekind e $\mathcal{P}$ um ideal primo de A. Defina

$$V = \{f(\mathsf{x}) \in \mathcal{I}(A) \, ; f(A) \subseteq \mathcal{P}\} .$$

Então existe $\pi \in \mathcal{P}^{-1}$ tal que

$$|\pi|_{\mathcal{P}} > 1 \quad \text{e} \quad \pi f(\mathsf{x}) \in \mathcal{I}(A)$$

para todo $f(\mathsf{x}) \in V$.

Demonstração:

Sabemos que $A \subset \mathcal{P}^{-1}$ estritamente e $\mathcal{P}^{-1} \subseteq K = \mathrm{Cfr}(A)$. Tome então $\pi \in \mathcal{P}^{-1} - A$. Assim, se $|\pi|_{\mathcal{P}} < 1$ então temos $\pi \in \mathcal{P} \subseteq A$, o que contraria a escolha de π, logo devemos ter

$$|\pi|_{\mathcal{P}} \geq 1 .$$

Suponha agora que $|\pi|_{\mathcal{P}} = 1$. Então para cada $p \in \mathcal{P}$ temos

$$|p\,\pi|_{\mathcal{P}} = |p|_{\mathcal{P}} < 1$$

donde segue que $\pi.p \in \mathcal{P}$. Assim

$$\pi\mathcal{P} \subseteq \mathcal{P}$$

e daí $\pi \in \mathcal{P}\,\mathcal{P}^{-1} = A$, o que contraria a escolha de π. Portanto devemos ter

$$|\pi|_{\mathcal{P}} > 1 \ .$$

Agora seja $f(\mathsf{x}) \in V$. Então temos

$$f(A) \subseteq \mathcal{P}$$

donde

$$f(A)\,\mathcal{P}^{-1} \subseteq A$$

e portanto

$$(f\,\mathcal{P}^{-1})(A) \subseteq A \ .$$

Mas $f\,\mathcal{P}^{-1} \subseteq K[\mathsf{x}]$ e então pelo que acabamos de mostrar,

$$f\,\mathcal{P}^{-1} \subseteq \mathcal{I}(A) \ .$$

Como $\pi \in \mathcal{P}^{-1}$, segue daí que

$$\pi f \in \mathcal{I}(A) \ .$$

Portanto $\pi f(\mathsf{x}) \in \mathcal{I}(A)$ para todo $f(\mathsf{x}) \in V$. ■

Agora, tendo caracterizado os ideais maximais de $\mathcal{I}(A)$, e com o auxílio do teorema A.4.3, e do lema 2.3.2, vamos mostrar que no caso em que A é um D^*-domínio, o anel $\mathcal{I}(A)$ é um domínio de Prüfer.

Teorema 2.3.4: Se A é um D^*-domínio então $\mathcal{I}(A)$ é um domínio de Prüfer.
Demonstração:

Pelos teoremas 2.3.1 e A.4.3, basta mostrarmos que para todo ideal maximal $M = M_{\alpha,\mathcal{P}}$ de $\mathcal{I}(A)$, onde $\mathcal{P} = M \cap A$ e $\alpha \in \overline{A}_{\mathcal{P}}$, o anel

$$\mathcal{I}(A)_{M_{\alpha,\mathcal{P}}}$$

é um domínio de valorização. Para isso devemos mostrar que dados $f(\mathsf{x}), g(\mathsf{x}) \in \mathcal{I}(A)_{M_{\alpha,\mathcal{P}}}$ não nulos temos

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} \in \mathcal{I}(A)_{M_{\alpha,\mathcal{P}}} \text{ , ou}$$

$$\left(\frac{f(\mathsf{x})}{g(\mathsf{x})}\right)^{-1} = \frac{g(\mathsf{x})}{f(\mathsf{x})} \in \mathcal{I}(A)_{M_{\alpha,\mathcal{P}}} .$$

Sejam então $M_{\alpha,\mathcal{P}}$ um ideal maximal de $\mathcal{I}(A)$ e $f(\mathsf{x}), g(\mathsf{x}) \in \mathcal{I}(A)_{M_{\alpha,\mathcal{P}}}$. Desde que $\mathcal{I}(A)_{M_{\alpha,\mathcal{P}}}$ é subanel do corpo de frações de $A[\mathsf{x}]$, podemos escrever

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} = \frac{\tilde{f}(\mathsf{x})}{\tilde{g}(\mathsf{x})}$$

onde $\tilde{f}(\mathsf{x}), \tilde{g}(\mathsf{x}) \in A[\mathsf{x}]$. Pode ocorrer que

$$\tilde{f}(\alpha) = \tilde{g}(\alpha) = 0 ,$$

mas nesse caso, tome $h(\mathsf{x}) \in A[\mathsf{x}]$ um polinômio de grau mínimo que tem α como raiz. Então $h(\mathsf{x})$ divide $\tilde{f}(\mathsf{x})$ e $\tilde{g}(\mathsf{x})$ em $K[\mathsf{x}]$, e daí podemos escrever

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} = \frac{\tilde{f}(\mathsf{x})}{\tilde{g}(\mathsf{x})} = \frac{h^r(\mathsf{x})\,\overline{f}(\mathsf{x})}{h^s(\mathsf{x})\,\overline{g}(\mathsf{x})}$$

onde r e s são números inteiros positivos, $\overline{f}(\mathsf{x}), \overline{g}(\mathsf{x}) \in K[\mathsf{x}]$ e $\overline{f}(\alpha) \neq 0, \overline{g}(\alpha) \neq 0$.

Agora, existe $a \in A$ não nulo tal que $a\,\overline{f}(\mathsf{x}), a\,\overline{g}(\mathsf{x}) \in A[\mathsf{x}]$. Também, sem perda de generalidade, podemos assumir $r \geq s$ (pois caso contrário basta tomarmos $\frac{\tilde{g}}{\tilde{f}}$), e então escrevemos

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} = \frac{\tilde{f}(\mathsf{x})}{\tilde{g}(\mathsf{x})} = \frac{\hat{f}(\mathsf{x})}{\hat{g}(\mathsf{x})}$$

onde $\hat{f}(\mathsf{x}), \hat{g}(\mathsf{x}) \in A[\mathsf{x}]$ e $\hat{g}(\alpha) \neq 0$.

Se $|\hat{f}(\alpha)|_{\mathcal{P}} \geq 1$ ou $|\hat{g}(\alpha)|_{\mathcal{P}} \geq 1$, então temos o resultado desejado pois nesse caso $\hat{f}(\mathsf{x})$ ou $\hat{g}(\mathsf{x})$ não pertence a $M_{\alpha,\mathcal{P}}$, donde $\frac{\hat{f}(\mathsf{x})}{\hat{g}(\mathsf{x})}$ ou $\frac{\hat{g}(\mathsf{x})}{\hat{f}(\mathsf{x})}$ pertence a $\mathcal{I}(A)_{M_{\alpha,\mathcal{P}}}$.

Suponhamos então que

$$|\hat{f}(\alpha)|_{\mathcal{P}} < 1 \text{ e } |\hat{g}(\alpha)|_{\mathcal{P}} < 1 .$$

Por hipótese, o anel $\frac{A}{\mathcal{P}}$ é finito; seja então N o número de elementos de $\frac{A}{\mathcal{P}}$. Assim para todo $a \in A$ temos

$$a^N - a \equiv 0 \ (\mathcal{P})$$

donde segue que os polinômios

$$\hat{f}^N(\mathsf{x}) - \hat{f}(\mathsf{x}) \text{ e } \hat{g}^N(\mathsf{x}) - \hat{g}(\mathsf{x})$$

satisfazem

$$(\hat{f}^N - \hat{f})(A) \subseteq \mathcal{P} \text{ e } (\hat{g}^N - \hat{g})(A) \subseteq \mathcal{P} .$$

Pelo lema 2.3.2 temos então que existe $\pi \in \mathcal{P}^{-1}$ tal que $|\pi|_{\mathcal{P}} > 1$ e

$$\pi(\hat{f}^N - \hat{f})(\mathsf{x}) \ , \ \pi(\hat{g}^N - \hat{g})(\mathsf{x}) \in \mathcal{I}(A) .$$

Daí podemos escrever

$$\frac{\hat{f}(\mathsf{x})}{\hat{g}(\mathsf{x})} = \frac{\pi(\hat{f}^N - \hat{f})(\hat{g}^{N-1} - 1)}{\pi(\hat{g}^N - \hat{g})(\hat{f}^{N-1} - 1)}$$

já que

$$\frac{(\hat{f}^N - \hat{f})(\hat{g}^{N-1} - 1)}{(\hat{g}^N - \hat{g})(\hat{f}^{N-1} - 1)} = \frac{\hat{f}}{\hat{g}} \frac{(\hat{f}^{N-1} - 1)(\hat{g}^{N-1} - 1)}{(\hat{g}^{N-1} - 1)(\hat{f}^{N-1} - 1)} .$$

Observamos agora que

$$|\hat{f}^{N-1}(\alpha)|_{\mathcal{P}} \leq |\hat{f}(\alpha)|_{\mathcal{P}} < 1 ,$$

pois $(\hat{f}^{N-1}(\alpha)) \subseteq (\hat{f}(\alpha))$, e que

$$|\hat{g}^N(\alpha)|_{\mathcal{P}} < |\hat{g}(\alpha)|_{\mathcal{P}} ,$$

pois $|\hat{g}^N(\alpha)|_{\mathcal{P}} = |\hat{g}^{N-1}(\alpha)|_{\mathcal{P}}|\hat{g}(\alpha)|_{\mathcal{P}} < |\hat{g}(\alpha)|_{\mathcal{P}}$ uma vez que $|\hat{g}^{N-1}(\alpha)|_{\mathcal{P}} = |\hat{g}(\alpha)|_{\mathcal{P}}^{N-1} < 1$.
Desse modo, pelo teorema A.3.7, segue que

$$|\hat{f}^{N-1}(\alpha) - 1|_{\mathcal{P}} = 1$$

e

$$|\hat{g}^N(\alpha) - \hat{g}(\alpha)|_{\mathcal{P}} = |\hat{g}(\alpha)|_{\mathcal{P}} .$$

Agora se tomamos

$$g_1(\mathsf{x}) = \pi(\hat{g}^N(\mathsf{x}) - \hat{g}(\mathsf{x}))(\hat{f}^{N-1}(\mathsf{x}) - 1)$$

então temos que $g_1(\mathsf{x}) \in \mathcal{I}(A)$, e ainda que

$$|g_1(\alpha)|_{\mathcal{P}} = |\pi|_{\mathcal{P}}|\hat{g}(\alpha)|_{\mathcal{P}} > |\hat{g}(\alpha)|_{\mathcal{P}}$$

já que $|\pi|_{\mathcal{P}} < 1$.

Tomando então

$$f_1(\mathsf{x}) = \pi(\hat{f}^N(\mathsf{x}) - \hat{f}(\mathsf{x}))(\hat{g}^{N-1}(\mathsf{x}) - 1)$$

vemos que podemos escrever

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} = \frac{\hat{f}(\mathsf{x})}{\hat{g}(\mathsf{x})} = \frac{f_1(\mathsf{x})}{g_1(\mathsf{x})}$$

onde $f_1(\mathsf{x}), g_1(\mathsf{x}) \in \mathcal{I}(A)$ e $|g_1(\alpha)|_{\mathcal{P}} > |\hat{g}(\alpha)|_{\mathcal{P}}$.

Assim, repetindo esse raciocínio, construímos seqüências de polinômios

$$f_1(\mathsf{x}), f_2(\mathsf{x}), \cdots \text{ e } g_1(\mathsf{x}), g_2(\mathsf{x}), \cdots$$

todos pertencendo a $\mathcal{I}(A)$ e tais que

$$\frac{\hat{f}(\mathsf{x})}{\hat{g}(\mathsf{x})} = \frac{f_1(\mathsf{x})}{g_1(\mathsf{x})} = \frac{f_2(\mathsf{x})}{g_2(\mathsf{x})} = \cdots$$

e

$$|\hat{g}(\alpha)|_{\mathcal{P}} < |g_1(\alpha)|_{\mathcal{P}} < |g_2(\alpha)|_{\mathcal{P}} < \cdots .$$

Daí segue que

$$e^{-v_{\mathcal{P}}(\hat{g}(\alpha))} < e^{-v_{\mathcal{P}}(g_1(\alpha))} < e^{-v_{\mathcal{P}}(g_2(\alpha))} < \cdots$$

donde

$$v_{\mathcal{P}}(\hat{g}(\alpha)) > v_{\mathcal{P}}(g_1(\alpha)) > v_{\mathcal{P}}(g_2(\alpha)) > \cdots$$

Mas essa é uma seqüência decrescente de números inteiros, logo existe $k \in \mathbf{N}$ tal que

$$v_{\mathcal{P}}(g_k(\alpha)) \leq 0$$

e portanto

$$|g_k(\alpha)|_{\mathcal{P}} \geq 1$$

donde segue que $g_k(\mathsf{x}) \notin M_{\alpha,\mathcal{P}}$. Desse modo temos que

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} = \frac{f_k(\mathsf{x})}{g_k(\mathsf{x})} \in \mathcal{I}(A)_{M_{\alpha,\mathcal{P}}} .$$

Observamos ainda que se tivermos $|f_i(\alpha)|_{\mathcal{P}} \geq 1$ para algum $j \leq k$, então

$$\frac{g_i(\mathsf{x})}{f_i(\mathsf{x})} \in \mathcal{I}(A)_{M_{\alpha,\mathcal{P}}} .$$

De qualquer modo temos que $\frac{f(\mathsf{x})}{g(\mathsf{x})}$ ou $\frac{g(\mathsf{x})}{f(\mathsf{x})}$ pertence a $\mathcal{I}(A)_{M_{\alpha,\mathcal{P}}}$ e portanto $\mathcal{I}(A)_{M_{\alpha,\mathcal{P}}}$ é um domínio de valorização. ■

Pode surgir então a seguinte questão:

"O anel $\mathcal{I}(A)$ é Noetheriano?"
Pois nesse caso concluiríamos que $\mathcal{I}(A)$, onde A é um D^*-domínio, é um domínio de Dedekind.

Mas a resposta a essa questão é que em geral $\mathcal{I}(A)$ não é Noetheriano, e no exemplo 3.7 do capítulo 3 damos um exemplo desse fato.

2.4 O Teorema S

Nesse parágrafo vamos enunciar e provar o resultado final desse capítulo, que nos dá uma propriedade muito interessante do anel $\mathcal{I}(A)$ no caso em que A é um D^*-domínio. Esse resultado será chamado de teorema S em referência a T. Skolem, uma vez que se trata de um resultado mais forte que se originou no teorema de Skolem que será chamada propriedade forte de Skolem.

Novamente estaremos considerando A um domínio e K o corpo de frações de A.

Definição 2.4.1: Um domínio A é dito um D-domínio se sempre que $f(\mathsf{x}), g(\mathsf{x}) \in A[\mathsf{x}]$ são tais que

$$\frac{f(a)}{g(a)} \in A$$

para quase todo $a \in A$, temos que

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} \in K[\mathsf{x}]$$

onde $K = \mathrm{Cfr}(A)$.

Uma forma equivalente de formular essa definição é dada pela proposição seguinte:

Proposição 2.4.2: Um domínio A é um D-domínio se, e somente se, para todo polinômio não constante $f(\mathsf{x}) \in A[\mathsf{x}]$ existe um ideal primo não nulo $\mathcal{P}$

de A tal que a congruência

$$f(\mathsf{x}) \equiv 0\ (\mathcal{P})$$

tem solução em A.

Demonstração:

Suponhamos inicialmente que A é um D-domínio. Suponhamos ainda, por absurdo, que existe um polinômio $f(\mathsf{x}) \in A[\mathsf{x}]$ não constante tal que a congruência

$$f(\mathsf{x}) \equiv 0\ (\mathcal{P})$$

não tem solução em A qualquer que seja o ideal primo $\mathcal{P}$ de A. Vamos denotar por U_A o grupo das unidades de A. Assim, se $a \in A$ então $f(a) \in U_A$, pois se $f(a) \notin U_A$ existe um ideal maximal M de A tal que $f(a) \in M$, o que contraria nossa suposição . Logo temos que

$$f(A) \subseteq U_A\ .$$

Mas isso é um absurdo pois nesse caso temos que $f(a)/1$ em A para todo $a \in A$, ou seja,

$$\frac{1}{f(a)} \in A$$

para todo $a \in A$, e no entanto

$$\frac{1}{f(\mathsf{x})} \notin K[\mathsf{x}]$$

uma vez que $f(\mathsf{x})$ não é constante, o que contraria a hipótese de A ser um D-domínio.

Reciprocamente, suponha agora que para todo polinômio $f(\mathsf{x}) \in A[\mathsf{x}]$ não constante existe um ideal primo $\mathcal{P}$ de A tal que a congruência $f(\mathsf{x}) \equiv 0\ (\mathcal{P})$ tem solução em A. Então para cada polinômio $f(\mathsf{x}) \in A[\mathsf{x}]$, defina

$$S(f) = \{\mathcal{P} \subseteq A : \mathcal{P} \text{ é ideal primo e } f(\mathsf{x}) \equiv 0\ (\mathcal{P}) \text{ tem solução em } A\}$$

Primeiramente vamos mostrar que se $f(\mathsf{x})$ é não constante então $S(f)$ é infinito. Suponhamos por absurdo que $S(f)$ é finito, isto é,

$$S(f) = \{\mathcal{P}_1, \cdots, \mathcal{P}_n\} .$$

Temos duas possibilidades:

$$(1)\ f(0) = 0$$

Nesse caso temos que $f(a) \in (a)$ para todo $a \in A$. Logo $S(f)$ é o conjunto de todos os ideais primos de A, pois dado um ideal primo $\mathcal{P}$ de A, basta tomar $a \in \mathcal{P}$ qualquer e temos $f(a) \equiv 0\ (\mathcal{P})$. Então a hipótese de $S(f)$ ser finito implica que A tem apenas um número finito de ideais maximais, digamos $\{M_1, \cdots, M_s\}$. Escolhendo, para cada $1 \leq i \leq s$, $a_i \in M_i$, $a_i \neq 0$, temos então que

$$\prod_{i=1}^{s} a_i \in \cap_{i=1}^{s} M_i \ \text{ e } \ \prod_{i=1}^{s} a_i \neq 0 .$$

Ou seja, o radical de Jacobson de A é não nulo. Tome então $m \neq 0$ pertencente ao radical de Jacobson de A. Assim se consideramos

$$g(\mathsf{x}) = 1 + m\mathsf{x}$$

então temos que $g(A) \subseteq U_A$. De fato, se $a \in A$ e $1 + ma$ não é unidade de A então existe um ideal maximal M_0 de A tal que

$$1 + m\,a \in M_0 .$$

Mas m pertence ao radical de Jacobson de A, logo em particular pertence a M_0, o que implica que

$$1 \in M_0$$

o que é um absurdo. Logo $1 + ma \in U_A$.

Mas se $g(A) \subseteq U_A$ então temos

$$S(g) = \phi$$

o que contraria nossa hipótese inicial.

$$(2)\ f(0) = a_0 \neq 0$$

Nesse caso tome

$$c \in \mathcal{P}_1.\cdots.\mathcal{P}_n \quad , c \neq 0\ ,$$

e defina o polinômio $h(\mathrm{x}) \in A[\mathrm{x}]$ pela relação

$$a_0\, h(\mathrm{x}) = f(a_0\, c\mathrm{x})\ .$$

Então temos que

$$S(h) \subseteq S(f)\ , h(0) = 1\ ,$$

e todo outro coeficiente de h está em

$$cA \subseteq \mathcal{P}_1.\cdots.\mathcal{P}_n\ .$$

Mas se

$$h(\mathrm{x}) \equiv 0\ (\mathcal{P}_i)$$

tem solução em A para algum $1 \leq i \leq n$, então existe $a \in A$ tal que

$$h(a) \in \mathcal{P}_i$$

e escrevendo

$$h(\mathrm{x}) = cb_m\mathrm{x}^m + \cdots + cb_1\mathrm{x} + 1$$

então temos

$$h(a) = cb_m a^m + \cdots + cb_1 a + 1 \in \mathcal{P}_i$$

e como $cA \subseteq \mathcal{P}_1.\cdots.\mathcal{P}_n \subseteq \mathcal{P}_i$, segue que $1 \in \mathcal{P}_i$ o que é um absurdo. Logo devemos ter

$$S(h) = \phi$$

o que novamente contraria nossa hipótese inicial.

Em ambos os casos chegamos a uma contradição. Portanto, se $f(\mathsf{x}) \in A[\mathsf{x}]$ é não constante,

$$S(f) \text{ é infinito.} \tag{2.4.3}$$

Agora seja $c \in A$, $c \neq 0$, e $f(\mathsf{x}) \in A[\mathsf{x}]$ não constante. Vamos mostrar que

$$S(f) - S(c) \text{ é infinito.}$$

Novamente temos dois casos:

$$(1')\ f(0) = 0\ .$$

Nesse caso, como vimos anteriormente, temos que $S(f)$ é o conjunto de todos os ideais primos de A. Assim se supomos que $S(f) - S(c)$ é finito, então podemos supor que c pertence a todo ideal primo de A, exceto um número finito, digamos $\mathcal{P}_1, \cdots, \mathcal{P}_r$.

Tome então

$$b \in \mathcal{P}_1.\cdots.\mathcal{P}_r\ , b \neq 0\ .$$

Daí temos $bc \neq 0$ e bc pertence a todo ideal primo de A. Assim bc pertence ao radical de Jacobson de A, e tomando

$$g(\mathsf{x}) = 1 + bc\mathsf{x}$$

então como vimos anteriormente, $S(g) = \phi$, o que é um absurdo por 2.4.2.

$$(2')\ f(0) = a_0 \neq 0\ .$$

Defina nesse caso $h(\mathsf{x}) \in A[\mathsf{x}]$ como anteriormente pela relação

$$a_0 h(\mathsf{x}) = f(a_0\, c\mathsf{x})\ .$$

Novamente temos $S(h) \subseteq S(f)$, $h(0) = 1$, e todos os outros coeficientes de h são divisíveis por c. Supondo $S(f) - S(c)$ finito, temos que c pertence a todo ideal $\mathcal{P}$ em $S(f)$, exceto um número finito. Como por 2.4.3, $S(h)$ é infinito e temos $S(h) \subseteq S(f)$, podemos escolher

$$\mathcal{P}_0 \in S(h) \text{ tal que } c \in \mathcal{P}_0 .$$

Como $\mathcal{P}_0 \in S(h)$, existe $a \in A$ tal que $h(a) \in \mathcal{P}_0$. Usando então o mesmo argumento usado em (2), temos que $1 \in \mathcal{P}_0$, o que é um absurdo.

Em ambos os casos chegamos a um absurdo, donde segue que

$$S(f) - S(c) \text{ é infinito.} \tag{2.4.3}$$

Agora tomando $a_0 \in A$, $a_0 \neq 0$, temos por 2.4.3 que existe um ideal primo $\mathcal{P}_0$ de A tal que $a_0 \notin \mathcal{P}_0$. Desse modo segue que $\mathcal{P}_0$ não é um ideal trivial, portanto A não é um corpo.

Finalmente, sejam $f(\mathsf{x}), g(\mathsf{x}) \in A[\mathsf{x}]$ polinômios tais que

$$\frac{f(a)}{g(a)} \in A$$

para quase todo $a \in A$. Vamos mostrar que $\frac{f(\mathsf{x})}{g(\mathsf{x})} \in K[\mathsf{x}]$. onde $K = \mathrm{Cfr}(A)$. Podemos assumir, sem perda de generalidade, que $f(\mathsf{x})$ e $g(\mathsf{x})$ são relativamente primos em $K[\mathsf{x}]$. Vamos mostrar que $g(\mathsf{x})$ é constante.

Suponha, por absurdo, que $\partial g > 0$. Como $f(\mathsf{x})$ e $g(\mathsf{x})$ são relativamente primos em $K[\mathsf{x}]$, podemos encontrar $u'(\mathsf{x}), v'(\mathsf{x}) \in K[\mathsf{x}]$ tais que

$$u'(\mathsf{x})f(\mathsf{x}) + v'(\mathsf{x})g(\mathsf{x}) = 1 .$$

Mas existe $c \in A$ não nulo tal que $cu'(\mathsf{x}) , cv'(\mathsf{x}) \in A[\mathsf{x}]$. Logo existem $c \in A$ $c \neq 0$, e $u(\mathsf{x}), v(\mathsf{x}) \in A[\mathsf{x}]$, tais que

$$u(\mathsf{x})f(\mathsf{x}) + v(\mathsf{x})g(\mathsf{x}) = c .$$

Então, como por hipótese $g(a)/f(a)$ em A, para quase todo $a \in A$, segue que $g(a)/c$ para quase todo $a \in A$. Agora, por 2.4.3, existem um ideal primo $\mathcal{P}$ de A e $a \in A$ tais que

$$g(a) \in \mathcal{P}, c \notin \mathcal{P} \text{ e } g(a)/c \text{ em } A$$

Assim podemos escrever

$$c = g(a)b$$

onde $b \in A$, e como $g(a) \in \mathcal{P}$ segue daí que $c \in \mathcal{P}$, o que é uma contradição.

Portanto devemos ter $\partial g = 0$, ou seja, $g(\mathsf{x})$ é constante. Logo

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} \in K[\mathsf{x}]$$

como queríamos mostrar. ■

Lema 2.4.3: Se A é um D^*-domínio então A é um D-domínio.

Demonstração:

Segue diretamente da proposição 2.4.2 e da definição de D^*-domínio. ■

Finalmente vamos ao teorema central desse capítulo, que é uma versão mais forte do teorema 2.2.1.

Teorema 2.4.4 (Teorema S): Sejam A um D^*-domínio e I e J ideais finitamente gerados de $\mathcal{I}(A)$ tais que $I(a) = J(a)$ para todo $a \in A$. Então temos $I = J$.

Demonstração:

Por hipótese, A é um anel de Dedekind, logo todo ideal de A é inversível. Em particular, para todo $a \in A$ temos que $I(a)$ e $J(a)$ são ideais de A e

portanto são inversíveis. Assim, para cada $a \in A$, como $I(a) = J(a)$ por hipótese, temos

$$I(a)J(a)^{-1} = A\ .$$

Primeiramente vamos mostrar que $IJ^{-1} \subseteq \mathcal{I}(A)$, onde $J^{-1} = \{h(\mathsf{x}) \in K[\mathsf{x}]; h(\mathsf{x})J \subseteq \mathcal{I}(A)\}$. Para isso tome

$$\sum_{i=1}^{n} f_i(\mathsf{x})g_i(\mathsf{x}) \in IJ^{-1}$$

onde $n \in \mathrm{N}$ e para todo $1 \leq i \leq n$ temos $f_i(\mathsf{x}) \in I$ e $g_i(\mathsf{x}) \in J^{-1}$. Então desde que

$$J^{-1} \subseteq K(\mathsf{x}) = \mathrm{Cfr}(K[\mathsf{x}])$$

temos que para cada $1 \leq i \leq n$, $g_i(\mathsf{x})$ é da forma

$$g_i(\mathsf{x}) = \frac{u_i(\mathsf{x})}{v_i(\mathsf{x})}$$

onde $u_i(\mathsf{x}), v_i(\mathsf{x}) \in K[\mathsf{x}]$. Desse modo cada $g_i(\mathsf{x})$ está definido para todo $a \in A$, exceto um número finito de pontos, que são as raízes de $v_i(\mathsf{x})$. Assim a soma

$$\sum_{i=1}^{n} f_i(a)g_i(a)$$

está definida para todo $a \in A$, exceto num número finito. Para cada $a \in A$ para o qual essa soma está definida temos que

$$f_i(a) \in I(a)$$

para todo $1 \leq i \leq n$. Também temos que $g_i(a) \in J(a)^{-1}$ para todo $1 \leq i \leq n$. De fato, se $t \in J(a)$ então $t = h(a)$ para algum $h(\mathsf{x}) \in J$, daí como $g_i(\mathsf{x}) \in J^{-1}$ para todo $1 \leq i \leq n$, segue que

$$g_i(\mathsf{x})h(\mathsf{x}) \in \mathcal{I}(A)$$

e desse modo

$$g_i(a).t = g_i(a)h(a) \in A$$

para $1 \leq i \leq n$. Logo $g_i(a) \in J(a)^{-1}$ para todo $1 \leq i \leq n$.

Com isso está mostrado que

$$\sum_{i=1}^{n} f_i(a)g_i(a) \in I(a)J(a)^{-1} \subseteq A$$

para todo $a \in A$ exceto um número finito.

Agora, como podemos escrever

$$\sum_{i=1}^{n} f_i(\mathsf{x})g_i(\mathsf{x}) = \frac{f(\mathsf{x})}{g(\mathsf{x})}$$

onde $f(\mathsf{x}), g(\mathsf{x}) \in A[\mathsf{x}]$, temos mostrado que

$$\frac{f(a)}{g(a)} \in A$$

para quase todo $a \in A$. Mas pelo lema 2.4.5, A é um D-domínio, donde segue que

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} \in K[\mathsf{x}] \, .$$

Assim temos que sempre que $g(a) = 0$, então também $f(a) = 0$. Logo podemos escrever

$$\frac{f(\mathsf{x})}{g(\mathsf{x})} = \frac{\overline{f}(\mathsf{x})}{\overline{g}(\mathsf{x})}$$

onde $\overline{g}(a) \neq 0$ para todo $a \in A$. Desse modo passamos a ter

$$\frac{\overline{f}(\mathsf{x})}{\overline{g}(\mathsf{x})} \in K[\mathsf{x}]$$

e

$$\frac{\overline{f}(a)}{\overline{g}(a)} \in A \text{ para todo } a \in A$$

uma vez que eliminamos a possibilidade de $g(a) = 0$. Isso implica que

$$\sum_{i=1}^{n} f_i(\mathrm{x})g_i(\mathrm{x}) = \frac{f(\mathrm{x})}{g(\mathrm{x})} = \frac{\overline{f}(\mathrm{x})}{\overline{g}(\mathrm{x})} \in \mathcal{I}(A)$$

e portanto

$$IJ^{-1} \subseteq \mathcal{I}(A) .$$

Agora, pelo teorema 2.3.4, temos que $\mathcal{I}(A)$ é um domínio de Prüfer; além disso, J é um ideal finitamente gerado de $\mathcal{I}(A)$, donde segue que J é inversível. Então temos

$$I.J^{-1}.J \subseteq \mathcal{I}(A).J \subseteq J$$

donde segue que

$$I.\mathcal{I}(A) \subseteq J$$

e daí

$$I \subseteq J .$$

Também por um raciocínio análogo temos que

$$J \subseteq I .$$

Portanto $I = J$ como queríamos mostrar. ■

No próximo capítulo daremos um exemplo da utilidade do teorema S. Além disso, no exemplo 3.7 mostramos que a hipótese dos ideais serem finitamente gerados não pode ser retirada.

Concluímos esse capítulo chamando a atenção para o fato de que se K é um corpo numérico e A é o anel de inteiros de K, então A é um D^*-domínio. Consequentemente os resultados desse capítulo são válidos para o anel $Int(A)$, inclusive o teorema S. Ou seja, mostramos nesse capítulo que o anel $Int(A)$ é um domínio de Prüfer e possui a propriedade descrita no teorema S.

onde $i = \sqrt{-1}$, e seja A o anel de inteiros de K. Desde que

$$-1 \equiv 3 \pmod 4$$

podemos escrever

$$A = \mathbf{Z}\,(i) = \{a + bi\,; a, b \in \mathbf{Z}\}\,.$$

Nesse caso o polinômio

$$P(\mathrm{x}) = \frac{\mathrm{x}(\mathrm{x}-1)}{i+1} \in K[\mathrm{x}]$$

é a valores inteiros sobre K mas claramente não é um polinômio inteiro sobre K.

Para verificar que $P(\mathrm{x})$ é a valores inteiros sobre K, tome $a + bi \in A$ e então temos

$$P(a+bi) = \frac{(a+bi)(a-1+bi)}{i+1} =$$
$$= \frac{(a(a-1)+b(2a-1-b)) + i(-a(a-1)+b(2a-1+b))}{2}$$

Mas $a(a-1)+b(2a-1-b)$ e $-a(a-1)+b(2a-1+b)$ são números pares, logo temos que

$$P(a+bi) = c + di$$

onde $c, d \in \mathbf{Z}$. Portanto

$$P(A) \subseteq A\,,$$

donde $P(\mathrm{x})$ é a valores inteiros sobre K.

Exemplo 3.2:

Sejam $K' = \mathbf{Q}$ e $K = \mathbf{Q}\,(i)$ como no exemplo 3.1. Sejam ainda $A' = \mathbf{Z}$ e $A = \mathbf{Z}\,(i)$ os anéis de inteiros de K' e K respectivamente. Então o polinômio

$$P(\mathrm{x}) = \frac{\mathrm{x}(\mathrm{x}-1)}{2} \in K'[\mathrm{x}] \subseteq K[\mathrm{x}]$$

é a valores inteiros sobre K' mas não o é sobre K.

De fato, para todo $a \in A' = \mathbf{Z}$, temos que ou a é par ou $a-1$ é par, logo

$$P(a) = \frac{a(a-1)}{2} \in \mathbf{Z} = A'$$

e portanto $P(A') \subseteq A'$, donde $P(\mathsf{x})$ é a valores inteiros sobre K'. Por outro lado, tome $i \in A = \mathbf{Z}$ (i) e então temos

$$P(i) = \frac{i(i-1)}{2} = -\left(\frac{1+i}{2}\right) \notin A$$

Desse modo, $P(A) \not\subseteq A$, ou seja, $P(\mathsf{x})$ não é a valores inteiros sobre K.

Ainda no parágrafo 1.1 , definimos base regular de polinômios a valores inteiros sobre um corpo numérico K, que é também uma A-base livre do A-módulo $Int(A)$. Em 3.3 usaremos resultados apresentados no parágrafo 1.2 para fornecer um exemplo concreto de uma tal base.

Exemplo 3.3:

Seja $K = \mathbf{Q}$; e nesse caso, $A = \mathbf{Z}$. Vamos mostrar que K possui uma base regular de polinômios a valores inteiros

$$\{F_n(\mathsf{x})\}_{n \in \mathbf{N}}$$

dada por

$$F_0(\mathsf{x}) = 1, e$$

$$F_m(\mathsf{x}) = \binom{\mathsf{x}}{m} = \frac{\mathsf{x}(\mathsf{x}-1)\cdots(\mathsf{x}-m+1)}{m!}$$

para $m \geq 1$. De fato, o teorema 1.2.4 nos garante que $\mathbf{Q}$ possui uma base regular de polinômios a valores inteiros, uma vez que $\mathbf{Z}$ é anel principal.Também a proposição 1.2.1 afirma que a sequência

$$\{F_n(\mathsf{x})\}_{n \in \mathbf{N}}$$

definida acima é uma $\mathbf{Q}$ -base para $\mathbf{Q}$ [x]. Vamos mostrar que essa sequência satisfaz as condições necessárias para ser uma base regular de polinômios a valores inteiros sobre $\mathbf{Q}$.

(1) Para cada $m \geq 0$ o polinômio $F_m(\mathbf{x}) = \binom{\mathbf{x}}{m}$ é a valores inteiros sobre $\mathbf{Q}$. É claro pois, se $n \in \mathbf{Z}$, é fácil verificar que

$$F_m(n) = \begin{cases} 0 \text{ , se } 0 \leq n < m \\ \binom{n}{m} \text{ , se } n \geq m \\ (-1)^n \binom{|n| + (m-1)}{m} \text{ , se } n < 0 \text{ .} \end{cases}$$

Em qualquer um dos casos temos $F_m(n) \in \mathbf{Z}$ donde $F_m(\mathbf{x}) \in Int(\mathbf{Z})$ para todo $m \in \mathrm{N}$.

(2) Para todo $m \in \mathrm{N}$ temos $\partial F_m(\mathbf{x}) = m$.

(3) Tome $P(\mathbf{x})$ um polinômio qualquer em $Int(\mathbf{Z})$ de grau m. Então , usando a proposição 1.2.1 e operador de Gregory-Newton

$$\Delta P(\mathbf{x}) = P(\mathbf{x}+1) - P(\mathbf{x})$$

definido no parágrafo 1.2, temos que

$$P(\mathbf{x}) = \Delta^m P(0) F_m(\mathbf{x}) + \cdots + \Delta^1 P(0) F_1(\mathbf{x}) + P(0) F_0(\mathbf{x}) \text{ .}$$

Mas como $P(\mathbf{x}) \in Int(\mathbf{Z})$ temos que

$$\Delta^i P(0) \in \mathbf{Z}$$

para todo $0 \leq i \leq m$. Logo $P(\mathbf{x})$ pode ser escrito na forma

$$P(\mathbf{x}) = \beta_m F_m(\mathbf{x}) + \cdots + \beta_1 F_1(\mathbf{x}) + \beta_0 F_0(\mathbf{x})$$

onde $\beta_i \in \mathbf{Z}$ para todo $0 \leq i \leq m$.

Portanto, por (1), (2) e (3), segue que $\{F_n(\mathrm{x})\}_{n\in\mathbf{N}}$ é uma base regular de polinômios a valores inteiros sobre $\mathbf{Q}$.

Observe ainda que, no caso do exemplo 3.3, a seqüência $\{\mu_n\}_{n\in\mathbf{N}}$ dada pelo teorema 1.2.6 pode ser tomada como

$$\{\mu_n\}_{n\in\mathbf{N}} \quad \text{onde} \quad \mu_n = n \ , \quad \text{para todo} \quad n \in \mathrm{N} \ .$$

O teorema 1.5.1 nos apresenta uma forma definitiva de decidir se um corpo quadrático K possui ou não uma base regular de polinômios a valores inteiros. O próximo exemplo ilustra esse fato.

Exemplo 3.4:

Considere o corpo quadrático $K = \mathbf{Q}\ (\sqrt{-5})$. Como $-5 = 3 \pmod 4$, temos que nesse caso $A = \mathbf{Z}\ [\sqrt{-5}]$ e o discriminante absoluto de K é $d = -20$. Pelo teorema 1.5.1, para sabermos se K possui ou não uma base regular de polinômios a valores inteiros basta analisarmos os números primos ramificados. Como $d = -20$, segue que os únicos primos ramificados neste caso são 2 e 5. Mas pelo teorema A.1.19, temos que

$$2.A = \mathcal{P}^2$$

onde $\mathcal{P} = (2, u + \sqrt{-5})$ com $0 \leq u \leq 2$ e $2/N(u + \sqrt{-5}) = u^2 - 5$. Assim, $u = 1$ e portanto

$$\mathcal{P} = (2, 1 + \sqrt{-5}) \ .$$

Ora, esse é um ideal primo de A que contém d e não é principal, donde concluímos pelo teorema 1.5.1 que K <u>não</u> possui uma base regular de polinômios a valores inteiros.

Vamos considerar agora, como no capítulo 2, A um domínio e K o corpo de frações de A. Apresentaremos agora exemplos sobre os resultados do capítulo 2.

No teorema 2.1.2, temos que $\mathcal{I}(\mathbf{Z}) = Int(\mathbf{Z})$ é um anel de Skolem. O exemplo 3.5 abaixo mostra que esse resultado não pode ser generalizado a um domínio A qualquer.

Exemplo 3.5:

Considere o domínio de Dedekind $A = \mathbf{Q}[\mathsf{x}]_{(\mathsf{x})}$ e seja $K = \mathrm{Cfr}(A)$. Vamos mostrar que $\mathcal{I}(A)$ não é um anel de Skolem. Para isso vamos utilizar o seguinte lema, provado por D. Brizolis em [4].

Lema: Sejam B um domínio de Dedekind e $\mathcal{P} \subsetneq B$ um ideal primo de B. Se o anel quociente $B/\mathcal{P}$ é infinito então $\mathcal{I}(B_{\mathcal{P}}) = B_{\mathcal{P}}[X]$.

Demonstração:

Sabemos que $B_{\mathcal{P}}[\mathsf{x}] \subseteq \mathcal{I}(B_{\mathcal{P}})$. Basta mostrar então a inclusão contrária. Seja $f(\mathsf{x}) \in \mathcal{I}(B_{\mathcal{P}})$ um polinômio qualquer em $\mathcal{I}(B_{\mathcal{P}})$. Podemos escrever

$$f(\mathsf{x}) = \frac{a_n}{b}\mathsf{x}^n + \cdots + \frac{a_1}{b}\mathsf{x} + \frac{a_0}{b} \ ,$$

onde $a_0, \cdots, a_n, b \in B_{\mathcal{P}}$. Daí temos

$$\begin{aligned} b.f(\mathsf{x}) &= a_n\mathsf{x}^n + \cdots + a_1\mathsf{x} + a_0 \\ &= a(a'_n\mathsf{x}^n + \cdots + a'_1\mathsf{x} + a'_0) \end{aligned}$$

onde $a, b \in B_{\mathcal{P}}$, $g(\mathsf{x}) = a'_n\mathsf{x}^n + \cdots + a'_1\mathsf{x} + a'_0 \in B_{\mathcal{P}}[\mathsf{x}]$ é tal que

$$\mathrm{mdc}(a'_0, a'_1, \cdots, a'_n) = 1 \ ,$$

e podemos supor $\mathrm{mdc}(a, b) = 1$. Mas como B é um domínio de Dedekind, $B_{\mathcal{P}}$ é um anel de valorização discreta e então

$$a = \pi^r.\varepsilon$$
$$b = \pi^s.\varepsilon'$$

onde ε e ε' são unidades de $B_{\mathcal{P}}$ e π é irredutível em $B_{\mathcal{P}}$. Assim, como $\text{mdc}(a,b) = 1$, temos que ou a ou b é unidade em $B_{\mathcal{P}}$, ou seja, ou $a \notin \mathcal{P}B_{\mathcal{P}}$ ou $b \notin \mathcal{P}B_{\mathcal{P}}$ (lembrando que $B_{\mathcal{P}}$ é anel local com ideal maximal $\mathcal{P}B_{\mathcal{P}}$). Por outro lado, como $\text{mdc}(a'_n, \cdots, a'_1, a'_0) = 1$, existe i com $0 \leq i \leq n$ tal que a'_i é unidade em $B_{\mathcal{P}}$, e daí $a_i \notin \mathcal{P}B_{\mathcal{P}}$.

Agora passando ao quociente $\frac{B_{\mathcal{P}}}{\mathcal{P}B_{\mathcal{P}}}$, temos

$$\overline{b}.\overline{f}(\mathsf{x}) = \overline{a}.\overline{g}(\mathsf{x})$$

onde $\overline{g}(\mathsf{x})$ não é o polinômio nulo pois $a_i \notin \mathcal{P}B_{\mathcal{P}}$. Mas temos que $\frac{B}{\mathcal{P}}$ é infinito e

$$\frac{B}{\overline{\mathcal{P}}} = \frac{B_{\mathcal{P}}}{\mathcal{P}B_{\mathcal{P}}} ,$$

donde $\frac{B_{\mathcal{P}}}{\mathcal{P}B_{\mathcal{P}}}$ é infinito. Logo existe $\alpha \in B_{\mathcal{P}}$ tal que $\overline{g}(\overline{\alpha}) \neq 0$, isto é, $g(\alpha) \notin \mathcal{P}B_{\mathcal{P}}$. Assim, se $a \in \mathcal{P}B_{\mathcal{P}}$ então $b \notin \mathcal{P}B_{\mathcal{P}}$, donde b é unidade em $B_{\mathcal{P}}$.

Por outro lado, se $a \notin \mathcal{P}B_{\mathcal{P}}$ então pela igualdade

$$bf(\alpha) = ag(\alpha)$$

temos que $bf(\alpha) \notin \mathcal{P}B_{\mathcal{P}}$, uma vez que $g(\alpha) \notin \mathcal{P}B_{\mathcal{P}}$: logo devemos ter $b \notin \mathcal{P}B_{\mathcal{P}}$ e novamente b é unidade em $B_{\mathcal{P}}$. Assim, em ambos os casos temos que b é unidade em $B_{\mathcal{P}}$ e daí segue que

$$f(\mathsf{x}) = \frac{a}{b}g(\mathsf{x}) \in B_{\mathcal{P}}[\mathsf{x}] ,$$

como queríamos mostrar. ■

Tomando então $B = \mathbb{Q}[\mathsf{x}]$ e $\mathcal{P} = (\mathsf{x})$, temos pelo lema que

$$\mathcal{I}(A) = A[\mathsf{y}] .$$

Agora, para cada $t(\mathsf{x}) \in A = \mathbb{Q}[\mathsf{x}]_{(\mathsf{x})}$, temos que

$$t(\mathsf{x}) = \frac{u(\mathsf{x})}{v(\mathsf{x})}$$

onde $u(\mathsf{x}), v(\mathsf{x}) \in \mathbb{Q}\,[\mathsf{x}]$ e $v(\mathsf{x}) \notin (\mathsf{x})$. Assim $v(0) \neq 0$. Além disso,

$$t(\mathsf{x})^2 + 1 = \frac{u(\mathsf{x})^2}{v(\mathsf{x})^2} + 1$$

donde

$$v(\mathsf{x})^2 \left(t(\mathsf{x})^2 + 1\right) = u(\mathsf{x})^2 + v(\mathsf{x})^2$$

Desde que $v(\mathsf{x}) \notin (\mathsf{x})$, temos que $v(\mathsf{x})$ é unidade em A, consequentemente $v(\mathsf{x})^2$ também é unidade em A.

Agora se $u(\mathsf{x})^2 + v(\mathsf{x})^2 \in (\mathsf{x})$ então temos que

$$u(0)^2 + v(0)^2 = 0$$

e portanto

$$v(0)^2 = -u(0)^2$$

o que é um absurdo, pois $v(0), u(0) \in \mathbb{Q}$ e $v(0) \neq 0$. Logo devemos ter

$$u(\mathsf{x})^2 + v(\mathsf{x})^2 \notin (\mathsf{x})$$

ou seja, $u(\mathsf{x})^2 + v(\mathsf{x})^2$ é unidade em A. Com isso mostramos então que

$$\left(t(\mathsf{x})^2 + 1\right) = (1) = A$$

para todo $t(\mathsf{x}) \in A$.

Mas por outro lado, temos que

$$(\mathsf{y}^2 + 1) \neq A[\mathsf{y}] = \mathcal{I}(A)$$

donde segue que $\mathcal{I}(A)$ não pode ser um anel de Skolem.

Vale observar que A não é um D^*-domínio, uma vez que $\frac{A}{M}$ não é finito, onde M é o único ideal maximal de A, pois podemos ver que $\mathbb{Q} = \frac{A}{M}$.

Os dois exemplos seguintes se referem ao teorema 2.4.6. No exemplo 3.6, ilustramos o uso desse teorema; já no exemplo 3.7 mostramos que a hipótese exigida de que I e J sejam finitamente gerados não pode ser retirada.

Exemplo 3.6:

Seja $A = \mathbf{Z}$ e considere os seguintes ideais de $\mathcal{I}(\mathbf{Z}) = Int(\mathbf{Z})$:

$$I = \left(2, x, \frac{x(x-1)}{2}\right) \quad \text{e} \quad J = \left(2, \frac{x(x^2+1)}{2}\right).$$

É fácil mostrar que se $a \in \mathbf{Z}$ então

$$I(a) = J(a) = \begin{cases} (2) & \text{se} \quad a \equiv 0 \pmod 4 \\ (1) & \text{se} \quad a \equiv 1,\ 2 \text{ ou } 3 \pmod 4 \end{cases}$$

Logo pelo teorema 2.4.6 temos que $I = J$.

Para comprovar isso explicitamente, basta verificar que

$$x = 2\left[\frac{x^2(x-1)^2}{4}\right] + \frac{x(x^2+1)}{2}(2-x)$$

e

$$\frac{x(x-1)}{2} = 2\left[-\frac{x^3(x+1)^3}{8}\right] + \frac{x(x^2+1)}{2}\left[\frac{x^2(x+3)+2(x-1)}{2}\right].$$

onde $\frac{x^2(x-1)^2}{4}$, $2-x$, $-\frac{x^3(x+1)^3}{8}$, $\frac{x^2(x+3)+2(x-1)}{2}$, são polinômios em $Int(\mathbf{Z})$. Logo $I \subseteq J$. Também temos

$$\frac{x(x^2+1)}{2} = x.x + \frac{x(x-1)}{2}(x-1)$$

onde $x,\ x-1 \in Int(\mathbf{Z})$, donde $J \subseteq I$.

Portanto $I = J$.

Como dissemos anteriormente, vamos agora mostrar que a hipótese de I e J serem finitamente gerados não é supérflua. Para isso vamos tomar um ideal I em $\mathcal{I}(\mathbf{Z}) = Int(\mathbf{Z})$ que não é finitamente gerado e tal que $I(a) = \mathbf{Z}$ para todo $a \in \mathbf{Z}$, mas $I \neq \mathcal{I}(\mathbf{Z})$.

Exemplo 3.7:

Considere $A = \mathbf{Z}$. Como foi provado no teorema 2.3.1, todo ideal maximal de $Int(\mathbf{Z})$ é da forma

$$M_{\alpha,p} = \{f(\mathbf{x}) \in Int(\mathbf{Z}); |f(\alpha)|_p < 1\}$$

onde $p \in \mathbf{Z}$ é um número primo e $\alpha \in \overline{\mathbf{Z}}_p$. Vamos mostrar que esses ideais não são finitamente gerados; para isso precisaremos de alguns resultados auxiliares.

Lema 3.0.7.1: Seja $p \in \mathbf{Z}$ um número primo. Se $\alpha \in \overline{\mathbf{Z}}_p$, $\alpha \neq 0$, então existe $n \in \mathbf{N}$ tal que

$$\left|\begin{pmatrix} \alpha \\ p^n \end{pmatrix}\right|_p = 1 .$$

Demonstração:

Podemos escrever, para algum $n \in \mathbf{Z}$,

$$\alpha = a_n p^n + a_{n+1} p^{n+1} + \cdots$$

onde $0 \leq a_i \leq p-1$ para todo $i \geq n$, $n \geq 0$ e $a_n \neq 0$.

Agora

$$\begin{aligned} \left|\begin{pmatrix} \alpha \\ p^n \end{pmatrix}\right|_p &= \left|\frac{\alpha(\alpha-1)\cdots(\alpha-p^n+1)}{p^n(p^n-1)\cdots 1}\right|_p \\ &= \left|\frac{\alpha}{p^n}\right|_p \cdot \left|\frac{\alpha-1}{p^n-1}\right|_p \cdot \ldots \cdot \left|\frac{\alpha-p^n+1}{1}\right|_p . \end{aligned}$$

Mas

$$\left|\frac{\alpha}{p^n}\right|_p . = |a_n + a_{n+1}p + \cdots| \leq \max\{|a_n|_p, |a_{n+1}p|_p, \cdots\}$$

e como $|a_{n+i}p^i| < 1$ para $i \geq 1$, segue então que

$$\left|\frac{\alpha}{p^n}\right|_p = |a_n|_p = 1$$

já que $0 \leq a_n \leq p-1$. Além disso,

$$|\alpha|_p \leq \max\{|a_n p^n|_p, |a_{n+1}p^{n+1}|_p, \cdots\}$$

donde

$$|\alpha|_p = |a_n p^n|_p = |p^n|_p = \frac{1}{e^n} ;$$

logo segue daí que se $0 < i < p^n$ devemos ter

$$|\alpha|_p < |i|_p .$$

Desse modo,

$$|p^n - i|_p = |\alpha - i|_p = |i|_p$$

e então

$$\left|\frac{\alpha - i}{p^n - i}\right|_p = 1$$

para todo $1 \leq i < p^n$.

Portanto temos que $\left|\begin{pmatrix} \alpha \\ p^n \end{pmatrix}\right|_p = 1.$ ■

Lema 3.0.7.2: Sejam $p \in \mathbf{Z}$ um número primo e $\alpha \in \overline{\mathbf{Z}}_p$. Então para todo $m \in \mathbf{Z}$, $m \geq 0$, o polinômio

$$f(\mathsf{x}) = \begin{pmatrix} \mathsf{x} - \alpha \\ m \end{pmatrix}$$

pode ser uniformemente aproximado em $\overline{\mathbf{Z}}_p$ por polinômios em $Int(\mathbf{Z})$.

Demonstração:

Basta notar que se $\alpha \in \overline{\mathbf{Z}}_p$ então pela densidade de $\mathbf{Z}$ em $\overline{\mathbf{Z}}_p$ temos que $\alpha = \lim_{n\to\infty} b_n$, onde $b_n \in \mathbf{Z}$ para todo $n \in \mathbf{N}$. É fácil mostrar então que $\begin{pmatrix} \mathrm{x}-\alpha \\ m \end{pmatrix} = \lim_{n\to\infty} \begin{pmatrix} \mathrm{x}-b_n \\ m \end{pmatrix}$. ■

Proposição 3.7.3: Sejam $p \in \mathbf{Z}$ um número primo e $\alpha, \beta \in \overline{\mathbf{Z}}_p$. Então $M_{\alpha,p} = M_{\beta,p}$ se, e somente se, $\alpha = \beta$.

Demonstração:

Suponhamos $M_{\alpha,p} = M_{\beta,p}$ e, por absurdo, que $\alpha - \beta \neq 0$. Então pelo lema 3.7.1, existe $n \in \mathbf{Z}$, $n \geq 0$, tal que

$$\left| \begin{pmatrix} \alpha-\beta \\ p^n \end{pmatrix} \right|_p = 1 \ .$$

Considere então o polinômio

$$f(\mathrm{x}) = \begin{pmatrix} \mathrm{x}-\alpha \\ p^n \end{pmatrix} = \frac{(\mathrm{x}-\alpha)(\mathrm{x}-\alpha-1)\cdots(\mathrm{x}-\alpha-p^n+1)}{p^n!} \ .$$

Pelo lema 3.7.2, existe $g(\mathrm{x}) \in Int(\mathbf{Z})$ tal que

$$|f(a) - g(a)|_p < 1$$

para todo $a \in \overline{\mathbf{Z}}_p$. Agora, desde que $f(\alpha) = 0$, temos que

$$|g(\alpha)|_p = |f(\alpha) - g(\alpha)|_p < 1$$

donde segue que $g(\mathrm{x}) \in M_{\alpha,p}$. Por outro lado,

$$|g(\beta)|_p = |(f(\beta) - g(\beta)) - f(\beta)|_p \leq \max\{|f(\beta) - g(3)|_p, |f(\beta)|_p\}$$

e como $|f(\beta) - g(\beta)|_p < 1 = |f(\beta)|_p$, segue daí que

$$|g(\beta)|_p = |f(\beta)|_p = 1 \ .$$

Logo $g(\mathsf{x}) \notin M_{\beta,p}$. Dessa forma concluímos que

$$g(\mathsf{x}) \in M_{\alpha,p} \backslash M_{\beta,p}$$

o que contraria a hipótese de que $M_{\alpha,p} = M_{\beta,p}$. Portanto devemos ter $\alpha = \beta$.

A recíproca é imediata. ■

Agora sejam $p \in \mathbf{Z}$ um número primo e $\alpha \in \overline{\mathbf{Z}}_p$. Vamos mostrar que $M_{\alpha,p}$ não é finitamente gerado. Suponhamos por absurdo que

$$M_{\alpha,p} = (f_1(\mathsf{x}), \cdots, f_n(\mathsf{x}))$$

onde $f_1(\mathsf{x}), \cdots, f_n(\mathsf{x}) \in M_{\alpha,p}$. Então

$$|f_i(\alpha)|_p < 1$$

para todo $1 \leq i \leq n$. Desde que $\mathbf{Z}$ é denso $\overline{\mathbf{Z}}_p$, temos que

$$\forall \varepsilon > 0 \; \exists a \in \mathbf{Z} \;\; , a \neq \alpha \;\; , \text{ tal que } \; |a - \alpha|_p < \varepsilon$$

e como $f_i(\mathsf{x})$ é contínua na topologia p-ádica para todo $1 \leq i \leq n$, temos ainda que

$$\forall \varepsilon_0 > 0 \;\; \text{tal que } \; |\alpha - \beta|_p < \varepsilon_0 \Rightarrow |f_i(\alpha) - f_i(\beta)|_p < 1$$

para todo $1 \leq i \leq n$. Assim, para este ε_0 existe $a \in \mathbf{Z}$, $a \neq \alpha$, tal que

$$|f_i(\alpha) - f_i(a)|_p < 1 \;,$$

para todo $1 \leq i \leq n$. Agora, para cada $1 \leq i \leq n$,

$$|f_i(\alpha) - f_i(a)|_p \leq \; \max\{|f_i(\alpha)|_p, |f_i(a)|_p\}$$

e $|f_i(\alpha)|_p < 1$, logo se $|f_i(a)|_p = 1$ teríamos

$$|f_i(\alpha) - f_i(a)|_p = 1$$

o que seria um absurdo, donde devemos ter

$$|f_i(a)|_p < 1 \ .$$

Ou seja, mostramos que $|f_i(a)|_p < 1$ para todo $1 \leq i \leq n$. Portanto

$$M_{\alpha,p} \subseteq M_{a,p}$$

e como $M_{\alpha,p}$ e $M_{a,p}$ são ideais maximais, segue daí que

$$M_{\alpha,p} = M_{a,p} \ .$$

Logo $\alpha = a$, o que contraria a escolha de a. Concluímos então que $M_{\alpha,p}$ não pode ser finitamente gerado.

Agora seja $p \in \mathbf{Z}$ um número primo e tome $\alpha \in \overline{\mathbf{Z}}_p$ tal que $\alpha \notin \mathbf{Z}$. Considere então o ideal

$$I = M_{\alpha,p} \subset Int(\mathbf{Z}) \quad \text{estritamente}$$

que é um ideal maximal de $Int(\mathbf{Z})$. Vamos mostrar que $I(a) = \mathbf{Z}$ para todo $a \in \mathbf{Z}$.

Primeiramente note que para todo $a \in \mathbf{Z}$ existe um polinômio $f_a(\mathsf{x}) \in M_{\alpha,p}$ tal que

$$|f_a(a)|_p = 1 \ .$$

De fato, se isso não ocorresse, teríamos

$$M_{\alpha,p} \subseteq M_{a,p}$$

donde

$$M_{\alpha,p} = M_{a,p}$$

pois esses são ideais maximais de $Int(\mathbf{Z})$; logo pela proposição 3.7.3, $\alpha = a$, o que é um absurdo pela escolha de α.

Seja então $a \in \mathbf{Z}$ e considere o polinômio

$$g(\mathsf{x}) = f_a(\mathsf{x}) - f_a(a) \in Int(\mathbf{Z}) .$$

Evidentemente $g(a) = 0$ e portanto temos que

$$|g(\alpha)|_p = |f_a(\alpha) - f_a(a)|_p = 1$$

já que $|f_a(\alpha)|_p < 1 = |f_a(a)|_p$. Segue daí que

$$g(\mathsf{x}) \notin M_{\alpha,p} = I$$

Mas I é ideal maximal de $Int(\mathbf{Z})$, logo temos que

$$I + (g(\mathsf{x})) = Int(\mathbf{Z})$$

donde segue que existem $h(\mathsf{x}) \in Int(\mathbf{Z})$ e $t(\mathsf{x}) \in I$ tais que

$$1 = t(\mathsf{x}) + h(\mathsf{x}).g(\mathsf{x}) .$$

Daí temos

$$1 = t(a) + h(a).g(a) = t(a)$$

ou seja, dado que $t(\mathsf{x}) \in I$,

$$1 \in I(a) .$$

Portanto temos que $I = M_{\alpha,p}$ é um ideal de $Int(\mathbf{Z})$ que <u>não</u> é finitamente gerado e tal que

$$I(a) = \mathbf{Z}$$

para todo $a \in \mathbf{Z}$. No entanto, $I \neq \mathbf{Z}$, uma vez que I é maximal. Logo o teorema 2.4.6 não é válido se um dos ideais I ou J não é finitamente gerado.

Observe que este exemplo nos mostra ainda que $Int(\mathbf{Z})$ é um domínio de Prüfer não Noetheriano. Em artigo recente, R. Gilmer, W. Heinzer e D. Lantz[9] mostraram um resultado mais geral, donde segue como conseqüência que se A é um D^*-domínio então $\mathcal{I}(A)$ não é Noetheriano.

Apêndice A

Notação e resultados auxiliares

Introdução

Finalizando nosso trabalho, apresentamos esse apêndice, cujos objetivos são esclarecer alguma dúvida que possa ter surgido sobre a notação utilizada e ainda relembrar alguns resultados da teoria de números necessários ao nosso estudo. Omitimos as demonstrações na maioria dos casos por se tratarem de resultados clássicos. No entanto, damos referências onde tais demonstrações podem ser encontradas.

Vamos admitir o conhecimento dos conceitos de anel, ideal, corpo, domínio e seu corpo de frações, anel de polinômios, módulo, bem como a teoria básica decorrente desses conceitos. Observamos que a leitura desse apêndice não é indispensável à compreensão do trabalho, podendo ser utilizado apenas como ponto de referência.

Primeiramente vamos fixar aqui algumas notações que são utilizadas. Como de costume, denotamos por $\mathbf{N}, \mathbf{Z}$ e $\mathbf{Q}$ os conjuntos dos números *naturais*, *inteiros* e *racionais* respectivamente. Dado um domínio A, denotaremos por $\mathrm{Cfr}(A)$ o corpo de frações de A e por $A[\mathrm{x}]$ o anel de polinômios a uma

variável sobre A. Além disso, dados um corpo K e uma extensão L de K, vamos denotar por $\mathrm{ch}(K)$ a característica do corpo K e por $[L : K]$ o grau da extensão L/K. Também, se A é um domínio e $f(\mathsf{x})$ é um polinômio em $A[\mathsf{x}]$, então denotamos por $\partial f(\mathsf{x})$ o grau do polinômio $f(\mathsf{x})$.

A seguir vamos definir alguns conceitos e enunciar resultados necessários ao trabalho.

A.1 Domínios de Dedekind e Anéis de Inteiros

Considere A um domínio e $K = \mathrm{Cfr}(A)$.

Definição A.1.1: Dizemos que A é Noetheriano se todo ideal de A é finitamente gerado.

Definição A.1.2: A é chamado um domínio de Dedekind se é Noetheriano, integralmente fechado e todo ideal primo não nulo de A é maximal.

Enunciaremos agora alguns resultados importantes sobre domínios de Dedekind.

Teorema A.1.3: Sejam A um domínio de Dedekind, $K = \mathrm{Cfr}(A)$, L uma extensão de K de grau finito e B o fecho integral de A em L. Suponhamos ainda que $\mathrm{ch}(K) = 0$. Então B é um domínio de Dedekind e um sub-módulo de um A-módulo livre de posto $[L : K]$.

Como conseqüência imediata desse teorema temos que B é um A-módulo finitamente gerado. Além disso, se A é ideal principal, então B é um A-módulo livre de posto $[L : K]$.

Em um domínio de Dedekind, todo ideal primo não nulo $\mathcal{P}$ é inversível, com ideal inverso dado por

$$\mathcal{P}^{-1} = \{a \in K; a.\mathcal{P} \subseteq A\} .$$

Usando esta notação, temos o seguinte teorema:

Teorema A.1.4: Sejam A um domínio de Dedekind e $\mathbf{P}$ o conjunto dos ideais primos de A. Então todo ideal fracionário não nulo I de A se escreve de modo único na forma

$$I = \prod_{\mathcal{P} \in \mathbf{P}} \mathcal{P}^{n_{\mathcal{P}}(I)}$$

onde $n_{\mathcal{P}}(I) \in \mathbb{Z}$ para todo $\mathcal{P} \in \mathbf{P}$, e são quase sempre nulos.

Desse modo temos que todo ideal fracionário não nulo I de um domínio de Dedekind A é inversível. De fato, se

$$I = \prod_{\mathcal{P} \in \mathbf{P}} \mathcal{P}^{n_{\mathcal{P}}(I)}$$

então o ideal inverso de I é dado por

$$I^{-1} = \prod_{\mathcal{P} \in \mathbf{P}} \mathcal{P}^{-n_{\mathcal{P}}(I)} .$$

Demonstrações para os teoremas A.1.3 e A.1.4 podem ser encontradas em [15].

Agora vamos considerar a seguinte situação: seja A um domínio de Dedekind com $K = \mathrm{Cfr}(A)$ tal que $\mathrm{ch}(K) = 0$, e sejam ainda L uma extensão finita de K e B o fecho integral de A em L. Pelo teorema A.1.3, temos que B é um domínio de Dedekind, logo seus ideais podem ser decompostos em produtos de ideais primos de B. Em particular, se I é um ideal de A,

então $I.B$ é ideal de B e pode ser decomposto daquele modo. Os próximos teoremas nos fornecem informações mais precisas sobre essa decomposição.

Teorema A.1.5: Sob as hipóteses descritas acima, seja $\mathcal{P}$ um ideal primo não nulo de A. Então $\mathcal{P}.B$ é um ideal de B tal que

$$\mathcal{P}.B = \prod_{i=1}^{q} \mathcal{B}_i^{e_i}$$

onde para todo $1 \leq i \leq q$ temos $e_i \in \mathrm{N}$ os ideais $\mathcal{B}_i$ são os ideais primos I, distintos dois a dois, de B tais que $I \cap A = \mathcal{P}$.

Teorema A.1.6: Sob as mesmas hipóteses do teorema A.1.5, temos que $\frac{B}{\mathcal{B}_i}$ é um espaço vetorial de dimensão finita f_i sobre $\frac{A}{\mathcal{P}}$. Ou seja,

$$f_i = \left[\frac{B}{\mathcal{B}_i} : \frac{A}{\mathcal{P}}\right] .$$

Teorema A.1.7: Sob as mesmas hipóteses e notações precedentes temos que

$$\left[\frac{B}{\mathcal{P}B} : \frac{A}{\mathcal{P}}\right] = \sum_{i=1}^{q} e_i f_i .$$

Consideremos então a seguinte situação:
Seja $B|A$ uma extensão de anéis tal que B é um A-módulo livre de posto n, e seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base livre de $B|A$. Para cada $b \in B$ considere a aplicação A-linear

$$\begin{aligned} m_b : \quad & B \to B \\ & \mathsf{y} \mapsto b.\mathsf{y} \end{aligned}$$

e tome $M_b = (a_{ij})$ a matriz dada por

$$m_b(\alpha_i) = \sum_{j=1}^{n} a_{ij}\alpha_j .$$

Sabemos que o traço da matriz M independe da escolha da base livre $\{\alpha_1, \cdots, \alpha_n\}$ e então podemos definir: se $b \in B$, chamamos o traço de b ao traço da matriz M_b, e denotaremos por $\mathrm{Tr}_{B|A}(b)$.

Definição A.1.8: Sejam $B|A$ uma extensão de anéis tal que B é um A-módulo livre de posto n e $(b_1, \cdots, b_n) \in B^n$. Chamamos de discriminante de $(b_1, \cdots, b_n)$ sobre A ao elemento definido por

$$d_{B|A}(b_1, \cdots, b_n) = \det\left(\mathrm{Tr}_{B|A}(b_i b_j)\right) \in A$$

Teorema A.1.9: Se $(\mathsf{y}_1, \cdots, \mathsf{y}_n) \in B^n$ é tal que para cada $1 \leq i \leq n$,

$$\mathsf{y}_i = \sum_{j=1}^{n} a_{ij} b_j \ ,$$

onde $a_{ij} \in A$ e $b_j \in B$ para todo $1 \leq j \leq n$, então

$$d_{B|A}(\mathsf{y}_1, \cdots, \mathsf{y}_n) = \det(a_{ij})^2 d_{B|A}(b_1, \cdots, b_n) \ .$$

Segue diretamente deste teorema que os discriminantes das bases de B sobre A são associados dois a dois. Em particular, se $A = \mathbf{Z}$ e B é o anel de inteiros de um corpo numérico, então o discriminante é sempre igual.

Definição A.1.10: Sejam $L|K$ uma extensão de corpos de grau n, A um subanel integralmente fechado de K tal que $\mathrm{Cfr}(A) = K$ e B o fecho integral de A em L. Chamamos o ideal discriminante de $B|A$ ao ideal de A gerado pelos discriminantes das bases de L sobre K que estão contidas em B, que denotaremos por $D_{B|A}$.

Observação: Pelo que foi comentado acima, se B é um A-módulo livre então

$D_{B|A}$ é um ideal principal.

Agora, voltando à situação do teorema A.1.5, dizemos que um ideal primo $\mathcal{P}$ de A se ramifica em B se existe $1 \leq i \leq n$ tal que $e_i \geq 2$.

Teorema A.1.11: Um ideal primo $\mathcal{P}$ de A se ramifica em B se, e somente se, $D_{B|A} \subseteq \mathcal{P}$.

Concluímos então que existe apenas um número finito de ideais primos de A que se ramificam em B, uma vez que A é um domínio de Dedekind. As demonstrações dos teoremas A.1.5 a A.1.11 podem ser encontradas em [15].

O próximo teorema é de grande utilidade para nós. sendo sua demonstração devida a Dedekind podendo ser encontrada em [10], à página 27.

Teorema A.1.12: Seja A um domínio de Dedekind com $K = \mathrm{Cfr}(A)$ tal que $ch(K) = 0$. Sejam L uma extensão finita de K e B o fecho integral de A em L, e suponha que $B = A[\alpha]$ para alguma $\alpha \in B$. Seja $\mathcal{P}$ um ideal primo não nulo de A e sejam $f(\mathsf{x})$ o polinômio mínimo de α sobre K e $\overline{f}(\mathsf{x})$ a redução de $f(\mathsf{x})$ ao quociente $\frac{A}{\mathcal{P}}$. Suponha

$$\overline{f}(\mathsf{x}) = \overline{f}_1(\mathsf{x})^{e_1} \cdots \overline{f}_r(\mathsf{x})^{e_r}$$

a fatoração de $\overline{f}(\mathsf{x})$ em fatores irredutíveis sobre $\frac{A}{\mathcal{P}}$ com coeficientes líderes 1. Então

$$\mathcal{P}.B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$$

é a decomposição de $\mathcal{P}$ em B, e temos

$$\mathcal{P}_i = \mathcal{P}.B + f_i(\alpha).B$$

onde $f_i(\mathsf{x}) \in A[\mathsf{x}]$ é um polinômio com coeficiente líder 1 cuja redução módulo $\mathcal{P}$ é $\overline{f}_i(\mathsf{x})$. Além disso,

$$\left[\frac{B}{\mathcal{P}_i} : \frac{A}{\mathcal{P}}\right] = \partial f_i(\mathsf{x}) .$$

Outra propriedade interessante dos domínios de Dedekind é dada pelo seguinte teorema:

Teorema A.1.13: Sejam A um domínio de Dedekind e I um ideal de A. Então dado $i \in I$ existe $a_i \in A$ tal que

$$I = (i, a_i) .$$

Um bom exemplo de um domínio de Dedekind é o anel de inteiros de um corpo numérico, que vamos estudar um pouco a partir de agora.

Definição A.1.14: Um corpo K é dito um corpo numérico, ou corpo de números algébricos, se é uma extensão finita de $\mathbf{Q}$, isto é, $[K : \mathbf{Q}] < \infty$.

Definição A.1.15: Seja K um corpo numérico. Dizemos que $a \in K$ é um inteiro de K se a é inteiro sobre $\mathbf{Z}$, isto é, se a é raiz de um polinômio mônico em $\mathbf{Z}$ [x].

Claramente o conjunto dos inteiros de um corpo numérico K é um anel, que chamaremos o anel de inteiros de K. Este anel, que vamos denotar por A, é um domínio de Dedekind, como podemos ver pelo teorema A.1.3.

Segue ainda do teorema A.1.3 que o anel de inteiros A de um corpo numérico K é um $\mathbf{Z}$ -módulo livre de posto $[K : \mathbf{Q}]$. Assim, pela teoria sobre discriminantes vista anteriormente, os discriminantes de todas as bases do $\mathbf{Z}$ -módulo A são iguais, e chamamos este valor comum de discriminante absoluto de K. Mais detalhes sobre este assunto podem ser encontrados em [15] e [10].

Ainda considerando K um corpo numérico com anel de inteiros A, tem-se no capítulo 3 de [15] que se I é um ideal não nulo de A então o anel $\frac{A}{I}$ é finito. Assim a definição seguinte faz sentido:

Definição A.1.16: Dado um ideal não nulo I de A, definimos a norma do ideal I, e denotamos por $N(I)$, como sendo a cardinalidade do anel $\frac{A}{I}$.

Agora vamos relembrar alguns resultados sobre corpos quadráticos, que são corpos numéricos tais que $[K : \mathbb{Q}] = 2$. Sabemos que se K é um corpo quadrático então é da forma

$$K = \mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n}; a, b \in \mathbb{Q}\}$$

onde n é um número inteiro livre de quadrados. O próximo teorema mostra como determinar o anel de inteiros de K através do inteiro n. Sua demonstração pode ser vista em [15] ou [5].

Teorema A.1.17: Seja $K = \mathbb{Q}(\sqrt{n})$ um corpo quadrático, onde n é um número inteiro livre de quadrados, logo $n \not\equiv 0 \pmod 4$.

(a) Se $n \equiv 2$ ou $n \equiv 3 \pmod 4$ então o anel de inteiros de K é dado por

$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n}; a, b \in \mathbb{Z}\}.$$

(b) Se $n \equiv 1 \pmod 4$ então o anel de inteiros de K é dado por

$$\begin{aligned} A &= \left\{ \frac{u + v\sqrt{n}}{2}; u, v \in \mathbb{Z} \text{ e têm a mesma paridade} \right\} \\ &= \mathbb{Z}\left[\frac{-1+\sqrt{n}}{2}\right]. \end{aligned}$$

Através do inteiro n podemos também calcular facilmente o discriminante

absoluto de K, como mostra o próximo teorema.

Teorema A.1.18: Seja $K = \mathbb{Q}(\sqrt{n})$ um corpo quadrático, onde n é inteiro livre de quadrados. Se d é o discriminante absoluto de K temos

(a) se $n \equiv 2$ ou $n \equiv 3 \pmod 4$ então $d = 4n$;

(b) se $n \equiv 1 \pmod 4$ então $d = n$.

Indicamos [15] como referência para mais detalhes.
Agora adotando a notação

$$\xi = \begin{cases} \sqrt{n}, \text{ se } n \not\equiv 1 \pmod 4 \\ \frac{\sqrt{n}-1}{2}, \text{ se } n \equiv 1 \pmod 4 \end{cases}$$

podemos provar que todo ideal I do anel de inteiros A de $K = \mathbb{Q}(\sqrt{n})$ é da forma

$$I = (kv, v(u + \xi))$$

onde $k, v, u \in \mathbf{Z}$, $v > 0$, $k > 0$ e são tais que $k/N(u + \xi)$,onde N denota a norma. Além disso, podemos escolher u tal que $0 \leq u < k$. Desse modo, se d é o discriminante absoluto de K, então temos o seguinte teorema sobre ramificação de primos em A.

Teorema A.1.19: Sejam $p \in \mathbf{Z}$ um número primo e $\mathcal{P} = (kv, v(u + \xi))$ um ideal primo de A tal que $\mathcal{P} \cap \mathbf{Z} = p\mathbf{Z}$. Então $\mathcal{P}$ satisfaz uma das três condições:

(a) Se p/d então $\mathcal{P} = \overline{\mathcal{P}}$. Nesse caso

$$\mathcal{P} = (p, u + \xi)$$

e $$pA = \mathcal{P}^2 .$$

(b) $pA = \mathcal{P}$ se, e somente se, $p = 2$ e $n \equiv 5 \pmod 8$ ou p é ímpar e a equação $x^2 \equiv n \pmod p$ não tem solução (segue dessas condições que p não divide d).

(c) $\mathcal{P} \neq \overline{\mathcal{P}}$ se, e somente se, $p = 2$ e $n \equiv 1 \pmod 8$ ou p é ímpar, p não divide d e a equação $x^2 \equiv n \pmod p$ tem solução. Neste caso

$$\mathcal{P} = (p, u + \xi)$$

e $$pA = \mathcal{P}\overline{\mathcal{P}} \ .$$

Esse teorema nos fornece uma maneira prática de decidir se um ideal primo de $\mathbb{Z}$ se ramifica em A.

A.2 Localização

Definição A.2.1: Sejam A um anel e S um subconjunto de A. Dizemos que S é um sistema multiplicativo de A se satisfaz

(a) $1 \in S$;

(b) quaisquer que sejam $x, y \in S$, o produto $x.y$ ainda pertence a S;

(c) $0 \notin S$.

Definição A.2.2: Sejam A um domínio com $K = \mathrm{Cfr}(A)$, e S um sistema multiplicativo de A. Definimos então a localização de A por S, que denotamos por $S^{-1}A$, como sendo o subanel de K que contém A

$$S^{-1}A = \left\{ \frac{a}{s} \in K; a \in A \ \text{e} \ s \in S \right\} .$$

Observe que se A é um anel e $\mathcal{P}$ é um ideal primo de A então $S = A\backslash\mathcal{P}$ é um sistema multiplicativo de A. Neste caso podemos então considerar o anel $S^{-1}A$, que vamos denotar por $A_{\mathcal{P}}$. Além disso, o anel $A_{\mathcal{P}}$ é um anel local com ideal maximal $M_{\mathcal{P}} = \mathcal{P}.A_{\mathcal{P}}$.

Teorema A.2.3: Sejam A um anel, S um sistema multiplicativo de A e I um ideal de $S^{-1}A$. Então

$$I = S^{-1}(I \cap A) .$$

Desse modo vemos que todo ideal de $S^{-1}A$ é da forma $S^{-1}.J$, onde J é ideal de A. Note ainda que um ideal não nulo $S^{-1}J$ de $S^{-1}A$ é próprio se, e somente se, $J \cap S = \phi$.

Teorema A.2.4: Sejam A um anel e S um sistema multiplicativo de A. Então temos

(a) se A é Noetheriano, então $S^{-1}A$ também é Noetheriano;

(b) se A é domínio de Dedekind então $S^{-1}A$ ainda é domínio de Dedekind.

Teorema A.2.5: Sejam A um domínio com $K = \mathrm{Cfr}(A)$, S um sistema multiplicativo de A, B um domínio contendo A com $L = \mathrm{Cfr}(B) \supseteq K$. Então podemos considerar

$$S^{-1}A \subseteq S^{-1}B$$

e ainda se $B|A$ é uma extensão integral então $S^{-1}B|S^{-1}A$ é também uma extensão integral.

As demonstrações destes resultados podem ser encontradas em [10].

O próximo teorema nos dá um resultado importante utilizado no capítulo 2.

Teorema A.2.6: Sejam A um domínio de Dedekind com $K = \mathrm{Cfr}(A)$, L uma extensão finita de K tal que $L = K(\alpha)$ para algum $\alpha \in B$, onde B é o fecho integral de A em L. Então temos que $B_{\mathcal{P}} = A_{\mathcal{P}}[\alpha]$ para todo ideal primo $\mathcal{P}$ de A exceto para um número finito.

Demonstração:

Como a extensão $L|K$ é finita, temos que B é um A-módulo finitamente gerado, isto é,

$$B = Ab_1 + \cdots + Ab_n$$

onde $b_1, \cdots, b_n \in B$. Considerando o anel $A[\alpha]$ temos que $A \subseteq A[\alpha] \subseteq B$. Assim, tomando

$$I = \{\mathrm{x} \in A[\alpha]; \mathrm{x}B \subseteq A[\alpha]\}$$

temos que $I \neq (0)$. De fato, para cada $1 \leq i \leq n$, temos que $b_i \in B \subseteq L = K(\alpha)$, logo podemos escrever

$$b_i = \frac{a_m}{c_i}\alpha^m + \cdots + \frac{a_1}{c_i}\alpha + \frac{a_0}{c_i}$$

onde $a_0, \cdots, a_m, c_i \in A$ e $c_i \neq 0$ para todo $1 \leq i \leq n$. Daí temos que

$$c_i b_i = a_m\alpha^m + \cdots + a_1\alpha + a_0 \in A[\alpha]$$

para todo $1 \leq i \leq n$. Tomando então $c = \prod_{i=1}^{n} c_i$ temos que $c \neq 0$ e $c \in I$, donde $I \neq (0)$.

Observamos ainda que I é ideal de B e de $A[\alpha]$. Assim se consideramos

$$J = I \cap A$$

temos que J é ideal não nulo de A, já que I é ideal não nulo de B. Mas A é domínio de Dedekind, logo existe apenas um número finito de ideais primos de A que contêm J, digamos $\mathcal{P}_1, \cdots, \mathcal{P}_m$. Desta forma, se tomamos $\mathcal{P}$ um ideal primo de A qualquer tal que

$$\mathcal{P} \notin \{\mathcal{P}_1, \cdots, \mathcal{P}_m\}$$

então temos que

$$A_{\mathcal{P}}[\alpha] \subseteq B_{\mathcal{P}}$$

uma vez que $A[\alpha] \subseteq B$. Por outro lado, pela escolha de $\mathcal{P}$, temos que $J \nsubseteq \mathcal{P}$. Logo existe $a \in J$ tal que $a \notin \mathcal{P}$. Agora como $a \in J = I \cap A$, segue que

$$aB \subseteq A[\alpha]$$

donde

$$aB_{\mathcal{P}} \subseteq A_{\mathcal{P}}[\alpha] \, .$$

Mas $a \notin \mathcal{P}$, logo a é uma unidade em $A_{\mathcal{P}}$ e $B_{\mathcal{P}}$ e, portanto

$$B_{\mathcal{P}} \subseteq A_{\mathcal{P}}[\alpha] \, .$$

Concluímos que $B_{\mathcal{P}} = A_{\mathcal{P}}[\alpha]$ para todo ideal primo $\mathcal{P}$ de A, exceto para um número finito. ■

A.3 Anéis de Valorização e Valores Absolutos não Archimedianos

Neste parágrafo vamos colocar alguns resultados básicos da teoria de anéis de valorização e valores absolutos não Archimedianos. Para um texto

mais detalhado recomendamos [1].

Definição A.3.1: Sejam K um corpo e $V \subseteq K$ um domínio. Dizemos que V é um anel de valorização de K se para todo $a \in K$ temos

$$a \in V \quad \text{ou} \quad a^{-1} \in V \ .$$

O próximo teorema é um resultado clássico, que nos dá formas equivalentes de se definir um anel de valorização no caso em que V é domínio e $K = \text{Cfr}(V)$.

Teorema A.3.2: Sejam V um domínio e $K = \text{Cfr}(V)$. São equivalentes:

(1) V é anel de valorização de K;

(2) se I e J são ideais de V, então $I \subseteq J$ ou $J \subseteq I$;

(3) se I e J são ideais finitamente gerados de V, então $I \subseteq J$ ou $J \subseteq I$;

(4) se $I = (a_1, \cdots, a_n)$ é um ideal finitamente gerado de V, então existe i, $1 \leq i \leq n$, tal que $I = (a_i)$.

Uma conseqüência imediata deste teorema é o fato de que todo anel de valorização V de K, onde $K = \text{Cfr}(V)$, é um anel local cujo único ideal maximal $\mathcal{M}_V$ é dado por

$$\mathcal{M}_V = \{a \in K; a = 0 \ \text{ ou } \ a^{-1} \notin V\} \ .$$

Definição A.3.3: Sejam K um corpo e $v : K - \{0\} \to G$, onde G é um grupo abeliano totalmente ordenado, uma função. Dizemos que v é uma valorização de K se satisfaz

(a) $v(a.b) = v(a) + v(b)$;

(b) $v(a + b) \geq \min\{v(a), v(b)\}$;

para todo $a, b \in K - \{0\}$.

Observamos que se K é um corpo e v é uma valorização de K então o conjunto

$$V = \{a \in K; a = 0 \text{ ou } v(a) \geq 0\}$$

é um anel de valorização de K cujo ideal maximal é dado por

$$\mathcal{M}_V = \{a \in K; a = 0 \text{ ou } v(a) > 0\}$$

uma vez que se $a \in K$ então $v(a) = 0$ se, e somente se, $a, a^{-1} \in V$. Neste caso dizemos que V é o anel de valorização associado à valorização v.

Na definição A.3.3, no caso em que $G = \mathbf{Z}$ dizemos que $v : K - \{0\} \to \mathbf{Z}$ é uma valorização discreta de K. É fácil mostrar que neste caso o anel de valorização associado a V é Noetheriano, o que nos leva à seguinte definição:

Definição A.3.4: Seja V um domínio de valorização de $K = \text{Cfr}(V)$. Dizemos que V é um anel de valorização discreta se V é Noetheriano.

Segue diretamente do teorema A.3.2 que se V é um anel de valorização de $K = \text{Cfr}(V)$ então V é anel de valorização discreta se, e somente se, V é domínio principal. Desse modo, se V é anel de valorização discreta com ideal maximal $\mathcal{M}_V$, então temos

$$\mathcal{M}_V = \pi.V$$

onde $\pi \in V$ é irredutível em V. Logo todo elemento $a \in V \backslash \{0\}$ pode ser escrito na forma

$$a = \pi^n.\mu$$

onde μ é uma unidade de V e $n \in \text{N}$.

É possível mostrar também que V é um anel de valorização discreta se, e somente se, existir uma valorização de $K = \text{Cfr}(V)$ sobrejetora, $v : K - \{0\} \to \mathbf{Z}$, tal que V é o anel de valorização associado a v.

A ligação entre anéis de valorização discreta e domínios de Dedekind vem da seguinte caracterização de tais domínios(ver [1]):

Teorema A.3.5: Se D é um domínio Noetheriano, então são equivalentes:

(1) D é domínio de Dedekind;

(2) para todo ideal primo não nulo $\mathcal{P}$ de D, o anel $D_{\mathcal{P}}$ é domínio de valorização discreta.

Assim, dados um domínio de Dedekind A e $\mathcal{P}$ um ideal primo não nulo de A, temos uma valorização discreta $v_{\mathcal{P}} : K - \{0\} \to \mathbf{Z}$, onde $K = \mathrm{Cfr}(A)$, chamada valorização $\mathcal{P}$-ádica, cujo anel de valorização associado é $A_{\mathcal{P}}$. Na verdade $v_{\mathcal{P}}$ é dada por

$$v_{\mathcal{P}}(a) = n$$

onde $a = \pi^n.\mu \in A_{\mathcal{P}}$, $\mathcal{P}.A_{\mathcal{P}} = \pi.A_{\mathcal{P}}$ é o ideal maximal de $A_{\mathcal{P}}$ e μ é unidade de $A_{\mathcal{P}}$.

Observe que a partir dessa valorização podemos definir uma função

$$\begin{aligned} |\ |_{\mathcal{P}} : \quad & K \to \mathbb{R} \\ & a \mapsto e^{-v_{\mathcal{P}}(a)} \end{aligned}$$

que possui as propriedades de um valor absoluto não Archimediano. Temos então a definição:

Definição A.3.6: Dado um corpo K, um valor absoluto não Archimediano sobre K é uma função

$$|\ | : K \to \mathbb{R}$$

que satisfaz

(1) $|a| \geq 0$ e $|a| = 0$ se, e só se, $a = 0$,

(2) $|a.b| = |a|.|b|$,

(3) $|a+b| \leq \max\{|a|,|b|\}$.

Observação: Dado um corpo K, o valor absoluto $|\ |: K \to \mathbb{R}$ dado por

$$|a| = \begin{cases} 0, \text{ se } a = 0 \\ 1, \text{ se } a \neq 0 \end{cases}$$

é chamado valor absoluto trivial.

É importante notar que dado um valor absoluto não Archimediano $|\ |$ sobre um corpo K, então ele induz uma métrica (chamada de ultra-métrica) sobre K dada por

$$d(a,b) = |a-b|$$

quaisquer que sejam $a, b \in K$.

Teorema A.3.7: Seja K um corpo com valor absoluto não Archimediano $|\ |$. Então temos

(a) se $a, b \in K$ e $|a| < |b|$, então $|a+b| = |b|$;

(b) $V = \{a \in K; |a| \leq 1\}$ é um anel de valorização de K cujo ideal maximal é $\mathcal{P} = \{a \in K; |a| < 1\}$. Tal V é chamado anel de valorização associado a $|\ |$.

(c) A função $v: K - \{0\} \to \mathbb{R}$ dada por $v(a) = -\ln|a|$ satisfaz

i. $v(ab) = v(a) + v(b)$;

ii. $v(a+b) \geq \min\{v(a), v(b)\}$;

iii. Se $v(a) < v(b)$, então $v(a+b) = v(a)$;

iv. $V = \{a \in K; v(a) \geq 0\}$.

Para a demonstração deste teorema veja [1]. Observe que a parte (c) do teorema tem uma recíproca óbvia, a saber:

Se K é um corpo e $v : K - \{0\} \to \mathbb{R}$ é uma valorização de K, então a função $|\ |_v : K \to \mathbb{R}$ dada por

$$|a|_v = \begin{cases} 0, \text{ se } a = 0 \\ e^{-v(a)}, \text{ se } a \neq 0 \end{cases}$$

é um valor absoluto não Archimediano de K.

Definição A.3.8: Dizemos que um corpo K com um valor absoluto não Archimediano $|\ |$ é completo se ele for completo em relação à topologia dada pela ultra-métrica induzida por $|\ |$.

Definição A.3.9: Sejam $K_1, |\ |_1, K_2, |\ |_2$ dois corpos com seus respectivos valores absolutos não Archimedianos e $\varphi : K_1 \to K_2$ um isomorfismo de corpos. Dizemos que φ é uma isometria se, para todo $a \in K_1$, temos

$$|\varphi(a)|_2 = |a|_1 .$$

Neste caso dizemos que K_1 e K_2 são isométricos.

Teorema A.3.10: Seja K um corpo com valor absoluto não Archimediano $|\ |$. Então existe um único corpo completo K' (a menos de isometria) com valor absoluto não Archimediano $|\ |'$, que é uma extensão de K e que satisfaz

(a) para todo $a \in K$, $|a| = |a|'$;

(b) K é denso em K'.

Tal corpo é chamado o completamento de K em relação a $|\ |$ e denotado por $\overline{K}$.

Para uma demonstração deste teorema veja [1].

O próximo resultado nos dá uma propriedade fundamental do completa-

mento de um corpo com relação a um valor absoluto não Archimediano.

Teorema A.3.11: Sejam K um corpo com valor absoluto não Archimediano, V seu anel de valorização associado, $(\overline{K}, |\ |)$ o seu completamento e $\overline{V}$ o fecho de V em $\overline{K}$. Então temos que

$$\overline{V} = \{a \in \overline{K}; |a| \leq 1\} ,$$

i.e., $\overline{V}$ é o anel de valorização associado a $(\overline{K}, |\ \ |)$. Mais ainda, o ideal maximal de $\overline{V}$ é o fecho em $\overline{K}$ do ideal maximal de V.

Demonstração:

Basta observar que se $a \in \overline{K}$, $a \neq 0$ e $a = \lim_{n\to\infty} a_n$, onde $a_n \in V$ para todo $n \in \mathbb{N}$. Então existe $n_0 \in \mathbb{N}$ tal que, para todo $n \geq n_0$ temos $|a_n| = |a|$. ■

Considere agora A um domínio de Dedekind com corpo de frações K e $\mathcal{P}$ um ideal primo não nulo de A. Como vimos anteriormente, temos então definida uma valorização sobre K, chamada valorização $\mathcal{P}$-ádica, a partir da qual podemos definir o valor absoluto $\mathcal{P}$-ádico $|\ |_{\mathcal{P}} : K \to \mathbb{R}$ dado por

$$|a|_{\mathcal{P}} = \begin{cases} 0, \text{ se } a = 0 \\ e^{-n}, \text{ se } a \neq 0 \end{cases}$$

onde $a \in K$ e $n = v_{\mathcal{P}}(a)$. É simples mostrar que $|\ |_{\mathcal{P}}$ é um valor absoluto não Archimediano cujo anel de valorização associado é $A_{\mathcal{P}}$.

Definição A.3.12: Sejam A um domínio de Dedekind com corpo de frações K e $\mathcal{P}$ um ideal primo não nulo de A. Chamamos de completamento $\mathcal{P}$-ádico de K e denotamos por $\overline{K}_{\mathcal{P}}$, o completamento de $(K, |\ |_{\mathcal{P}})$. Denotamos ainda por $\overline{A}_{\mathcal{P}}$ o fecho de A em $\overline{K}_{\mathcal{P}}$ e por $|\ \ |_{\mathcal{P}}$ também o valor absoluto não

Archimediano de $\overline{K}_{\mathcal{P}}$.

Lema A.3.13: Nas condições descritas acima temos que o fecho de A em $(K, |\ |_{\mathcal{P}})$ é $A_{\mathcal{P}}$.

Demonstração:

Dado $\frac{a}{s} \in A_{\mathcal{P}}$, onde $a \in A$ e $s \in A \backslash \mathcal{P}$, temos que para todo $n \in \mathbf{N}$, $As + \mathcal{P}^n = A$. Assim existem, para todo $n \in \mathbf{N}$, $t_n \in A$ e $p_n \in \mathcal{P}^n$ tais que

$$1 = t_n s + p_n \ ,$$

donde

$$|a - t_n.s.a|_{\mathcal{P}} \leq \frac{1}{e^n} \ .$$

Segue então que

$$\frac{a}{s} = \lim_{n \to \infty} t_n.a$$

uma vez que $|s|_{\mathcal{P}} = 1$.

Por outro lado, $A_{\mathcal{P}}$ é fechado em $(K, |\ |_{\mathcal{P}})$ já que $|\ |_{\mathcal{P}}$ é contínua e $A_{\mathcal{P}} = \{\alpha \in K; |\alpha|_{\mathcal{P}} \leq 1\}$. Portanto concluímos que o fecho de A em $(K, |\ |_{\mathcal{P}})$ é $A_{\mathcal{P}}$. ■

Teorema A.3.14: Nas condições da definição A.3.12 temos que

$$\overline{A}_{\mathcal{P}} = \{\alpha \in \overline{K}_{\mathcal{P}}; |\alpha|_{\mathcal{P}} \leq 1\} \ ,$$

isto é, $\overline{A}_{\mathcal{P}}$ é o anel de valorização de $\overline{K}_{\mathcal{P}}$ associado ao valor absoluto $|\ |_{\mathcal{P}}$.

Demonstração: Pelo lema A.3.13, o fecho de A em $(K, |\ |_{\mathcal{P}})$ é $A_{\mathcal{P}}$, que é o anel de valorização associado a $|\ |_{\mathcal{P}}$. Agora, pelo teorema A.3.11, temos que o fecho de $A_{\mathcal{P}}$ em $\overline{K}_{\mathcal{P}}$ é o conjunto dado por $\{a \in \overline{K}_{\mathcal{P}}; |a|_{\mathcal{P}} \leq 1\}$. Assim temos que

$$\overline{A}_{\mathcal{P}} = \{a \in \overline{K}_{\mathcal{P}}; |a|_{\mathcal{P}} \leq 1\} \ ,$$

como queríamos demonstrar. ■

Teorema A.3.15: $\overline{A}_{\mathcal{P}}$ é compacto na topologia $\mathcal{P}$-ádica.

Para demonstração vide [10], página 46.

O próximo resultado é conhecido como método de Newton em corpos completos, sendo na verdade um caso particular do Lema de Hensel.

Teorema A.3.16: Sejam $\overline{K}$ um corpo completo em relação a um valor absoluto não Archimediano $|\ |$, e V o anel de valorização associado a $(\overline{K}, |\ |)$. Se $f(\mathsf{x}) \in V[\mathsf{x}]$ é um polinômio mônico e $\alpha_1 \in V$ é tal que

$$|f(\alpha_1)| < 1 \quad \text{e} \quad |f'(\alpha_1)| = 1$$

então a seqüência dada por

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}$$

para todo $n > 1$, converge para um $\alpha \in V$ tal que $f(\alpha) = 0$.

Demonstrações destes últimos teoremas podem ser encontradas em [1] e [10].

A.4 Domínios de Prüfer

Neste parágrafo apresentamos um resultado sobre domínios de Prüfer, que é utilizado no capítulo 2.

Definição A.4.1: Um domínio D é dito um domínio de Prüfer se todo ideal não nulo finitamente gerado de D é inversível.

Para mostrar o próximo resultado, vamos precisar de um lema auxiliar

sobre domínios locais.

Lema A.4.2: Todo ideal inversível I em um domínio local D é principal.

Demonstração:

Seja D um domínio local com $K = \mathrm{Cfr}(D)$, e seja M seu único ideal maximal. Seja I um ideal inversível de D. Então existe um ideal fracionário J de D , a saber, $J = \{\mathsf{x} \in K; \mathsf{x}I \subseteq D\}$, tal que

$$I.J = D \ .$$

Logo existem $n \in \mathrm{N}$ e $a_1, \cdots, a_n \in I$, $b_1, \cdots, b_n \in J$ tais que

$$1 = \sum_{i=1}^{n} a_i b_i \ .$$

Agora, se para todo $1 \leq i \leq n$, $a_i b_i$ não fosse unidade de D, então teríamos, uma vez que M é o conjunto das não unidades de D,

$$R = (\sum_{i=1}^{n} a_i b_i) \subseteq M$$

o que contraria a maximalidade de M. Logo existe $i_0 \in \mathrm{N}$, $1 \leq i_0 \leq n$, tal que $a_{i_0} b_{i_0}$ é unidade de D, isto é, $(a_{i_0} b_{i_0})^{-1} \in D$.

Assim, se $a \in I$ então temos

$$\begin{aligned} a &= a(\textstyle\sum_{i=1}^{n} a_i b_i) = \sum_{i=1}^{n} a a_i b_i = \\ &= \sum_{i=1}^{n} a a_i b_i (a_{i_0} b_{i_0})(a_{i_0} b_{i_0})^{-1} = \\ &= a_{i_0}(\textstyle\sum_{i=1}^{n} a b_{i_0} a_i b_i (a_{i_0} b_{i_0})^{-1}) \end{aligned}$$

e $\{a b_{i_0}, a_1 b_1, \cdots, a_n b_n, (a_{i_0} b_{i_0})^{-1}\} \subseteq R$. Ou seja, $I = (a_{i_0})$ é ideal principal.

■

Teorema A.4.3: Seja D um domínio. Então D é um domínio de Prüfer se,

e somente se, D_M é domínio de valorização para todo ideal maximal M de D.

Demonstração:

Suponhamos que D é domínio de Prüfer e seja M um ideal maximal de D. Sabemos pelo teorema A.3.2 que D_M é domínio de valorização se, e somente se, todo ideal finitamente gerado de D_M é principal. Tomemos então J um ideal finitamente gerado de D_M e suponhamos

$$J = \left(\frac{a_1}{s_1}, \cdots, \frac{a_n}{s_n}\right)$$

onde $a_i, s_i \in D$ e $s_i \notin M$ para todo $1 \leq i \leq n$. Assim temos que $J = I_M$, onde $I = (a_1, \cdots, a_n)$ é o ideal de D gerado por $a_1, \cdots, a_n$. Agora M é ideal primo de D, logo D_M é um domínio local. Também temos por hipótese que I é inversível, donde I_M é inversível. Segue então , pelo lema A.4.2, que $J = I_M$ é ideal principal de D_M. Portanto D_M é domínio de valorização.

Reciprocamente, suponhamos agora que D_M é domínio de valorização para todo ideal maximal M de D. Tomemos I um ideal finitamente gerado e não nulo de D e suponhamos

$$I = (a_1, \cdots, a_n)$$

onde $a_i \in D$ para todo $1 \leq i \leq n$. Vamos mostrar que I é inversível. Consideremos $K = \mathrm{Cfr}(D)$ e o ideal fracionário de D

$$J = \{\mathrm{x} \in K; \mathrm{x}I \subseteq D\} .$$

Suponamos que $I.J \subset D$ estritamente. Então existe um ideal maximal M_0 de D tal que

$$I.J \subseteq M_0 .$$

Agora, por hipótese, D_{M_0} é um domínio de valorização, e como I é ideal de D finitamente gerado, segue pelo teorema A.3.2 que I_{M_0} é ideal principal de

D_{M_0}. Assim existem $a \in I - \{0\}$ e $s \in D - M_0$ tais que

$$I_{M_0} = \left(\frac{a}{s}\right) .$$

Então , como para cada $1 \leq i \leq n$temos $a_i \in I_{M_0}$, temos que para cada $1 \leq i \leq n$ existem $t_i, r_i \in D$ com $r_i \notin M_0$ tais que

$$a_i = \frac{t_i}{r_i}.\frac{a}{s} ,$$

ou seja,

$$r_i.s.a_i \in (a) .$$

Chamando $s_i = r_i.s$ para cada $1 \leq i \leq n$ e tomando

$$k = s_1 \cdots s_n$$

temos que para todo $1 \leq i \leq n$,

$$\frac{k}{a}.a_i = \frac{s_1 \cdots s_n}{a}.\frac{t_i a}{s_i} = s_1 \cdots s_{i-1} s_{i+1} \cdots t_i \in D$$

donde $\frac{k}{a} \in J$. Desse modo

$$k = \frac{k}{a}.a \in I.J \subseteq M_0$$

ou seja, $k \in M_0$. Logo existe $i_0, 1 \leq i_0 \leq n$, tal que

$$s_{i_0} \in M_0$$

donde segue que $s \in M_0$ ou $r_{i_0} \in M_0$, o que é um absurdo. Portanto devemos ter

$$I.J = D ,$$

ou seja, I é inversível e conseqüentemente D é um domínio de Prüfer. ■

Bibliografia

[1] G. Bachman. *Introduction to p-adic numbers and Valuation theory.* Academic Press, 1964.

[2] D. Brizolis. A Theorem on ideals in rings of integer-valued polynomials. *Comm.in Alg.*, 7(10):pp.1065–1077, 1979.

[3] D. Brizolis. Ideals in rings of integer-valued polynomials. *J. für Reine Ang. Math.*, 285:pp.28–52, 1976.

[4] D. Brizolis. Hilbert rings of integral-valued polynomials. *Comm.in Alg.*, 3(12):pp.1051–1081, 1975.

[5] O. Endler. *Teoria dos Números Algébricos.* IMPA, Rio de Janeiro, 1986.

[6] O. Endler. *Valuation Theory*, Springer, Berlin, 1972.

[7] R. Gilmer. *Multiplicative Ideal Theory*, Dekker, New York, 1972.

[8] R. Gilmer. Sets that determine integer-valued polynomials. *J.of Number Theory*, 33:pp.95–100, 1989.

[9] R. Gilmer, W. Heinzer, D. Lantz. The Noetherian property in rings of integer-valued polynomials. *Trans. of the American Society*, 338(1):pp.187–199, 1993.

[10] S. Lang. *Algebraic Number Theory.* Addison-Wesley, Massachusetts, 1970.

[11] D.L. McQuillan. On a theorem of R. Gilmer. *J. of Number Theory*, 39:pp.245–250, 1991.

[12] D.L. McQuillan. On the coefficients and values of polynomial rings. *Arch. Math.*, 30(1), 1978.

[13] A. Ostrowski. Ueber ganzwertige polynome in algebraischen zahlkörpern. *J. Reine Angew. Math.*, 149:pp.117–124, 1919.

[14] G. Polya. Ueber ganzwertige polynome in algebraischen zahlkörpern. *J. Reine Angew. Math.*, 149:pp.97–116, 1919.

[15] P. Samuel. *Teoría Algebraica de Números.* Omega, Barcelona, 1972.

[16] T. Skolem. Ein satz über ganzwertige polynome. *Norske Vid. Selsk. (Trondheim)*, 9:pp.111–113, 1936.