1150005305
IMECC
T/UNICAMP Si38e

ESTRUTURAS ALGÉBRICAS E SÉRIES FORMAIS

LUIZ VASCONCELOS DA SILVA

Este exemplar corresponde a redação final da tese defendida pelo Sr. Luiz Vasconcelos da Silva e aprovada pela Comissão Julgadora.

T. N. Viswanathan

Orientador:
Prof. Dr. TENKASI M. VISWANATHAN

Dissertação apresentada no Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas, como requisito parcial para obtenção do título de Mestre em Matemática.

DEZEMBRO/1983

T.M.
Si38i
IM/T483

I M E C C.
B I B L I O T E C A

Ao meu pai Josué;

À memória da minha mãe Clonice;

À minha esposa Luciene e

Ao meu filho Luiz.

BIBLIOTECA
IMECC

AGRADECIMENTOS

Ao Prof. Dr. Tenkasi M. Viswanathan pelos comentários que apresentou enriquecendo este trabalho;

Ao Prof. Dr. Antônio J. Engler pelo seu acompanhamento, ajudando-me a compreender vários pontos desta dissertação e pelas discussões que nos levaram ao segundo caminho para a estrutura do fecho algébrico de $k((T))$, mostrado no Capítulo IV;

Ao Prof. Dr. Nelo da Silva Allan pela sua importante colaboração nos meus estudos visando o Exame de Qualificação, quando orientou os seminários das diversas disciplinas que dele fizeram parte;

À minha esposa Luciene;

À Célia pelo bom trabalho de datilografia

e à CAPES pelo apoio financeiro.

ÍNDICE

INTRODUÇÃO..... 1

CAPÍTULO I - PRELIMINARES SOBRE CORPOS VALORIZADOS..... 6
1. Valorizações Discretas de Posto 1..... 6
2. Completamentos e Extensões de Valorizações..... 12
3. Completamento de Anel Local..... 25

CAPÍTULO II - CORPOS COMPLETOS E O TEOREMA DE REPRESENTAÇÃO 26

CAPÍTULO III - ESTRUTURA DE CORPOS COMPLETOS A RESPEITO DE VALORIZAÇÕES DISCRETAS..... 45

CAPÍTULO IV - O FECHO ALGÉBRICO DO CORPO DE SÉRIES FORMAIS K((T))..... 53

CAPÍTULO V - MÓDULOS FINITAMENTE GERADOS SOBRE O ANEL DE POLINÔMIOS k[X]..... 67

CAPÍTULO VI - MÓDULOS FINITAMENTE GERADOS SOBRE O ANEL DE SÉRIES FORMAIS $\mathbb{Z}_p[[X]]$..... 92
1. Teorema de Preparação de Weierstrass..... 94
2. Estrutura de Módulos Finitamente Gerados sobre $\mathbb{Z}_p[[X]]$.. 104

BIBLIOGRAFIA..... 148

INTRODUÇÃO

Este trabalho é um estudo sobre estruturas algébricas relacionadas com séries formais. Seu ponto crucial está no Capítulo VI, onde tratamos da estrutura de módulos finitamente gerados sobre o anel de séries formais $\mathbb{Z}_p[[X]]$ onde $\mathbb{Z}_p$ é o anel dos inteiros p-ádicos.

Esta tese também trata dos seguintes resultados: 1) No Capítulo III descrevemos a estrutura de um corpo valorizado completo a respeito de uma valorização discreta e tendo característica igual à característica do corpo de restos. A estrutura é a de um corpo de séries formais $\bar{k}((T))$; 2) No Capítulo IV descrevemos o fecho algébrico de um corpo de séries formais $k((T))$, onde k é algebricamente fechado e de característica 0. Toda extensão finita é também um corpo de séries formais! Para todo inteiro $n \geq 1$, existe apenas uma extensão de grau n. O grupo absoluto de Galois em questão é procíclico, sendo isomorfo a $\hat{\mathbb{Z}}$.

O resultado do Capítulo VI é o seguinte: Seja M um módulo finitamente gerado sobre o anel $\Lambda = \mathbb{Z}_p[[X]]$; onde p é um inteiro primo e $\mathbb{Z}_p$ é o anel dos inteiros p-ádicos. Diz-se que $f \in \Lambda$ é um polinômio distinguido se f é da forma $f = X + a_{n-1}X^{n-1} + \ldots + a_o \in \Lambda[X]$ onde p divide a_i, $\forall\, i = 0,1,\ldots,n-1$. Existem inteiros $r,s,t \geq 0$, $k_1,\ldots,k_s \geq 1$, polinômios distinguidos $f_1, f_2, \ldots, f_r$ e um homomorfismo $\theta : M \longrightarrow M'$ onde

$$M' = \Lambda^t \oplus \frac{\Lambda}{(f_1)} \oplus \ldots \oplus \frac{\Lambda}{(f_r)} \oplus \frac{\Lambda}{(p^{k_1})} \oplus \frac{\Lambda}{(p^{k_2})} \oplus \ldots \oplus \frac{\Lambda}{(p^{k_s})} \quad ,$$

tais que $\ker \theta$ e $\operatorname{coker} \theta$ são finitos. Assim o teorema de estrutura em questão não se trata de um isomorfismo, mas sim de um "pseudo-isomorfismo" ($\ker \theta$ e $\operatorname{coker} \theta$ são finitos).

A importância deste resultado de Iwasawa pode ser vista da seguinte maneira: Vamos supor que de fato M é um grupo de Galois $\mathrm{Gal}(L/k)$. Então $\ker \theta$ é um subgrupo finito de M e temos o seguinte quadro:

$$\text{finito} \left\{ \begin{array}{ll} L & (1) \\ & \\ F & \ker \theta \end{array} \right.$$

$$k \qquad M = \mathrm{Gal}\,(L/k) \ .$$

Se F é o subcorpo fixo por $\ker \theta$, então L/F é uma extensão finita e F/k é uma extensão Galoisiana tendo $\theta(M)$ como grupo de Galois e $\theta(M)$ é um submódulo de índice finito em M'. Do ponto de vista da Teoria de Galois o que interessa é a extensão infinita F/k. Nesta situação então o resultado atende perfeitamente ao objetivo de descrever M.

Iwasawa considerou uma $\mathbb{Z}_p$-extensão de um corpo de números algébricos k, isto é, uma extensão Galoisiana L/k cujo grupo

de Galois é isomorfo ao grupo aditivo $\mathbb{Z}_p$. Como $\mathbb{Z}_p \supset (p) \supset (p^2) \supset \ldots \supset (p^n) \supset \ldots$ temos uma cadeia ascendente de corpos $k = k_o \subset k_1 \subset \ldots \subset k_n \ldots$ sendo k_n o subcorpo fixo por (p^n) (isto é, pelo subgrupo isomorfo a (p^n)). Seja C_n o p-Sylow subgrupo do grupo das classes de k_n. Temos homomorfismos naturais $C_{n+1} \longrightarrow C_n$ e isto define $C = \lim_{\leftarrow} C_n$. Um Teorema de Iwasawa descreve a cardinalidade de C_n e esta conclusão decorre do fato de que C é um $\mathbb{Z}_p[[X]]$-módulo finitamente gerado.

Não chegamos a demonstrar esses resultados sobre grupos de classes. O Teorema 3 do Capítulo VI trata da estrutura dos A-módulos finitamente gerados. A nossa abordagem segue a de Lang [6], que é matricial. O módulo M é descrito por geradores e relações, e os coeficientes dessas relações dão origem a uma matriz $m \times n$ que chamamos matriz de relações. A nossa finalidade é mudar esta matriz sucessivamente via operações admissíveis - por exemplo, permutar linhas ou colunas, multiplicar uma linha por elementos unidades, etc. - para conseguir uma matriz diagonal de relações.

Para esclarecer o papel dessas mudanças de matrizes, proporcionamos no Capítulo V a estrutura de módulos finitamente gerados sobre o anel de polinômios $k[X]$. A prova é matricial e traz de modo claro o significado de efetuar uma operação elementar sobre a matriz para o módulo em questão. O resultado do Capítulo V é bem conhecido, no entanto não encontrei um livro que abordasse o assunto via matrizes. A inclusão desse resultado nesta tese foi

motivada pela orientação que fornece para a demonstração do principal teorema do Capítulo VI.

No Capítulo IV tratamos do fecho algébrico do corpo de séries formais conforme segundo parágrafo. Esse resultado é mostrado de duas maneiras: a primeira, usando teoria de ramificação e, a segunda, mais elementar, usando o fato de que se L/K é uma extensão totalmente ramificada e $\text{car } \bar{K} = 0$ ou $\text{car } \bar{K}$ não divide e (índice de ramificação da extensão L/K) então $L = K(\sqrt[e]{\pi})$ onde π é um elemento primo de K.

O Capítulo III, onde desenvolvemos a estrutura de um corpo completo com respeito a uma valorização discreta, usa o Teorema de Representação do Capítulo II que afirma o seguinte: Seja A um anel de valorização discreta completo cujo corpo de frações é K. Se S é um conjunto de representantes do corpo de restos $\bar{K}$ em A e π é um elemento primo de A, então todo elemento $a \in A$ pode ser escrito de modo único como uma série convergente $a = \sum_{n=0}^{\infty} s_n \pi^n$ com $s_n \in S$. Analogamente, todo elemento $x \in K$ pode ser escrito como $x = \sum_{n=r}^{\infty} s_n \pi^n$ onde $v(x) = r = \min \{n \in \mathbb{Z};$ $s_n \neq 0\}$.

Esse teorema dá condições para uma boa compreensão do fecho algébrico do corpo $k((T))$.

As definições e os resultados importantes necessários para o desenvolvimento do exposto acima estão relacionados no Capítulo I.

Cabe mencionar que a demonstração do Teorema 3 do Capítulo VI contém elementos novos e simplifica de maneira substancial a prova desse mesmo resultado em Lang [6] e Washington [15]. O Capítulo II também contém elementos novos, por exemplo, a periodicidade da representação por séries de um elemento do completamento de um corpo com respeito a uma valorização discreta não é invariante por mudança de conjunto de representantes.

CAPÍTULO I

PRELIMINARES SOBRE CORPOS VALORIZADOS

Este capítulo tem a finalidade de reunir os conceitos básicos sobre valorizações e alguns resultados pertinentes sobre elas empregados nos capítulos II, III e IV.

Alguns resultados são apenas citados enquanto outros aparecem com provas devido a interesse neles investidos nesta tese. As referências básicas sobre a matéria são [4], [7] e [16].

1. VALORIZAÇÕES DISCRETAS DE POSTO 1

Sejam K um corpo, G um grupo abeliano totalmente ordenado e ∞ um símbolo tal que para todo $g \in G$, $g+\infty = \infty+g = \infty$ e, além disso, $\infty+\infty = \infty$ e $g < \infty$.

Definimos uma *valorização de* K como sendo uma função $v: K \to G \cup \{\infty\}$ satisfazendo às seguintes condições:

(i) $v(x) = \infty \iff x = 0$ em K;

(ii) $v(xy) = v(x)+v(y)$ para todos $x,y \in K$;

(iii) $v(x+y) \geq \min\{v(x),v(y)\}$ para todos $x,y \in K$.

Decorre de (ii) e (iii) que se $v(x) \neq v(y)$ então $v(x+y) = \min\{v(x),v(y)\}$.

EXEMPLO 1: Valorização Trivial: $v(x) = 0$ para todo $x \in K^*$.

UNICAMP
BIBLIOTECA CENTR

EXEMPLO 2: Sejam A um anel fatorial, K seu corpo de frações e Λ uma família dos primos não-associados de A. Então qualquer elemento $a \in A$ se escreve de modo único como $a = \varepsilon p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ onde ε é uma unidade de A, $n_i \in \mathbb{N}$ e $p_i \in \Lambda$ para todo $i \in \{1,2,\ldots,r\}$. Assim, para cada primo p de Λ, podemos definir uma aplicação $n_p : A \to \mathbb{Z}$ que a cada $x \in A$ associa o inteiro $n_p(x)$, expoente de p na decomposição de x em fatores primos. Considere agora a seguinte função: $v_p : K \to \mathbb{Z} \cup \{\infty\}$ definida por $v_p(\frac{a}{b}) = n_p(a) - n_p(b)$ se $\frac{a}{b} \neq 0$, e $v_p(0) = \infty$. Então v_p é uma valorização de K que é denominada *valorização p-ádica* de K.

Dada uma valorização de um corpo K definimos $A_v = \{x \in K;\ v(x) \geq 0\}$ e $M_v = \{x \in K;\ v(x) > 0\}$. A_v é um subanel de K e M_v é o único ideal maximal de A_v. De fato, se x e $y \in A_v$ então $v(x)$ e $v(y) \geq 0$. Logo $v(xy) = v(x)+v(y) \geq 0$ e daí $xy \in A_v$. Além disso, $v(x+y) \geq \min\{v(x),v(y)\} \geq 0$ o que coloca $x+y$ também em A_v. Sejam agora $x,y \in M_v$. Então $v(x)$ e $v(y) > 0$. Logo $v(x+y) \geq \min\{v(x),v(y)\} > 0$, donde $x+y \in M_v$. Se $x \in M_v$ e $y \in A_v$ então $v(xy) = v(x)+v(v) > 0$ e temos $xy \in M_v$. Segue-se que M_v é um ideal de A_v. Como todos os elementos $x \in A_v$ tais que $x \notin M_v$ são unidades de A_v, temos que M_v é o único ideal maximal de A_v.

Chamamos A_v de *anel de valorização* associada a v, M_v de *ideal de valorização de* v e o corpo quociente $A_v/M_v = \bar{K}$ de *corpo de resíduos* de v.

EXEMPLO 1: Se v é a valorização trivial do corpo dos racionais, então $A_v = Q$, $M_v = (0)$ e $\bar{Q} = Q$.

EXEMPLO 2: Seja p um número inteiro primo. Se v é a valorização p-ádica de Q então $A_v = \{\frac{a}{b}; (a,b) = 1 \text{ e } p \nmid b\}$, $M_v = \{\frac{a}{b}; (a,b) = 1 \text{ e } p \mid a\}$ e $\bar{Q} \simeq \mathbb{Z}/p\mathbb{Z}$ com o isomorfismo dado por

$$\theta : \mathbb{Z}/p\mathbb{Z} \longrightarrow \bar{Q} = A_v/M_v$$

$$\bar{i} \longmapsto i + M_v .$$

Sejam v_1 e v_2 duas valorizações de um corpo K com grupos de valores G_1 e G_2, respectivamente. Dizemos que v_1 é equivalente a v_2, $v_1 \sim v_2$, se existir um isomorfismo σ de grupos de G_1 em G_2 preservando a ordem.

Dizemos que $A \subseteq K$ é *um anel de valorização de* K, se dado $x \in K^*$ tivermos $x \in A$ ou $x^{-1} \in A$. Se v é uma valorização de K, então o anel A_v de valorização associada a v é um anel de valorização de K. Todo anel de valorização de K é de fato dado por uma valorização de K. Com efeito, existe uma correspondência bijetora entre as classes de equivalência de valorizações de um corpo K e os anéis de valorização desse corpo dada por $\bar{v} \longmapsto A_v$, $\bar{w} \longleftarrow\!\shortmid A$ onde $w : K \longrightarrow K^*/U_A \cup \{\infty\}$ é definida por $w(x) = xU_A$ se $x \neq 0$ e $w(0) = \infty$, e a ordem em K^*/U_A é definida da seguinte maneira: $xU_A \leq yU_A$ se $x \mid y$, isto é, se $y = ax$ para algum $a \in A$, ou $Ax \supseteq Ay$. É de fácil verificação que K^*/U_A com

esta ordem é um grupo ordenado.

Estes e outros fatos relevantes na Teoria de Valorizações po dem ser encontrados em [4].

Um grupo abeliano G é de *posto* 1 se $G \neq (0)$ e G não possui subgrupo convexo diferente de G e (0). Os grupos abelianos ordenados podem ser caracterizados da seguinte maneira:

PROPOSIÇÃO 1: *Seja* G *um grupo ordenado diferente de* (0). *Então são equivalentes as seguintes condições:*

(i) G *é arquimediano, isto é, se* $g,h \in G$ *com* $g > 0$, *então existe* $n \in \mathbb{Z}$, $n \geq 1$, *tal que* $ng \geq h$;

(ii) G *é ordem-isomorfo a um subgrupo de* $(\mathbb{R},+)$;

(iii) G *tem posto* 1.

Dizemos que um anel de valorização A é discreto de posto 1 se o seu grupo de valores G é isomorfo (como grupo ordenado) a um subgrupo discreto (como subespaço topológico) de $(\mathbb{R},+)$.

Só existem dois tipos de subgrupos de $(\mathbb{R},+)$: os subgrupos discretos são cíclicos e os subgrupos não-discretos são densos como subespaços topológicos de $(\mathbb{R},+)$. Neste trabalho estaremos interessados apenas em valorizações discretas de posto 1 e a proposição seguinte caracteriza essas valorizações em função dos subgrupos de $(\mathbb{R},+)$.

PROPOSIÇÃO 2: *Seja* G *um subgrupo de* $(\mathbb{R},+)$, $G \neq (0)$. *Então*

são equivalentes as seguintes condições:

(i) G *é discreto como subespaço topológico de* $\mathbb{R}$;

(ii) G *é não denso em* $\mathbb{R}$ *como subespaço topológico;*

(iii) G *tem um menor elemento positivo;*

(iv) G *é cíclico. De fato,* $G \simeq \rho\mathbb{Z}$ *para algum real* $\rho > 0$.

DEMONSTRAÇÃO: (i) => (ii) é imediato.

(ii) => (iii). Se não vale (iii), dado qualquer número real $\varepsilon > 0$, existe $g \in G$ tal que $0 < g < \varepsilon$. Se $r \in \mathbb{R}$, então $(r-\varepsilon, r+\varepsilon)$ contém um elemento de G. Com efeito, tome $g \in G$ tal que $0 < g < \varepsilon$. Como G é arquimediano, existe $n \geq 1$ tal que $ng \leq r < (n+1)g$ e $(n+1)g < r+\varepsilon$, logo $r < (n+1)g < r+\varepsilon$ o que contradiz (ii).

(iii) => (iv). Seja g_o o menos elemento positivo de G. Afirmo que $G = \langle g_o \rangle$. De fato, seja $g \in G$ tal que $g > 0$. Como G é arquimediano, existe $n \geq 1$ tal que $ng_o \leq g < (n+1)g_o$. Se $g \neq ng_o$ então $ng_o < g < (n+1)g_o$ implica $0 < a < g_o$ onde $a = (n+1)g_o - g \in G$ o que contradiz a escolha de g_o.

(iv) => (i). Tome um número real ε tal que $0 < \varepsilon < \rho$. Então para todo $g \in G$, $(g-\varepsilon, g+\varepsilon)$ contém apenas $g \in G$ e portanto G é discreto. □

Num domínio de ideais principais A, os ideais primos não-nulos são os ideais da forma πA, onde π é um elemento irredutível. Se A é um anel de valorização discreto então A possui um único

BIBLIOTECA
IMECC

elemento irredutível, a menos de multiplicação por uma unidade ; chamaremos tal elemento de *elemento primo* ou *elemento uniformizante* de A. Mais precisamente:

TEOREMA 1: *Seja A um anel de valorização discreto de posto 1. Então A é um domínio de ideais principais (logo noetheriano), A é um anel fatorial com uma só classe de elementos primos associados.*

DEMONSTRAÇÃO: Seja $p \in A$ tal que $v(p) > 0$ e $v(p)$ é o menor elemento positivo de $v(K^*) = G$. Pela Proposição 2, $G = \mathbb{Z}v(p)$. Logo, se $x \in K^*$, $v(x) = nv(p)$ para algum $n \in \mathbb{Z}$; $v(x) = v(p^n)$ o que significa $v(x.p^{-n}) = 0$, isto é, $xp^{-n} = \varepsilon$ é uma unidade de A. Logo $x = \varepsilon p^n$ com ε unidade de A, $p \in M_A$ e $n \in \mathbb{Z}$. Afirmo que p é um elemento primo de A, isto é, se $a,b \in A$ são tais que $p|ab$ então $p|a$ ou $p|b$. Basta mostrar que Ap é um ideal primo de A, na verdade $Ap = M_A$. De fato, sendo $v(p) > 0$, $p \in M_A$ e daí $Ap \subseteq M_A$. Por outro lado, se $y \in M_A$ então $y = \eta p^m$ com η unidade de A e $m \geq 1$, ou seja, $y \in Ap$ e temos $M_A \subseteq Ap$. Portanto $M_A = Ap$ e Ap é um ideal primo.

Da primeira parte da demonstração tem-se que todo $y \in A$ é escrito como $y = \varepsilon p^m$ com $m \geq 0$ e ε unidade de A ; e da segunda parte, que A é um anel fatorial com único elemento primo p (a menos de multiplicação por unidade). Portanto A é um anel fatorial com uma única classe de elementos primos associados.

Seja agora I um ideal não nulo de A ; $v(I)$ tem um elemen-

to mínimo $v(x_o) \geq 0$. É evidente que $Ax_o \subseteq I$. Reciprocamente, se $y \in I$ então $v(y) \geq v(x_o)$ e temos $v(yx_o^{-1}) \geq 0$, donde $yx_o^{-1} = a \in A$ e $y = ax_o \in Ax_o$. Logo $I = Ax_o$ e A é um domínio principal. □

2. COMPLETAMENTOS E EXTENSÕES DE VALORIZAÇÕES

Seja v uma valorização discreta de posto 1 de um corpo K. A aplicação d_v de $K \times K$ em $\mathbb{R}_+$ definida por $d_v(x,y) = \exp(-v(x-y))$ para todos $x,y \in K$ é uma métrica e, portanto, define sobre K uma topologia Hausdorff, T_v. Para qualquer $x \in K$, o conjunto de todos os $v_\varepsilon(x) = \{y \in K;\ v(y-x) < \varepsilon,\ \varepsilon > 0\}$ é uma base de vizinhanças abertas de x. O corpo K com a topologia T_v é chamado de *corpo topológico valorizado*.

Dizemos que uma sequência $\{x_i\}_{i \in \mathbb{N}}$ de elementos de K é convergente para x se ela converge na topologia T_v, isto é, dado $\varepsilon > 0$, existe $n_o \in \mathbb{N}$ tal que $d_v(x_n,x) < \varepsilon$ sempre que $n \geq n_o$. Nesse caso escrevemos $\lim\{x_i\}_{i \in \mathbb{N}} = x$ e isso ocorre se, e somente se, a sequência $\{v(x_i-x)\}_{i \in \mathbb{N}}$ converge a ∞ em $\mathbb{R}$ na topologia usual. Quando isso acontece $\{v(x_i)\}_{i \in \mathbb{N}}$ é estacionária; isto é, $v(x_i) = v(x_j)$ para todo $i,j \geq$ um certo n_o. Neste caso $v(x) = v(\lim\{x_i\}_{i \in \mathbb{N}}) = v(x_{n_o}) = v(x_{n_o+1}) = \ldots$ etc.

Dizemos que uma sequência $\{x_i\}_{i \in \mathbb{N}}$ é uma sequência de Cauchy se ela é uma sequência de Cauchy com respeito a d_v, isto é, para que qualquer inteiro N, existe $n_o \in \mathbb{N}$ tal que $v(x_n-x_m) > N$ sempre que $n,m \geq n_o$. Toda sequênica convergente é uma sequência

de Cauchy. Se toda sequência de Cauchy de elementos de um corpo K convergir em K dizemos que K é *completo*.

Seja v uma valorização de posto 1 de K. Então

(i) O conjunto C de todas as sequências de Cauchy $X = \{x_i\}_{i \in \mathbb{N}}$ de elementos de K é um anel com respeito à adição e multiplicação conponente a componente;

(ii) O conjunto O de todas as sequências que convergem a 0 é um ideal maximal de C;

(iii) A aplicação Φ de C *em* $\mathbb{R} \cup \{\infty\}$ definida por $\Phi X = \lim\{(v(x_i)\}_{i \in \mathbb{N}}$ tem as seguintes propriedades: $\Phi(X+Y) = \Phi X + \Phi Y$; $\Phi(X.Y) = \Phi X . \Phi Y$ e $\Phi X = \infty \Leftrightarrow X \in O$.

Chamamos de *corpo valorizado* ao par (K,v) onde K é um corpo e v uma valorização de K. Escrevemos $(K,v) \subseteq (L,w)$ se K é um subcorpo de L e $v = w/L$. Um homomorfismo injetor λ de K em L é chamado de imersão de (K,v) em (L,w) se $w \circ \lambda = v$; nesse caso escreveremos $\lambda : (K,v) \to (L,w)$. Se K e L são munidos das topologias T_v e T_w, respectivamente então a aplicação λ é contínua. Chamaremos de isomorfismo a uma imersão sobrejetora.

Dizemos que o corpo valorizado (K,v) é completo se K é completo com respeito à topologia T_v definida pela valorização v. Enquanto que o completamento de (K,v) é uma imersão λ de (K,v) em (L,w) tal que (L,w) é completo e λK é denso em L

com respeito a T_w. Nesse caso existe um isomorfismo $\sim$ de (L,w) em (L',w') onde (L',w') $\supseteq$ (K,v) é o completamento no sentido usual.

A existência de completamentos é assegurada pela seguinte proposição demonstrada em [4]:

PROPOSIÇÃO 3: *Seja* (K,v) *um corpo valorizado e sejam* C, O *e* Φ *como anteriormente. Então* Φ *induz uma valorização* $\hat{v}$ *do corpo* $\hat{K} = C/O$ *e* $\mu : (K,v) \to (\hat{K},\hat{v})$ *é um completamento onde* $\mu(x) = \{x\}_{i \in \mathbb{N}} + O$ *para todo* $x \in K$.

EXEMPLO: O completamento $(\hat{Q}_p,\hat{v}_p)$ de (Q,v_p) é chamado corpo dos números p-ádicos.

TEOREMA 2: *Seja* (K,v) *completo e* L/K *uma extensão finita. Então existe no máximo uma valorização* w *de* L *que estende* v *e* (L,w) *é completo.*

DEMONSTRAÇÃO: Ver [4].

Se considerarmos L/K uma extensão algébrica não teremos (L,w) completo, mas ainda vale um resultado muito útil que é conquência do fato de que toda extensão algébrica é a união de suas subextensões finitas.

COROLÁRIO: *Seja* (K,v) *completo e* L/K *uma extensão algébrica.*

Então existe no máximo uma valorização de L *que estende* v .

3. EXTENSÕES DE ANÉIS DE VALORIZAÇÃO

Seja L/K uma extensão arbitrária de K . Sejam A e B anéis de valorização de K e L , respectivamente. Dizemos que B estende de A se $A = B \cap K$.

Note que qualquer anel de valorização de L estende exatamente um anel de valorização de K , a saber, $B \cap K$. Enquanto que dado um anel de valorização A de K , existe pelo menos um anel de valorização B de L que estende A . Estaremos interessados no caso em que L/K é extensão algébrica.

PROPOSIÇÃO 4: *Sejam* A *um anel de valorização de um corpo* K , L/K *uma extensão e* D *é o fecho integral de* A *em* L . *Então são equivalentes as seguintes condições:*

(i) L/K *é uma extensão algébrica e* D *é um anel local (anel com um único ideal maximal);*

(ii) *Existe um único anel de valorização de* L *que estende* A*;*

(iii) D *é um anel de valorização de* L .

Nesse caso, D *é o único anel de valorização de* L *que estende* A.

Esse resultado junto com o Teorema 2 assegura que se L/K for extensão finita e (K,v) completo então D é completo.

Seja L/K uma extensão arbitrária e sejam v e w valoriza-

ções de K e L respectivamente. No caso de w ser uma extensão de v, isto é, v = w/K, o anel de valorização B de L correspondente a w estende o anel de valorização A de K correspondente a v. Qualquer valorização w de L estende exatamente uma valorização de K, a saber, w/K. Por outro lado, dada uma valorização v de K e um anel de valorização B de L que estende o anel de valorização A correspondente a v, a restrição a K de qualquer valorização w de L correspondente a B é equivalente apenas a v. Sendo assim, podemos mostrar que w pode ser escolhida de modo que w/K = v. Feito isso, o grupo de valores G de w contém o grupo de valores H de v. O par (G,H) é determinado por B e A a menos de isomorfismo de grupos ordenados, portanto o índice (G:H) depende apenas de B e K. Esse índice é chamado de *índice de ramificação* e é denotado por $e_{B/K}$ ou simplesmente e. Chamamos de *grau residual* de B/K e denotamos por $f_{B/K}$ ou, simplesmente f, ao grau da extensão $[B/M_B : A/M_A]$.

Se L/K é uma extensão finita então $e.f \leq [L:K]$ para qualquer anel de valorização B de L. Se K é completo e L/K separável, então vale ef = [L:K]. Com esse resultado, provamos o

TEOREMA 3: *Seja* L/K *uma extensão finita e* A *um anel de valorização discreto de* K. *Então qualquer anel de valorização* B *de* L *que estende* A *é discreto.*

DEMONSTRAÇÃO: Seja v uma valorização discreta de K correspondente a A e seja w uma valorização de L com grupo de valores

BIBLIOTECA
IMECC

G, correspondente a B e que estende v. Pela afirmação anterior que precede esse teorema, $G/\mathbb{Z}$ é finito, logo existe $n \in \mathbb{N}$, $n \neq 0$, tal que a aplicação $\delta \longmapsto n\delta$ $(\delta \in G)$ é um isomorfismo de G num subgrupo discreto de $\mathbb{R}$. Portanto w é discreta. □

A fim de demonstrarmos o Lema de Hensel vamos fixar algumas notações. Sejam v uma valorização discreta de posto 1 de um corpo K, A o seu anel de valorização e X uma indeterminada. A aplicação canônica $a \longmapsto \bar{a}$ de A no corpo de resíduos $\bar{K}$ determina um homomorfismo de anéis de A[X] em $\bar{K}[X]$ definido da seguinte maneira: se $f(X) = a_o+a_1X+\ldots+a_nX^n \in A[X]$, então $f(X) \longmapsto \bar{f}(X) = \bar{a}_o+\bar{a}_1X+\ldots+\bar{a}_nX^n \in \bar{K}[X]$. Quando $\bar{f}(X) \neq 0$ diremos que f(X) é primitivo. Além disso, para $f(X) = a_o+\ldots+a_nX^n$ em K[X] colocaremos $\bar{v}(f) = \min\{v(a_o),\ldots,v(a_n)\}$.

LEMA DE HENSEL: *Seja* (K,v) *um corpo valorizado discreto completo e seja* $f(X) \in A[X]$ *um polinômio primitivo. Suponha que* $G(X)$ *e* $H(X)$ *são polinômios relativamente primos em* $\bar{K}[X]$ *tais que* $\bar{f}(X) = G(X)H(X)$. *Então existem* g(X) *e* h(X) *em* A[X] *tais que*

(i) $f(X) = g(X)\,h(X)$;

(ii) $\bar{g}(X) = G(X)$, $\bar{h}(X) = H(X)$;

(iii) $\partial g(X) = \partial G(X)$.

DEMONSTRAÇÃO: Sejam $\partial f(X) = s$ e $\partial G(X) = r$ de modo que $\partial \bar{f}(X) \leq s$ e $\partial H(X) \leq s-r$. Existem $g_1(X)$ e $h_1(X)$ em A[X]

tais que $\bar{g}_1(X) = G(X)$, $\bar{h}_1(X) = H(X)$, $\partial g_1(X) = \partial G(X)$ e $h_1(X) = \partial H(X)$. Como $G(X)$ e $H(X)$ são primos entre si, existem $a(X)$ e $b(X)$ em $A[X]$ tais que

$$\bar{a}(X)G(X) + \bar{b}(X)H(X) = 1.$$

Então $f-g_1h_1 \in M[X]$ e $ag_1+bh_1-1 \in M[X]$. Seja $\varepsilon = \min\{\bar{v}(f-g_1h_1), \bar{v}(ag_1+bh_1-1)\}$. Se $\varepsilon = \infty$ então $f(X) = g_1(X)h_1(X)$ e terminamos. Suponha portanto que $0 < \varepsilon < \infty$ e escolha $\pi \in K$ um elemento primo, tal que $v(\pi) = 1$. Assim $f \equiv g_1h_1 \pmod{\pi}$, isto é, $f-g_1h_1 \in \pi A[X]$ ou $\bar{v}(f-g_1h_1) \geq \varepsilon \geq 1 = v(\pi)$ e temos $\bar{g}_1 = G$, $\bar{h}_1 = H$; $\partial g_1 = \partial G = r$ e $\partial h_1 \leq s-r$. Agora provamos por indução que para cada $i = 1,2,\ldots$ existem $g_i(X)$, $h_i(X) \in A[X]$ tais que

(1) $f \equiv g_ih_i \pmod{\pi^i}$;

(2) $g_i \equiv g_{i-1} \pmod{\pi^{i-1}}$, $h_i \equiv h_{i-1} \pmod{\pi^{i-1}}$, $i > 1$;

(3) $\bar{g}_i = G$ e $\bar{h}_i = H$;

(4) $\partial g_i = \partial G = r$ e $\partial h_i \leq s-r$.

Já demonstramos esse fato para $i = 1$. Suponha por indução que tenhamos construído os polinômios g_i e h_i para $i = n-1$, $n \geq 2$. Ponha $g_n(X) = g_{n-1}(X) + \pi^{n-1}u(X)$ e $h_n(X) = h_{n-1}(X) + \pi^{n-1}t(X)$ com os polinômios $u(X)$ e $t(X)$ em $A[X]$ a serem determinados. Assim as condições (2) e (3) se verificam para $i = n$. Como $g_nh_n = g_{n-1}h_{n-1} + \pi^{n-1}(g_{n-1}t + h_{n-1}u) + \pi^{2n-2}ut$ e $2n-2 \geq n$, temos

$f \equiv g_n h_n \pmod{\pi^n} \Leftrightarrow f \equiv g_{n-1} h_{n-1} + \pi^{n-1} (g_{n-1} t + h_{n-1} u) \pmod{\pi^n}$.
Por hipótese de indução,

$$w = \frac{f - g_{n-1} h_{n-1}}{\pi^{n-1}} \in A[X],$$

logo $f \equiv g_n h_n \pmod{\pi^n} \Leftrightarrow w \equiv g_{n-1} t + h_{n-1} u \pmod{\pi}$. Agora resta-nos escolher escolher u e t. De $ag_1 + bh_1 \equiv 1 \pmod{\pi}$ temos $wag_1 + wbh_1 \equiv w \pmod{\pi}$. Pelo algoritmo de Euclides podemos escrever $w(X)b(X) = q(X)q_1(X) + u(X)$ com $\partial u(X) < \partial g_1(X) = r$. Sem perda de generalidade podemos supor que $G(X)$ é mônico e tomar $g_1(X) \in A[X]$ como sendo mônico. Segue-se desse modo que $u(X) \in A[X]$. Logo $(wa+qh_1)g_1 + uh_1 \equiv w \pmod{\pi}$. Seja t o polinômio obtido substituindo-se todo coeficiente de $wa+qh_1$ divisível por π por 0. Então $t \in A[X]$ e

$$(*) \qquad tg_1 + uh_1 \equiv w \pmod{\pi} .$$

Como $g_{n-1} \equiv g_1 \pmod{\pi}$ e $h_{n-1} \equiv h_1 \pmod{\pi}$, a condição (1) é satisfeita para $i = n$. Falta apenas mostrar (4). Temos $\partial g_n = \partial g_{n-1} = r$ pois $\partial u < r$. Também, se $\partial h_n > s-r$, então $\partial t > s-r$. Como $\partial w \leq \partial uh_1 \leq s$ e g_1 é mônico com $\partial g_1 = r$, a relação (*) dá uma contradição. Portanto $\partial h_n \leq s-r$ e a construção está completa.

Para $i = 1,2,\ldots$ escreva $g_i(X) = a_o^{(i)} + a_1^{(i)} X + \ldots + a_r^{(i)} X^r$ onde $a_j^{(i)} \in A$. Então para $j = 0,1,\ldots,r$, $g_{i+1} \equiv g_i \pmod{\pi^i}$

implica $a_j^{(i+1)} \equiv a_j^{(i)} \pmod{\pi^i}$, logo $\{a_j^{(i)}\}_{i\in\mathbb{N}}$ é uma sequência de Cauchy. Como (K,v) é completo, $\lim \{a_j^{(i)}\}_{i\in\mathbb{N}} = a_j \in A$. Ponha $g(X) = a_o+a_1X+\ldots+a_rX^r$. Como $a_j \equiv a_j^{(i)} \pmod{\pi^i}$, temos $g(X) \equiv g_i(X) \pmod{\pi^i}$, $i = 1,2,\ldots$. Analogamente obtem-se $h(X) = b_o+b_1X+\ldots+b_{s-r}X^{s-r} \in A[X]$ com $h(X) \equiv h_i(X) \pmod{\pi^i}$. Portanto $f(X) \equiv g_i(X)h_i(X) \equiv g(X)h(X) \pmod{\pi^i}$ para todo i, de modo que $f(X) = f(X)h(X)$. Finalmente, $\bar{g} = \bar{g}_i = G$, $\bar{h} = \bar{h}_i = H$ e, como $\partial g_1 \leq r$, $\partial h \leq s-r$ e $\partial f = \partial g+\partial h$ e segue-se que $\partial g = r = \partial G$. □

OBSERVAÇÃO: Esse resultado pode ser obtido sem a hipótese adicional de $G(X)$ é mônico como é feito em [4].

Uma consequência importante do Lema de Hensel é dada pelo

COROLÁRIO: *Suponha que* $f(X) \in A[X]$ *e que* $\alpha \in \bar{K}$ *é uma raiz simples de* $\bar{f}(X)$. *Então existe um elemento* $a \in A$ *tal que* $\bar{a} = \alpha$ *e* $f(a) = 0$.

DEMONSTRAÇÃO: Por hipótese, $\bar{f}(X) = (X-\alpha)H(X)$ com $X-\alpha$ e $H(X)$ relativamente primos. Aplicando o Lema de Hensel temos $f(X) = g(X)h(X)$ onde $g(X)$ e $h(X) \in A[X]$ e $g(X)$ é mônico de grau 1. Portanto $g(X) = X-a$ para algum $a \in A$. □

Dizemos que um corpo valorizado (K,v) é *henseliano* se ele verifica a propriedade descrita pelo Lema de Hensel.

O resultado seguinte é fundamental para o desenvolvimento do Capítulo 4.

TEOREMA 4: *Sejam* A *um anel de valorização discreta completo de um corpo* K, L/K *uma extensão finita e* $\bar{L}$ *e* $\bar{K}$ *os corpos de resíduos de* B *e* A, *respectivamente. Suponha que* $\bar{L}/\bar{K}$ *é separável. Então* B *tem uma base sobre* A *composta de potências* $1, x, \ldots, x^{n-1}$ *de um elemento* x.

DEMONSTRAÇÃO: Sejam e o índice de ramificação de L/K e $f = [\bar{L}:\bar{K}]$ tais que $n = ef$. Seja π um elemento primo de B e seja $x \in B$ um representante de um elemento primitivo para a extensão residual $\bar{L}/\bar{K}$. Os ef elementos $x^i\pi^j$, $0 \leq i < f$ e $0 \leq j < e$ são linearmente independentes sobre K. De fato, suponha que existem $a_{ij} \in K$ não todos nulos tais que

$$\sum_{i=0}^{f-1} \sum_{j=0}^{e-1} a_{ij}\, x^i\, \pi^j = 0 .$$

Podemos supor que $w(a_{oo}\pi^o) \leq w(a_{ij}\pi^j)$ para todos i,j onde w é a valorização associada a B tal que w/K é a valorização associada a A. Então a desigualdade é estrita para todo $j > 0$. Caso contrário, se $w(a_{oo}\pi^o) = w(a_{ij}\pi^j)$ para algum $j > 0$, teríamos $w(\pi^o) - w(\pi^j) = w(a_{ij}) - w(a_{oo}) \in w(K^*)$ o que significa $\overline{w(\pi^o)} = \overline{w(\pi^j)}$, uma contradição à escolha de π. Assim, da equação de dependência linear obtemos

$$\sum_{i=0}^{f-1} \frac{a_{i0}\pi^o}{a_{oo}\pi^o}\, x^i = -\sum_{i=0}^{f-1} \sum_{j=1}^{e-1} \frac{a_{ij}\pi^j}{a_{oo}\pi^o}\, x^i \in M_B .$$

Portanto $\sum_{i=0}^{f-1} \left(\frac{\overline{a_{i0}\pi^0}}{\overline{a_{00}\pi^0}}\right) \bar{x}^i = \bar{0}$ contradizendo a escolha de x.

Seja agora π_K um elemento primo de K. Então π e π_K são associados em B; isto é, $\pi^e B = \pi_K B$. Seja $E = \sum_{i=0}^{f-1} Ax^i$. Temos então $B = E+\pi B$. Com efeito, $E+\pi B \subseteq B$; e se $\alpha \in B$ então $\bar{\alpha} = \bar{a}_o + \bar{a}_1\bar{x}+\ldots+\bar{a}_{f-1}\bar{x}^{f-1}$ com $a_o,\ldots,a_{f-1} \in A$ e assim $\alpha = a_o + a_1x+\ldots+ a_{f-1}x^{f-1} + \pi\alpha_o$ com $\alpha_o \in A$. Segue-se que

$$B = E+\pi(E+\pi B) = \ldots = E+\pi E+\ldots+\pi^{e-1}E+\pi^e B .$$

Seja $M = E+\pi E+\ldots+\pi^{e-1}E$. Observe que $M = \sum_{i,j} \oplus Ax^i\pi^j$. É suficiente portanto mostrar que $M = B$. Primeiro temos

$$B = M+\pi^e B = M+\pi_K B = \ldots = M+\pi_K M+\ldots+\pi_K^{r-1}M+\pi_K^r B$$

para todo $r \geq 1$. Como $\pi_K^s E \subset E$ para todo $s \geq 1$, tem-se que $\pi_K^s M \subset M$ e daí $M = M+\pi_K M+\ldots+\pi_K^{r-1}M$ para todo $r \geq 1$. Isso significa que $B = M+\pi_K^r B$ para todo $r \geq 1$. Como $\{\pi_K^r B / r = 1,2,\ldots\}$ é um sistema fundamental de vizinhanças de 0 em L, concluímos que M é denso em B. Por outro lado, $\{x^i\pi^j \;/\; 0 \leq i < f,\ 0 \leq j < e\}$ é parte de uma base de L sobre K e A é aberto e fechado em K. Como a aplicação $\xi \longmapsto (a_{ij})_{i,j}$ onde $\xi = \sum_{i,j} a_{ij}x^i\pi^j$ com $a_{ij} \in A$ é um isomorfismo topológico (e algébrico) de M em $A^{(ef)}$, temos que $M = \sum_{i,j} \oplus Ax^i\pi^j$ é fechado em L e em B. Portanto $M=B$.

Finalmente, o elemento x pode ser escolhido de modo que exista um polinômio mônico $R(X)$ de grau f com coeficientes em

A , tal que $R(x)$ seja um elemento primo de B . De fato, vamos primeiro escolher x tal que $\bar{L} = \bar{K}(\bar{x})$. Seja R um polinômio mônico com coeficientes em A cujo reduzido $\bar{R}$ é o polinômio minimal de $\bar{x}$. Então $w(R(x)) \geq 1$ pois a imagem de $R(x)$ em $\bar{L}$ é zero. Se vale a igualdade então $R(x)$ já é um elemento primo de B e acabamos. Caso contrário, $w(R(x)) \geq 2$. Seja h um elemento qualquer de valor 1 ($h \in M_B$). Pela fórmula de Taylor

$$R(x+h) = R(x) + hR'(x) + h^2 b$$

com $b \in B$. Como $\bar{L}/\bar{K}$ é separável, $\bar{x}$ é raiz simples de $\bar{R}$ e temos $\bar{R}'(\bar{x}) \neq 0$, logo $R'(x)$ é inversível, daí $w(R'(x)) = 0$ e temos $w(hR'(x)) = w(h)+w(R'(x)) = w(h) = 1$. Como os outros termos em $R(x+h)$ tem valor ≥ 2,

$$w(R(x+h)) = \min \{w(R(x)), w(hR'(x)), w(h^2 b)\} = 1$$

e portanto $x+h$ é a solução.

Terminamos agora a demonstração do Teorema 4. Escolha um elemento x como acima e faça $\pi = R(x)$. Pelo que mostramos inicialmente, os produtos $x^i R(x)^j$, $0 \leq i < f$ e $0 \leq j < e$ formam uma base de B sobre A. Portanto $B = A[x]$ e como x satisfaz um polinômio mônico de grau n, segue-se que as potências $1, x, x^2, \ldots, x^{n-1}$ formam uma base. □

Dizemos que uma extensão finita L/K é *não-ramificada* quando

(i) $f = [L:K]$;

(ii) $\bar{L}/\bar{K}$ é separável.

Uma extensão finita L/K é chamada de *totalmente ramificada* se $e = [L:K]$. Nesse caso nenhuma hipótese é feita sobre a separabilidade de $\bar{L}/\bar{K}$ pois L/K é totalmente ramificada se, e somente se, $f = 1$ se, e somente se, $\bar{L} = \bar{K}$. Não há modificação no corpo de resíduos.

O resultado seguinte, que usaremos na caracterização de extensões totalmente ramificadas L/K onde característica de $\bar{K}$ não divide $e = [L:K]$, no Capítulo 4, conhecido como *Lema de Krasner*, estabelece que $K(\alpha) = K(\beta)$ para quaisquer dois elementos separáveis sobre K que estão suficientemente próximos na topologia definida pela única extensão de uma valorização henseliana de K.

Seja Ω o fecho algébrico de K. Para qualquer $\alpha \in \Omega$ seja $C_\alpha = \{\sigma\alpha \ / \ \alpha \in G\}$ onde $G = \mathrm{Aut}\,(\Omega\,/K)$.

LEMA DE KRASNER: *Sejam* A *um anel henseliano de* K *e* w *uma valorização de* Ω *tal que* w/K *corresponde a* A. *Se* α *e* $\beta \in \Omega$ *são tais que* $w(\beta-\alpha) > \max\{w(\alpha'-\alpha);\ \alpha' \in C_\alpha \setminus \{\alpha\}\}$ *então* $K(\alpha,\beta)$ *é puramente inseparável sobre* $K(\beta)$. *Além disso, se* α *é separável sobre* K *então* $K(\alpha) \subseteq K(\beta)$.

DEMONSTRAÇÃO: Como o grau de separabilidade de $K(\alpha,\beta)$ sobre $K(\beta)$ é igual ao número de $K(\beta)$- monomorfismos $\rho : K(\alpha,\beta) \longrightarrow \Omega$

e qualquer desses ρ é a restrição de algum $K(\beta)$ - automorfismo de Ω, basta provar que qualquer $\sigma \in \mathrm{Aut}\,(\Omega/K(\beta))$ induz identidade $i_{K(\alpha,\beta)}$ de $K(\alpha,\beta)$. De fato, temos $w \circ \sigma = w$, logo $w(\sigma\alpha-\alpha) = w((\beta-\alpha)-(\sigma\beta-\sigma\alpha)) \geq w(\beta-\alpha) > w(\alpha'-\alpha)$ para todo $\alpha' \in C_\alpha \setminus \{\alpha\}$. Isso implica $\sigma\alpha = \alpha$. Portanto $\sigma\big|_{K(\alpha,\beta)} = i_{K(\alpha,\beta)}$ para qualquer $\sigma \in \mathrm{Aut}\,(\Omega/K(\beta))$. Assim, se α é separável sobre K, então $K(\alpha,\beta)$ é separável sobre $K(\beta)$ e como $[K(\alpha,\beta) : K(\beta)]$ é o número de $K(\beta)$-monomorfismos de $K(\alpha,\beta)$ em Ω que é igual a 1, segue que $[K(\alpha,\beta) : K(\beta)] = 1$ ou seja $K(\alpha) \subseteq K(\beta)$.

3. COMPLETAMENTO DE ANEL LOCAL

Entendemos por *anel local* um anel noetheriano R com um único ideal maximal, que denotaremos por M.

Se R é um anel local então pelo Teorema de Krull, $\bigcap_{n=1}^{\infty} M^n = (0)$. Assim podemos definir sobre R uma topologia tomando as potências $\{M^n\}$ como base de vizinhanças de 0. Esta é a topologia M-ádica do anel local R. $\bigcap_{n=1}^{\infty} M^n = (0)$ significa que R com essa topologia é um espaço Hausdorff.

Uma sequência $\{a_n\}_{n \in \mathbb{N}}$ de elementos de R é uma sequência de Cauchy se dado um número natural N, existir $n_o(N)$ tal que $a_n - a_{n+1} \in M^N$, sempre que $n \geq n_o(N)$.

Dizemos que R é completo se ele é completo na topologia M-ádica ou, equivalentemente, se toda sequência de Cauchy de elementos de R converge em R.

CAPÍTULO II

CORPOS COMPLETOS E O TEOREMA DE REPRESENTAÇÃO

Neste capítulo desenvolvemos o bem conhecido teorema de representação por séries de elementos de corpos valorizados completos a valorizações discretas. Tratamos de exemplos canônicos, embora não falte um ponto de vista original no caso de alguns exemplos. O teorema de representação citado aqui é um resultado chave para compreender o fecho algébrico do corpo de séries formais $k((T))$ sendo k algebricamente fechado. Teorema este desenvolvido no capítulo IV.

Seja A um anel de valorização discreto completo com corpo de frações K e corpo de resíduos $\bar{K}$. Fixemos um elemento primo π de A e escolhamos o conjunto S de representantes de $\bar{K}$ em A tal que $0,1 \in S$, embora isto não seja necessário.

No que segue, a convergência se refere à topologia do corpo valorizado conforme parágrafo 2, Capítulo I.

LEMA 1: *A série* $\sum_{n=0}^{\infty} s_n \pi^n$ *com* $s_n \in S$ *é convergente em* K.

DEMONSTRAÇÃO: Considere a sequência de somas parciais $\{\sum_{n=0}^{m} s_n \pi^n\}_{m=0}^{\infty} = \{x_m\}$. Seja r o primeiro número natural com

$s_r \neq 0$. Então $v(x_m) = r$ para todo $m \geq 0$ e, se $m \leq m'$, $v(x_m, -x_m) \geq m+1$. Logo, dado N suficientemente grande, se $r_o = N$ então $\forall\, m,m' \geq r_o$ com $m \leq m'$, $v(x_m, -x_m) > r_o$. Portanto $\{x_m\}$ é uma consequência de Cauchy. Como K é completo, ela converge e seu limite é $\sum_{n=0}^{\infty} s_n \pi^n$. □

LEMA 2: *Se* $r \in \mathbb{Z}$ *e* $s_n \in S$ *para todo* $n \geq r$, *então* $\sum_{n=r}^{\infty} s_n \pi^n$ *é convergente em* K.

DEMONSTRAÇÃO: Se $r \geq 0$ esse resultado segue do Lema 1. Seja $r < 0$. Pelo Lema 1, $\sum_{n=0}^{\infty} s_n \pi^n = x$, digamos. Então $\sum_{n=r}^{\infty} s_n \pi^n = x + \sum_{n=r}^{-1} s_n \pi^n$ mostrando a convergência de $\sum_{n=r}^{\infty} s_n \pi^n$. □

O seguinte resultado proporciona uma representação eficiente de elementos de um corpo completo com respeito à valorização discreta. Ela sugere que os corpos desse gênero tem uma estrutura mais simples a tratar.

TEOREMA 1 (TEOREMA DE REPRESENTAÇÃO): *Todo elemento* $a \in A$ *pode ser escrito de modo único como uma série convergente* $a = \sum_{n=0}^{\infty} s_n \pi^n$, *com* $s_n \in S$. *Analogamente, todo elemento* $x \in K$ *pode ser escrito como* $x = \sum_{n=r}^{\infty} s_n \pi^n$, *onde* $v(x) = r = \min \{n \in \mathbb{Z};\ s_n \neq 0\}$.

DEMONSTRAÇÃO: Seja $a \in A$. Por definição do conjunto S de representantes, existe um $s_o \in S$, o qual pode ser 0, tal que $a - s_o \equiv 0 \mod \pi$. Logo $a = s_o + a_1\pi$ para algum $a_1 \in A$. Suponha, por indução, que encontramos $s_{n-1} \in S$ tal que $a = s_o + s_1\pi + \ldots + s_{n-1}\pi^{n-1} + a_n\pi^n$ para algum $a_n \in A$. Então existe $s_n \in S$ tal que $a_n - s_n \equiv 0 \mod \pi$, o que implica na existência de $a_{n+1} \in A$ tal que $a_n = s_n + a_{n+1}\pi$. Da hipótese de indução segue-se que $a = s_o + s_1\pi + \ldots + (s_n + a_{n+1}\pi)\pi^n = s_o + s_1\pi + \ldots + s_n\pi^n + a_{n+1}\pi^{n+1}$. Assim, por indução, temos uma sequência $\{s_n\}$ de elementos de S. Considere agora a série $\sum_{n=0}^{\infty} s_n\pi^n$. Esta série converge pelo Lema 1. Mostremos que $a = \sum_{n=0}^{\infty} s_n\pi^n$. Ora, $a = s_o + s_1\pi + \ldots + s_n\pi^n + a_{n+1}\pi^{n+1}$. Se $\{x_m\}$ é a sequência das somas parciais do Lema 1 então $v(a-x_m) = v(a_{m+1}\pi^{m+1}) \geq m+1$. Se N é suficientemente grande então para todo $m \geq N$, $v(a-x_m) > N$. Logo $\lim \{x_m\} = a$, ou seja, $a = \sum_{n=0}^{\infty} s_n\pi^n$. Isso mostra que todo elemento $a \in A$ é da forma $a = \sum_{n=0}^{\infty} s_n\pi^n$. Se $x \in K$ então $v(x) = r = v(\pi^r)$. Daí $v(x\pi^{-r}) \geq 0$. Logo $x\pi^{-r} \in A$, donde $x\pi^{-r} = \sum_{n=0}^{\infty} s_n\pi^n$. Segue-se que $x = \sum_{n=0}^{\infty} s_n\pi^{n+r} = \sum_{n=r}^{\infty} s'_n\pi^n$. Finalmente, observe que se $v(x) = r$, então $v(x\pi^{-r}) = 0$. Daí $x\pi^{-r} = s_o + a_1\pi$ com $s_o \neq 0$. Logo $x = s_r\pi^r + s_{r+1}\pi^{r+1} + \ldots$ com $s_r \neq 0$. Portanto, $v(x) = \min \{n \in \mathbb{Z};\ s_n \neq 0\}$.

Para estabelecer a unicidade da representação acima, observe que pelo Lema 1, toda sequência $\sum_{n=0}^{\infty} t_n\pi^n$ com $t_n \in S$ converge

em K. Assim, se $a = \sum_{n=0}^{\infty} s_n \pi^n = \sum_{n=0}^{\infty} t_n \pi^n$ com s_n e t_n em S, então $\sum_{n=0}^{\infty} (s_n - t_n)\pi^n = 0$. Se $s_n - t_n \neq 0$ para algum $n \geq 0$, seja r_o o primeiro inteiro tal que $s_{r_o} - t_{r_o} \neq 0$. Então $v(\sum_{n=0}^{\infty} (s_n - t_n)\pi^n) = r_o$ enquanto que $v(0) = \infty$, uma contradição. □

OBSERVAÇÃO: A demonstração não requer que 0 e 1 estejam em S. Por exemplo, se escolhemos π e 1 como representantes de $\bar{0}$ e $\bar{1}$, respectivamente em $\bar{K}$, então a representação de 0 é a seguinte: $0 = \pi.1 - 1.\pi + \pi.\pi^2 - 1.\pi^3 + \pi.\pi^4 - 1\pi^5 + \ldots$ Se escolhemos 0 como representante de $\bar{0}$ então $0 = \sum_{n=0}^{\infty} s_n \pi^n$ onde $s_n = 0$ para todo $n \geq 0$. Por isso escolhemos S tal que 0 e 1 pertencessem a S.

A escolha adequada do conjunto S de representantes é importante para uma melhor compreensão do corpo completo K e melhor apresentação dos seus elementos. Por exemplo, seja $K = \mathbb{Q}_p$ o corpo dos números p-ádicos, ou seja, o completamento do corpo $\mathbb{Q}$ dos racionais com relação à valorização p-ádica. Então, $\bar{K} = \mathbb{Z}/p\mathbb{Z}$, e uma escolha para S pode ser $S = \{0,1,\ldots,p-1\}$. Assim, todo elemento $a \in K$ pode ser escrito de maneira única como $a = \sum_{n \geq r} s_n p^n$, $r \in \mathbb{Z}$ e $s_n \in \{0,1,\ldots,p-1\}$. Nesse caso, a série $\sum_{n \geq r} s_n p^n$ é chamada de desenvolvimento p-ádico ou representação p-ádica de a. Uma outra escolha é obtida da seguinte maneira: como A é henseliano e $\bar{K}$ é um corpo de raízes de $X^{p-1}-1$, K contém todas as raízes (p-1)-ésimas da unidade, $1,w,\ldots,w^{p-2}$.

Consideramos então o conjunto de representantes $T = \{0,1,w,\ldots,w^{p-2}\}$.

Duas perguntas interessantes surgem naturalmente: Se $x = \sum_{n \geq r} s_n p^n$ com $s_n \in \{0,1,2,\ldots,p-1\}$ então quais as condições para que x seja (i) racional e (ii) algébrico sobre $\mathbb{Q}$? Elas são relevantes pois $\mathbb{Q}_p | \mathbb{Q}$ é extensão transcendente. De fato, se (K,v) é um corpo valorizado completo discreto e S é um conjunto de representantes de $\bar{K}$; como $\#K = \#Y$ onde $Y = \{f : \mathbb{Z} \to S;\ f(n) = 0$ quase sempre se $n < 0\}$ e $\#Y > (\#S)^{N_o} \geq 2^{N_o}$, temos que K é não-enumerável. Em particular, $\mathbb{Q}_p$ é não-enumerável e, portanto, $\mathbb{Q}_p | \mathbb{Q}$ é extensão transcendente.

A segunda pergunta é certamente difícil e permanece em aberto até hoje. Vamos responder a primeira:

PROPOSIÇÃO 1: *Um número p-ádico* $x = \sum_{n \geq n_o} a_n \pi^n$ *é racional se, e somente se, o seu desenvolvimento p-ádico é periódico, isto é, existem inteiros* $h \geq n_o$ *e* $\ell \geq 1$ *tais que* $a_n = a_{n+\ell}$ *para* $n \geq h$.

DEMONSTRAÇÃO: Basta mostrar que $y = \sum_{n \geq 0} a_n p^n$ é racional se, e somente se, a série $\sum_{n \geq 0} a_n p^n$ é periódica, pois qualquer número p-ádico x é da forma $x = p^{n_o}.y$ com $n_o \in \mathbb{Z}$. Suponhamos inicialmente que a série $\sum_{n \geq 0} a_n p^n$ é periódica. Então existem inteiros $h \geq 0$ e $\ell \geq 1$ tais que $a_n = a_{n+\ell}$ para todo $n \geq h$. Escrevamos $b = a_o + a_1 p + a_2 p^2 + \ldots + a_{h-1} p^{h-1}$ e

$c = p^h(a_h + a_{h+1}p + \ldots + a_{h+\ell-1}\,p^{\ell-1})$. Então $y = b + c(1 + p^\ell + p^{2\ell} + \ldots)$. Como a série $1 + p^\ell + p^{2\ell} + \ldots$ converge e sua soma é $\frac{1}{1-p^\ell}$, temos $y = b + \frac{c}{1-p^\ell}$ que é racional pois b e $c \in \mathbb{Z}$. Reciprocamente, se y é racional então $x = p^{n_o}\frac{r}{s}$ onde n_o, r e $s \in \mathbb{Z}$ com $s > 0$, $(r,s) = 1$ e $(p,r) = (p,s) = 1$. Basta mostrar então que o desenvolvimento p-ádico de $y = \frac{r}{s}$ é periódico. Observe inicialmente que se $0 \leq c < p^m - 1$ então $\frac{c}{1-p^m}$ é periódico. De fato, da condição $0 \leq c < p^m - 1$ tem-se que c é da forma $c = c_o + c_1 p + \ldots + c_{m-1}\,p^{m-1}$ onde $c_i \in \{0,1,\ldots,p-1\}$. Então

$$\frac{c}{1-p^m} = (c_o + c_1 p + \ldots + c_{m-1}\,p^{m-1})\,(1 + p^m + p^{2m} + \ldots) =$$

$$= c_o + c_1 p + \ldots + c_{m-1}\,p^{m-1} + c_o p^m + c_1\,p^{m+1} + \ldots + c_{m-1}\,p^{2m-1} + c_o\,p^{2m} + \ldots$$

é uma série periódica. Se $b \geq 0$ e $0 \leq c < p^m - 1$ são inteiros, então $b + \frac{c}{p-p^m}$ também tem desenvolvimento periódico pois a série de b é finita. Afirmo que todo número racional $\frac{r}{s} \neq 0$, com $s > 0$, $(r,s) = (p,r) = (p,s) = 1$ é da forma $\frac{r}{s} = b + \frac{c}{1-p^m}$ com $b \geq 0$ e $0 \leq c < p^m - 1$ para algum $m \geq 1$. Com efeito, sendo $(p,s) = 1$ existem inteiros m e $t \geq 1$ tais que $p^m - 1 = st$, pois $(p,s) = 1$ implica $\bar{p} \in \mathbb{P}(s)$, grupo multiplicativo dos inteiros primos em relação a s com multiplicação módulo s, e basta tomarmos $m = 0(\bar{p})$. Daí $p^m \equiv 1 \bmod s$ ou seja $p^m - 1 = st$. Então $\frac{r}{s} = \frac{rt}{st} = \frac{rt}{p^m-1}$. Se $r > 0$, pelo Algorítmo de Euclides existem

inteiros $b' \geq 0$ e $0 \leq c' < p^m-1$ tais que $rt = b'(p^m-1)+c'$ o que implica $\frac{rt}{p^m-1} = b' + \frac{c'}{p^m-1}$. Se $c' = 0$, $\frac{r}{s}$ é número natural e logo periódico. Se $c > 0$,

$$\frac{rt}{p^m-1} = (b'+1) + \frac{c'-(p^m-1)}{p^m-1} = (b'+1) - \frac{(p^m-1)-c'}{p^m-1} = b + \frac{c}{1-p^m}$$

onde $b = b'+1 \geq 0$ e $c = (p^m-1)-c'$ com $0 \leq c < p^m-1$. Assim obtemos a forma desejada de $\frac{r}{s}$. Se $r < 0$ então $\frac{r}{s} = -\frac{r'}{s}$ com $r' > 0$. Pelo primeiro caso $\frac{r'}{s}$ é periódico e pelo lema a seguir $\frac{r}{s} = -\frac{r'}{s}$ é também periódico.

LEMA 3: *Se um número p-ádico* x *tem representação periódica, o mesmo acontece com* -x.

DEMONSTRAÇÃO: É suficiente considerar o caso onde $x = a_o + a_1 p + a_2 p_2 + \ldots$ com $a_o \neq 0$. Suponhamos que o período de x seja ℓ e que $a_h, a_{h+1}, \ldots, a_{h+\ell-1}$ se repetem. Então

$$x = a_o + a_1 p + \ldots + a_{h-1} p^{h-1} + a_h p^h + \ldots + a_{h+\ell-1} p^{h+\ell-1} + a_{h+\ell} p^{h+\ell} + \ldots$$

onde $a_n = a_{n+\ell}$ $\forall$ $n \geq h$. Ora, pela adição em Q_p, $-x = b_o + b_1 p + b_2 p^2 + \ldots$, onde $a_o + b_o \equiv 0 \pmod p$ etc., e se $v(x) = r$, então $a_r + b_r \equiv 0 \pmod p$ e $a_i + b_i + 1 \equiv 0 \pmod p$ $\forall$ $i > r$. Daí $b_{n+\ell} = b_n$, $\forall$ $n \geq h+\ell$. Assim -x também tem representação periódica.

□

BIBLIOTECA
IMECC

EXEMPLO: Tome $x = 1 + 2p + 3p^2 + p^3 + 2p^4 + 3p^5 + \ldots$ onde $p = 5$. x tem período 3 e $h = 0$ acima.

$$-x = 4 + 2p + p^2 + 3p^3 + 2p^4 + p^5 + 3p^6 + 2p^7 + p^8 + \ldots ,$$

o qual tem período 3 e $h = 3$.

Consideremos agora o conjunto de representantes $T = \{0,1,w, \ldots,w^{p-2}\}$. A periodicidade da representação de um elemento de Q_p é invariante com relação à mudança do conjunto de representantes? A resposta é negativa: mostraremos adiante que em Q_5, 2 não tem representação periódica quando usamos T, embora isso ocorra quando usamos o conjunto S, pois 2 é inteiro e o seu desenvolvimento 5-ádico é uma série finita, portanto periódica.

Antes, porém, estudemos uma situação mais geral. Seja K um corpo completo com respeito a uma valorização discreta e suponhamos que o corpo de resíduos $\bar{K}$ é finito. Seja S um conjunto de representantes de $\bar{K}$ contendo 0 e 1. Seja D o conjunto de todas as séries de K escritas usando apenas os representantes 0 e 1.

Dada uma série $f = \sum_{n \geq n_o} a_n \pi^n$, chamamos de suporte de f e denotamos por sup (f) ao conjunto $\{n \in \mathbb{Z};\ a_n \neq 0\}$.

PROPOSIÇÃO 2: *Com a hipótese de que $\bar{K}$ é finito, se $S = \{0,1,n_2, \ldots,n_\ell\}$ então toda série f de K pode ser escrita de maneira única como uma soma finita $f = d_1 + n_2 d_2 + \ldots + n_\ell d_\ell$ com $d_i \in D$ pa*

ra todo $i \in \{1,2,\ldots,\ell\}$ *distintos com suportes disjuntos dois a dois.*

DEMONSTRAÇÃO: Seja $f = \sum_{n \geq n_o} f(n)\pi^n$ onde $f(n) = a_n$. Considere as funções $f_1, f_2, \ldots, f_\ell$ definidas como segue:

$$f_1(n) = \begin{cases} 0, & \text{se } f(n) \notin \{0,1\} \\ f(n), & \text{se } f(n) \in \{0,1\} \end{cases}$$

e, para $1 < i \leq \ell$,

$$f_i(n) = \begin{cases} 0, & \text{se } f(n) \notin \{0,n_i\} \\ f(n), & \text{se } f(n) \in \{0,n_i\} \end{cases}.$$

$f_1, f_2, \ldots, f_\ell$ são séries com coeficientes em S, portanto, convergentes. Como K é completo, pertencem a K. É evidente que $\sup(f_i) \cap \sup(f_j) = \emptyset$ se $i \neq j$, $0 \leq i, j \leq \ell$, e que $f = f_1 + \ldots + f_\ell$. Ora $f_i = n_i d_i$ com $d_i \in D$. Logo $f = d_1 + n_2 d_2 + \ldots + n_\ell d_\ell$ com suportes dos d_i disjuntos dois a dois. A unicidade dessa representação segue do fato de serem disjuntos dois a dois os suportes dos d_i. □

Se $\bar{K}$ é finito, chamamos a representação $f = d_1 + n_2 d_2 + \ldots + n_\ell d_\ell$ onde $n_i \in S$ e $d_i \in D$ $i \in \{1,\ldots,\ell\}$ de *representação padrão* de f por representantes de S. Observe que os suportes de f_i são disjuntos dois a dois.

PROPOSIÇÃO 3: *Uma série* f *é periódica se, e somente se, para todos os componentes* f_i *da representação padrão de* f, *os suportes de* f_i *eventualmente formam progressões aritméticas de uma mesma razão* r.

DEMONSTRAÇÃO: Seja $f = f_1+f_2+\ldots+f_\ell$ como acima. Se $i \neq j$, então $\sup(f_i) \cap \sup(f_j) = \emptyset$. Se f é periódica, então existem inteiros m e r tais que para todo $n \geq m$, $a_n = a_{n+r}$. Logo $\sup(f_i)$ contém uma progressão aritmética com a razão r, o termo inicial estando entre a_n e a_{n+r-1}. Reciprocamente, se os $\sup(f_i)$ contêm eventualmente progressões aritméticas de uma mesma razão r, então existe um inteiro m tal que $a_n = a_{n+r}$ $\forall\, n \geq m$, pois no caso n pertence a apenas um dos $\sup(f_i)$, digamos $f_t = n_t d_t$, então $a_n = n_t = a_{n+r}$, etc. Logo f é periódica. □

Provemos agora que 2 não tem representação periódica em Q_5 quando usamos o conjunto de representantes $T = \{0, \pm 1, \pm w\}$. Se isso ocorresse, existiriam d_1, d_2, d_3 e d_4 em D, periódicos, portanto racionais (Proposição 1) tais que $2 = d_1 + wd_2 - d_3 - wd_4$. Como 1 e w são linearmente independentes sobre Q, segue-se da igualdade acima que $2 = d_1 - d_3$ e $d_2 - d_4 = 0$. Logo $d_1 = 2+d_3$. Ora, d_1 e d_3 têm suportes disjuntos e $d_1 = \Sigma\, a_n 5^n$ e $d_3 = \Sigma\, b_n 5^n$ onde $a_n, b_n \in \{0,1\}$, e $a_n b_n = 0$. De $d_1 = 2 + d_3$, tem-se $a_o = 2 + b_o$ e $a_n = b_n$ $\forall\, n \neq 0$. Se $b_o = 1$, $a_o = 3 \notin \{0,1\}$ - impossível. Se $b_o = 0$, $a_o = 2 \notin \{0,1\}$ - impossível também.

Assim 2 não é periódico, se usamos T como conjunto de representantes.

A caracterização dos elementos de Q_p que têm representação periódica com coeficientes em $T = \{0,1,w,\ldots,w^{p-2}\} = \{0,t_o,t_1,\ldots,t_{p-2}\}$ é dada pela proposição seguinte que é consequência das Proposições 1 e 3.

PROPOSIÇÃO 4: *Seja* $D = D \cap Q$. *Um elemento* $f \in Q_p$ *tem representação periódica no sistema* T *se, e somente se, existem* $d_1,\ldots,d_{p-2} \in D$ *tais que* $f = \sum_{i=o}^{p-2} t_i d_i$ *é a representação padrão de* f *com representantes em* T.

Outros completamentos de corpos obtidos de maneira análoga, através de valorização discreta, e também importantes na Matemática, são os completamentos de K(X) que estudaremos a seguir.

Para isso, definamos as valorizações de K(X) triviais sobre K. Seja p(X) um polinômio irredutível sobre K. Então a aplicação $v_{p(X)}$ que a cada elemento não nulo f(X) em K(X) associa o inteiro $v_{p(X)}(f(X))$, potência de p(X) na decomposição de f(X) em fatores irredutíveis, e $v_{p(X)}(0) = \infty$ é uma valorização discreta denominada valorização p(X)-ádica. Outra valorização discreta de K(X) é a v_∞ que a cada f(X) não nulo associa o inteiro $-\partial f(X)$ e $v_\infty(0) = \infty$.

A proposição seguinte (Ver McCarthy, P.J., "Algebraic Extensions of Fields"), assegura que além das valorizações mencionadas

acima, $K(X)$ possui apenas uma valorização trivial sobre K, a saber, a valorização trivial de $K(X)$.

PROPOSIÇÃO 5: *Seja* K *um corpo,* X *uma indeterminada e* $K(X)$ *o corpo das funções racionais sobre* K. *Seja* v *uma valorização de* $K(X)$ *trivial sobre* K. *Então* v *é equivalente a uma das seguintes valorizações:*

i) *a valorização trivial de* $K(X)$;

ii) $v_{p(X)}$, *a valorização* $p(X)$*-ádica;*

iii) v_∞, *a valorização dada pelo grau.*

Passamos a tratar da escolha de representantes para os corpos de resíduos.

PROPOSIÇÃO 6: *Seja* v *a valorização* $p(X)$*-ádica do corpo* $K(X)$. *Então o corpo de resíduos* $\overline{K(X)}_{p(X)}$ *é canonicamente isomorfo a* $K(\alpha)$, *onde* α *é uma raiz de* $p(X)$ *num fecho algébrico de* K. *Em particular,* $\text{car}\,(K(X)) = \text{car}\,(\overline{K(X)}_{p(X)})$. *Se* K *é algebricamente fechado então para todo polinômio irredutível* $p(X)$ *(necessariamente linear), o corpo de resíduos correspondente é o próprio* K. *Se* K *é perfeito então* $\overline{K(X)}_{p(X)}$ *também o é. Um conjunto natural de representantes de* $\overline{K(X)}_{p(X)}$ *é dado por* $S = \{f(X) \in K[X];\ \partial f(X) < \partial p(X)\} \cup \{0\}$.

DEMONSTRAÇÃO: Sejam

$$A_v = \left\{ \frac{f(X)}{g(X)};\ f(X),\ g(X) \in K[X],\ g(X) \neq 0 \quad \text{e} \quad p(X) \nmid g(X) \right\}$$

e $M_v = \left\{ \frac{f(X)}{g(X)} \in A_v ;\ p(X) \mid f(X) \right\}$. Seja $\varphi : A_v \longrightarrow K(\alpha)$ que leva $\frac{f(X)}{g(X)}$ em $\frac{f(\alpha)}{g(\alpha)}$. Como $p(X)$ não divide $g(X)$, $g(\alpha) \neq 0$. É evidente que φ é um homomorfismo sobrejetor. Seu núcleo

$$\ker \varphi = \left\{ \frac{f(X)}{g(X)} \in A_v ;\ \varphi\left(\frac{f(X)}{g(x)}\right) = 0 \right\}$$

é M_v. De fato, se $\varphi\left(\frac{f(X)}{g(X)}\right) = \frac{f(\alpha)}{g(\alpha)} = 0$, então $f(\alpha) = 0$ e $p(X)$ divide $f(X)$, donde $\frac{f(X)}{g(X)} \in M_v$ e $\ker \varphi \subseteq M_v$. Como $M_v \subseteq \ker \varphi$ segue-se a igualdade. Pelo teorema de isomorfismo $\overline{K(X)} = A_v/M_v \simeq K(\alpha)$. Observe que $K \subseteq \overline{K(X)}$. Segue-se que car $(\overline{K(X)})$ = car $(K(X))$. Se K é algebricamente fechado e $p(X) \in K(X)$ então qualquer raiz α de $p(X)$ está em K e pelo que foi mostrado anteriormente, $\overline{K(X)} \simeq K(\alpha) = K$. Suponhamos agora que o corpo K é perfeito. Se $\overline{K(X)}$ não fosse perfeito existiria $\beta \in L$ tal que β é inseparável sobre $\overline{K(X)}$. O isomorfismo φ de $\overline{K(X)}$ em $K(\alpha)$ se estende a um $\overline{K(X)}$-isomorfismo $\hat{\varphi}$ de $\overline{K(X)}(\beta)$ num fecho algébrico de $K(\alpha)$. Logo $\hat{\varphi}(\beta) = \lambda$ é inseparável sobre $K(\alpha)$ o que é absurdo, pois K é perfeito. $S = \{f(X) \in K[X];\ \partial f(X) < \partial p(X)\} \cup \{0\}$ é de fato um conjunto de representantes para $\overline{K(X)}$. De fato, $K(\alpha) \simeq \frac{K[X]}{(p(X))}$ e como $K[X] \subseteq A_v$, segue que o homomorfismo $\varphi : A_v \longrightarrow K(\alpha)$ restrito a S é uma aplicação bijetora, via a divisão Euclideana. Assim S é um conjunto de representantes de $\overline{K(X)}_{p(X)}$.

Segue o análogo da Proposição 6 para a valorização dada pelo grau.

PROPOSIÇÃO 7: *Seja* V_∞ *a valorização de* $K(X)$ *dada pelo grau. Então o corpo de resíduos* $\overline{K(X)}_\infty$ *é canonicamente isomorfo a* K.

DEMONSTRAÇÃO: Com efeito,

$$A_{V_\infty} = \left\{ \frac{f(X)}{g(X)} \in K(X);\ (f(X),g(X)) = 1 \ \text{ e } \ \partial g(X) \geq \partial f(X) \right\} \cup \{0\} .$$

Logo,

$$\overline{K(X)}_{V_\infty} = A_{V_\infty}/M_{V_\infty} = \left\{ \frac{f(X)}{g(X)} + M_{V_\infty};\ (f(X),g(X)) = 1 \ \text{ e } \ \partial g(X) = \partial f(X) \right\} \cup \{M_{V_\infty}\} .$$

Ora, dado $\frac{f(X)}{g(X)}$ em $K(X)$ tal que $(f(X),g(X)) = 1$ e $\partial f(X) = \partial g(X)$, pelo Algorítmo de Euclides existe $s \in K$ e $r(X) \in K[X]$ tais que $f(X) = s.g(X) + r(X)$ com $\partial r(X) < \partial g(X)$ ou $r(X) = 0$. A aplicação φ de $\overline{K(X)}_{V_\infty}$ em K que associa a cada elemento $\frac{f(X)}{g(X)} + M_{V_\infty}$ o elemento s como acima é isomorfismo de $\overline{K(X)}_{V_\infty}$ sobre K. Assim um conjunto natural de representantes é dado por K.

Seguem-se os análogos ao resultado da Proposição 1 sobre representação periódica nos corpos $K(X)_{p(X)}$ e $K(X)_\infty$.

PROPOSIÇÃO 8: *Seja* $p(X)$ *um polinômio irredutível sobre o corpo* K. *Então um elemento* ζ de $K(X)_{p(X)}$ *admite representação periódica*

dica se, e somente se, ζ *é uma função racional da forma*

$\zeta = \dfrac{f(X)}{p^r(X)(1-p^\ell(X))}$ *onde* $f(X)$ *é um polinômio,* $r \geq 0$ *e* $\ell \geq 1$ *são inteiros.*

DEMONSTRAÇÃO: Sabemos que ζ é escrito como $\zeta = \sum_{n \geq n_o} a_n p^n(X)$ em $K(X)_{p(X)}$. Suponhamos que esta representação seja periódica. Considere inicialmente $n_o \geq 0$. Então existem inteiros $h \geq 0$ e $\ell \geq 1$ tais que

$$\zeta = a_o + a_1 p(X) + \ldots + a_{h-1} p^{h-1}(X) + a_h p^h(X) + \ldots + a_{h+\ell-1} p^{h+\ell-1}(X) + a_{h+\ell} p^{h+\ell}(X) + \ldots$$

onde $a_{n+\ell} = a_n$ para todo $n \geq h$. Seja $y = a_h p^h(X) + \ldots + a_{h+\ell-1} p^{h+\ell-1}(X)$. Então

$$\zeta = a_o + a_1 p(X) + \ldots + a_{h-1} p^{h-1}(X) + y(1 + p^\ell(X) + p^{2\ell}(X) + \ldots)$$

$$= a_o + a_1 p(X) + \ldots + a_{h-1} p^{h-1}(X) + \frac{y}{1-p^\ell(X)}$$

pois a série $1 + p^\ell(X) + p^{2\ell}(X) + \ldots$ converge para $\dfrac{1}{1-p^\ell(X)}$ na topologia $p(X)$-ádica do corpo completo $K(X)_{p(X)}$. Assim $\zeta = \dfrac{f(X)}{1-p^\ell(X)}$ onde $f(X)$ é um polinômio.

Reciprocamente, a representação no corpo completo $K(X)_{p(X)}$

de uma função racional $\frac{f(X)}{1-p^{\ell}(X)}$ onde $f(X)$ é um polinômio e $\ell \geq 1$ é inteiro, é evidentemente periódica.

Considere agora $n_o < 0$. Se $\zeta = \sum_{n \geq n_o} a_n p^n(X)$ é uma representação periódica, então existem inteiros $h \geq n_o$ e $\ell \geq 1$ tais que

$$\zeta = a_{n_o} p^{n_o}(X) + \ldots + a_{-1} p^{-1}(X) + a_o + a_1 p(X) + \ldots + a_{h-1} p^{h-1}(X) + a_h p^h(X) + \ldots$$

onde $a_{n+\ell} = a_n$ para todo $n \geq h$. Sejam $r = -n_o > 0$ e $y = a_h p^h(X) + \ldots + a_{h+\ell-1} p^{h+\ell-1}(X)$. Pelo mesmo argumento anterior

$$\zeta = \frac{1}{p^r(X)} \left(a_{-r} + \ldots + a_{-1} p^{r-1}(X)\right) + a_o + \ldots + a_{h-1} p^{h-1}(X) + \frac{y}{1-p^{\ell}(X)} .$$

Portanto,

$$\zeta = \frac{f(X)}{(p^r(X)\ (1-p^{\ell}(X))}$$

onde $f(X)$ é um polinômio.

Reciprocamente, a representação no corpo completo $K(X)_{p(X)}$ de uma função racional como acima é também periódica.

Observe que nem toda função racional é do tipo descrito acima. Com efeito, considere por exemplo K um corpo de característica zero, $p(X) = X-1$ um polinômio de $K(X)$ e a função racio-

nal $\frac{1}{2-(X-1)} = \frac{1}{3-X}$. Se $\frac{1}{3-X} = \frac{f(X)}{p^r(X)(1-p^\ell(X))}$ para algum polinômio $f(X)$ e inteiros $r \geq 0$ e $\ell \geq 1$, então $p^r(X)(1-p^\ell(X)) = (3-X)f(X)$. Logo $(3-X) \mid p^r(X)(1-p^\ell(X))$. Como $(3-X)$ é irredutível sobre K, $(3-X) \mid p(X)$ ou $(3-X) \mid (1-p^\ell(X))$. Como $p(X)$ é também irredutível, a primeira alternativa não se verifica. Daí $(3-X) \mid (1-p^\ell(X))$, isto é, $1-p^\ell(X) = (3-X)g(X)$ para algum $g(X)$. Mas para $X = 3$, segue-se dessa igualdade que $1-2^\ell = 0$, uma contradição pois $\ell \geq 1$. □

PROPOSIÇÃO 9: *Seja* $\zeta = \sum_{n \geq n_o} \frac{a_n}{X^n}$, $n_o \in \mathbb{Z}$, *um elemento de* $K(X)_\infty$. *A representação de* ζ *é periódica se, e somente se,* ζ *é uma função racional da forma* $\frac{f(X)}{X^h(X^\ell-1)}$ *onde* $f(X)$ *é um polinômio,* $h \geq r$ *e* $\ell \geq 1$ *são inteiros.*

DEMONSTRAÇÃO: Suponhamos que a representação $\zeta = \sum_{n \geq n_o} \frac{a_n}{X^n}$ é periódica. Considere inicialmente $n_o \geq 0$. Então existem inteiros $h \geq 0$ e $\ell \geq 1$ tais que

$$\zeta = a_o + \frac{a_1}{X} + \ldots + \frac{a_{h-1}}{X^{h-1}} + \frac{a_h}{X^h} + \ldots + \frac{a_{h+\ell-1}}{X^{h+\ell-1}} + \frac{a_{h+\ell}}{X^{h+\ell}} + \ldots$$

onde $a_{n+\ell} = a_n$ para todo $n \geq h$. Seja $y = \frac{a_h}{X^h} + \ldots + \frac{a_{h+\ell-1}}{X^{h+\ell-1}}$. Então

$$\zeta = a_o + \frac{a_1}{X} + \ldots + \frac{a_{h-1}}{X^{h-1}} + y\left(1 + \frac{1}{X^\ell} + \frac{1}{X^{2\ell}} + \ldots\right) =$$

$$= a_o + \frac{a_1}{X} + \ldots + \frac{a_{h-1}}{X^{h-1}} + \frac{y}{1 - \frac{1}{X^\ell}}$$

pois a série $1 + \frac{1}{X^\ell} + \frac{1}{X^{2\ell}} + \ldots$ converge para $\frac{1}{1-\frac{1}{X^\ell}}$ na topologia do corpo completo $K(X)_\infty$. Logo

$$\zeta = \frac{g(X)}{X^{h-1}} + \frac{yX^\ell}{X^\ell - 1} = \frac{Xg(X) + yX^{h+\ell}}{X^h(X^\ell - 1)}$$

onde $g(X) = a_o X^{h-1} + \ldots + a_{h-1}$. Assim $\zeta = \frac{f(X)}{X^h(X-1)}$ onde $f(X)$ é um polinômio.

Reciprocamente, se ζ é uma função racional da forma $\frac{f(X)}{X^h(X^\ell - 1)}$ onde $f(X)$ é um polinômio e $h \geq 0$ e $\ell \geq 1$ são inteiros, então

$$\zeta = \frac{f(X)}{X^h(X^\ell - 1)} = \frac{f(X)}{X^{h+\ell}\left(1 - \frac{1}{X^\ell}\right)} = \frac{f(X)}{X^{h+\ell}}\left(1 + \frac{1}{X^\ell} + \frac{1}{X^{2\ell}} + \ldots\right)$$

e portanto tem representação periódica.

Considere agora $n_o < 0$. Se $\zeta = \sum_{n \geq n_o} \frac{a_n}{X^n}$ é uma representação periódica, então existem inteiros $h \geq n_o$ e $\ell \geq 1$ tais que $a_{n+\ell} = a_n$ para todo $n \geq h$. Sejam

$$y = \frac{a_n}{X^h} + \ldots + \frac{a_{h+\ell-1}}{X^{h+\ell-1}}$$

e $r = -n_o > 0$. Pelo mesmo argumento anterior

$$\zeta = a_{-r}X^r + \ldots + a_{-1}X + \frac{Xg(X) + yX^{h+\ell}}{X^h(X^\ell - 1)}.$$

Logo $\zeta = \frac{f(X)}{X^h(X^\ell - 1)}$ onde $f(X)$ é um polinômio.

Reciprocamente, a representação no corpo completo $K(X)_\infty$ de uma função racional como acima é periódica.

Observe de novo que nem toda função racional é do tipo descrito acima. Com efeito, considere K um corpo de característica zero e a função racional $\frac{1}{X-2}$. Se $\frac{1}{X-2} = \frac{f(X)}{X^h(X^\ell - 1)}$ para algum polinômio $f(X)$ e inteiros h e $\ell \geq 1$. Então $X^h(X^\ell - 1) = (X-2)f(X)$. Logo $(X-2) \mid X^h(X^\ell - 1)$. Daí $(X-2) \mid X$ ou $(X-2) \mid (X^\ell - 1)$. Como a primeira alternativa é impossível, devemos ter $(X^\ell - 1) = (X-2)\lambda(X)$ para algum polinômio $\lambda(X)$. Mas para $X = 2$, segue-se dessa igualdade que $2^\ell - 1 = 0$, uma contradição, pois $\ell \geq 1$. □

BIBLIOTECA
IMECC

CAPÍTULO III

ESTRUTURA DE CORPOS COMPLETOS A RESPEITO DE VALORIZAÇÕES DISCRETAS

O Teorema de representação do Capítulo II sugere que deverá haver relações interessantes entre um corpo K completo a respeito de uma valorização discreta v e o corpo de séries formais $\bar{K}((T))$, onde $\bar{K}$ é o corpo de resíduos de (K,v) e T uma indeterminada. Se conseguimos dentro de K um subcorpo S isomorfo a $\bar{K}$, então o próprio S pode ser tomado como um conjunto de representantes de $\bar{K}$ e teremos um isomorfismo natural $\varphi : K \longrightarrow \bar{K}((T))$ dado por $\varphi(\sum_{n \geq n_o} s_n \pi^n) = \sum_{n \geq n_o} \bar{s}_n \pi^n$. Observe que se este for o caso, então caract K = caract $\bar{K}$. Assim a questão da existência do isomorfismo φ se reduz à escolha de um subcorpo S como sistema de representantes de $\bar{K}$. Este capítulo trata desta questão; o teorema principal afirma que se K e $\bar{K}$ possuem a mesma característica e se $\bar{K}$ é um corpo perfeito, então a especificada escolha é possível e a estrutura de K é bem simples:

TEOREMA 1: *Seja* A *um anel de valorização discreto com corpo de resíduos* $\bar{K}$. *Suponha que* A *e* $\bar{K}$ *tem a mesma característica e* $\bar{K}$ *é perfeito. Então* A *é isomorfo a* $\bar{K}[[T]]$.

Este fato permanece verdadeiro mesmo quando $\bar{K}$ não é perfei-

to. Para a demonstração desse resultado mais tarde, veja por exemplo Cohen [3] e Roquette [11].

DEMONSTRAÇÃO: Pela observação feita inicialmente, basta provar que A contém um conjunto de representantes que é um corpo. Para isso, dividiremos a demonstração em dois casos: primeiro consideraremos K e $\bar{K}$ com características iguais a zero e, em seguida, K e $\bar{K}$ com características iguais a $p \neq 0$.

(i) car K = car $\bar{K}$ = 0. Neste caso, a existência de um corpo de representantes é verdadeira para anéis locais que são muito mais gerais do que anéis de valorização discretos. O desejado resultado segue da Proposição 1.

(ii) car K = car $\bar{K}$ = $p > 0$. Nesse caso o resultado segue da Proposição 3.

PROPOSIÇÃO 1: *Seja* A *um anel local que é Hausdorff e completo com relação à topologia definida pela sequência decrescente* $I_1 \supset I_2 \supset \ldots$ *de ideais tais que* $I_n . I_m \subset I_{n+m}$. *Suponha que* $\bar{K} = A/I_1$ *é um corpo de característica zero. Então* A *contém um conjunto de representantes de* $\bar{K}$ *que é um corpo.*

A primeira hipótese sobre A é satisfeita se A é um anel local noetheriano com ideal maximal *M* e completo na topologia *M*-ádica.

DEMONSTRAÇÃO DA PROPOSIÇÃO 1: Como car K = car $\bar{K}$ = 0, o corpo primo de K é isomorfo ao corpo Q dos racionais e a aplicação $\mathbb{Z} \longrightarrow A \longrightarrow \bar{K}$ é injetora. Se $x \in \mathbb{Z}$ e $x \neq 0$ então $\bar{x} = x.1 + I_1 \neq \bar{0}$. Logo $x.1 \notin I_1$ e portanto é inversível em A. Daí $Q \subseteq A$. Pelo Lema de Zorn existe um subcorpo $S \subseteq A$ maximal em relação a inclusão. Seja $\bar{S}$ a imagem de S em $\bar{K}$. Vamos provar que $\bar{S} = \bar{K}$. Observe que $\bar{K}$ é extensão algébrica de $\bar{S}$. De fato, seja $\bar{a} \in \bar{K} \setminus \bar{S}$. Considere o anel $S[a] \subseteq A$. Se $S[a] \cap I_1 = (0)$ então $S[a] \subseteq U_A$, conjunto das unidades de A, logo o corpo $S(a) \subseteq A$. Como S é subcorpo maximal de A, tem-se $S(a) = S$, e daí $a \in S$, uma contradição. Assim $S[a] \cap I_1 \neq (0)$. Seja $s_n a^n + \ldots + s_o \neq 0$ com $s_n \neq 0$ um elemento não-nulo de $S[a] \cap I_1$. Então $\bar{s}_n \bar{a}^n + \ldots + \bar{s}_o = \bar{0}$, logo $\bar{a}$ é algébrico sobre $\bar{S}$. Provamos a seguir que $\bar{K} = \bar{S}$. Sejam $\alpha \in \bar{K}$ e $\bar{f}$ o polinômio mínimo de α sobre $\bar{S}$ e levante $\bar{f}$ para $f \in S[x]$. Como car $\bar{K}$ = 0, α é raiz simples de $\bar{f}$. Pela Proposição 2 que segue, existe $x \in A$ tal que $\bar{x} = \alpha$ e $f(x) = 0$. Como $\bar{f}$ é irredutível sobre $\bar{S}$, f é irredutível sobre S e $S[x] \subset A$ é isomorfo a $\bar{S}[\alpha]$ que é um corpo. Então $S \subseteq S(x) \subseteq A$. Pela maximalidade de S, tem-se $S(x) = S$ o que implica $x \in S$ e $\alpha = \bar{x} \in \bar{S}$. Assim $\bar{K} \subseteq \bar{S}$ e consequentemente $\bar{K} = \bar{S}$.

Falta-nos provar a seguinte proposição que é um caso especial do Lema de Hensel:

PROPOSIÇÃO 2: *Seja* A *como na Proposição* 1. *Se* $f(X) \in A[X]$ *é*

tal que $\bar{f}(X) \in \bar{K}[X]$ *tem uma raiz simples* $\lambda \in \bar{K}$, *então* f *tem uma única raiz* $\alpha \in A$ *tal que* $\bar{\alpha} = \lambda$.

DEMONSTRAÇÃO: Primeiro mostramos a unicidade. Se α é uma tal raiz, temos $f(X) = (X-\alpha)g(X)$ com $\bar{g}(\lambda) \neq 0$. Se α' também é uma raiz com essa propriedade, substituindo X por α' obtemos $0 = (\alpha-\alpha')g(\alpha')$. Como $\overline{g(\alpha')} = \bar{g}(\lambda)$, $g(\alpha')$ é inversível em A. Daí $\alpha' = \alpha$ provando a unicidade. Para provar existência usamos o método de aproximação de Newton. Seja $\alpha_1 \in A$ tal que $\bar{\alpha}_1 = \lambda$; temos $f(\alpha_1) \equiv 0 \bmod I_1$. Suponha que existe $\alpha_n \in A$ tal que $\bar{\alpha}_n = \lambda$ e $f(\alpha_n) \equiv 0 \bmod I_n$. Vamos mostrar que podemos encontrar $\alpha_{n+1} \in A$ tal que $\alpha_{n+1} \equiv \alpha_n \bmod I_n$ e $f(\alpha_{n+1}) \equiv 0 \bmod I_{n+1}$. Completaremos a demonstração tomando $\alpha = \lim \alpha_n$. Para encontrar α_{n+1}, escreva $\alpha_{n+1} = \alpha_n + h$ com $h \in I_n$ e aplique a fórmula de Taylor:

$$f(\alpha_{n+1}) = f(\alpha_n) + h\, f'(\alpha_n) + h^2 y \quad \text{com} \quad y \in A.$$

Tem-se $h^2 y \in I_n \cdot I_n \subset I_{2n} \subset I_{n+1}$ e basta encontrar um $h \in I_n$ tal que $f(\alpha_n) + h\, f'(\alpha_n) \equiv 0 \bmod I_{n+1}$. Como λ é raiz simples de $\bar{f}$, temos $\overline{f'(\alpha_n)} = \bar{f}'(\lambda) \neq 0$, logo $f'(\alpha_n)$ é inversível em A. Como $f(\alpha_n) \in I_n$, a congruência acima tem solução; basta tomarmos $h = -f(\alpha_n)/f'(\alpha_n)$.

Consideremos agora

(ii) car K = car $\bar{K}$ = p $\neq$ 0. Nesse caso o resultado decorre da seguinte proposição:

PROPOSIÇÃO 3: *Sejam* K *um corpo completo com relação a uma valorização discreta,* A *o anel de valorização e* $\bar{K}$ *o seu corpo de resíduos. Suponhamos que* $\bar{K}$ *é perfeito com* $\operatorname{car} \bar{K} = p \neq 0$. *Então existem um sistema de representantes* S *de* $\bar{K}$ *e uma aplicação injetora* $f : \bar{K} \longrightarrow S$ *tais que*

(i) $f(\alpha^p) = f(\alpha)^p \quad \forall\, \alpha \in \bar{K}$;

(ii) *o sistema de representantes* S *e a aplicação* $f : \bar{K} \to S$ *são unicamente determinados por* (i);

(iii) $SS \subseteq S$;

(iv) $0, 1 \in S$.

Finalmente, S *é um corpo isomorfo a* $\bar{K}$ *se e somente se* $\operatorname{car} K = p$.

DEMONSTRAÇÃO: Seja $\alpha \in \bar{K}$. Como $\bar{K}$ é perfeito, $\alpha^{p^{-1}}, \alpha^{p^{-2}}, \ldots, \alpha^{p^{-n}} \in \bar{K}$. Para cada $n \geq 0$ fixamos um representante $a_n \in A$ tal que $\overline{a_n^{p^n}} = \alpha^{p^{-n}}$. Então $a_n^{p^n} = \alpha$ para todo $n \geq 0$. A sequência $\{a_n^{p^n}\}_{n \in \mathbb{N}}$ é de Cauchy. De fato, $\overline{a_{n+1}^{p}} = (\alpha^{p^{-(n+1)}})^p = \alpha^{p^{-n}} = \bar{a}_n$. Logo $a_{n+1}^p \equiv a_n \bmod M$. Daí $a_{n+1}^p = a_n + m$ para algum $m \in M$. Assim,

$$a_{n+1}^{p^{n+1}} - a_n^{p^n} = (a_{n+1}^p)^{p^n} - a_n^{p^n} = (a_n + m)^{p^n} - a_n^{p^n} = \sum_{i=1}^{p^n} \binom{p^n}{i} m^i a_n^{p^n - i}.$$

Se $i \neq p^n$ então $\binom{p^n}{i} \in M^{p^n} \subseteq M^n$, pois $p \in M$. Se $i = p^n$ então $m^{p^n} \in M^{p^n} \subset M^n$. Logo $a_{n+1}^{p^{n+1}} - a_n^{p^n} \in M^n$. Portanto, dado $N > 0$, se

$n > m \geq N+1$ então

$$a_n^{p^n} - a_m^{p^m} = a_n^{p^n} - a_{n-1}^{p^{n-1}} + a_{n-1}^{p^{n-1}} - a_{n-2}^{p^{n-2}} + \ldots + a_{m-1}^{p^{m-1}} - a_m^{p^m} \in M^m \subset M^{N+1}.$$

Logo a sequência $\{a_n^{p^n}\}_{n \in \mathbb{N}}$ é de Cauchy. Como K é completo, existe um elemento $a \in K$ tal que $\lim \{a_n^{p^n}\}_{n \in \mathbb{N}} = a$. Como $a_n^{p^n} \in A$ para todo $n \in \mathbb{N}$ e A é fechado em K, temos que $a \in A$. Para cada $\alpha \in \bar{K}$ escolhemos um a da maneira indicada acima. Vamos mostrar que a depende apenas de α e não da escolha dos representantes $a_n \in A$, $n \geq 0$. Se $b_n \in A$ é tal que $\bar{b}_n = \alpha^{p^{-n}}$ para todo $n \geq 0$, então $b_n \equiv a_n \bmod M$. Como car $\bar{K} = p$, o mesmo argumento acima mostra que $b_n^{p^n} \equiv a_n^{p^n} \bmod M^{p^n} \subseteq M^{n+1}$ pois $p^n \geq n+1$ para todo $n \geq 0$. Daí $\lim \{b_n^{p^n}\}_{n \in \mathbb{N}} = a$ pois $a - b_n^{p^n} = a - a_n^{p^n} + a_n^{p^n} - b_n^{p^n}$ e, dado $N > 0$, pela convergência de $\{a_n^{p^n}\}_{n \in \mathbb{N}}$, existe $m \in \mathbb{N}$ tal que para todo $n \geq m$ temos $a - a_n^{p^n} \in M^{N+1}$. Em particular $a - b_n^{p^n} = a - a_n^{p^n} + a_n^{p^n} - b_n^{p^n} \in M^{N+1}$. Portanto, para cada $\alpha \in K$ existe um único $a \in A$ obtido da maneira indicada. Seja S o conjunto desses a's e $f : \bar{K} \longrightarrow S$ definida por $f(\alpha) = a$. Se $a,b \in S$ então existem α e $\beta \in \bar{K}$ tais que a e b representam α e β, respectivamente, isto é, $a = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}}$ com $\bar{a}_n = \alpha^{p^{-n}}$ e $b = \lim \{b_n^{p^n}\}_{n \in \mathbb{N}}$ com $\bar{b}_n = \beta^{p^{-n}}$. É claro que $\overline{a_n b_n} = (\alpha\beta)^{p^{-n}}$ e

$$ab = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}} \cdot \lim \{b_n^{p^n}\}_{n \in \mathbb{N}} = \lim \{(a_n b_n)^{p^n}\}_{n \in \mathbb{N}} .$$

Se $\alpha, \beta \in \bar{K}$ e $f(\alpha) = a$, $f(\beta) = b$ então

$$f(\alpha).f(\beta) = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}} \lim \{b_n^{p^n}\}_{n \in \mathbb{N}} = \lim \{(a_n b_n)^{p^n}\}_{n \in \mathbb{N}} = f(\alpha\beta).$$

Logo $f(\alpha^p) = f(\alpha)^p$. Isto prova (iii). Para (iv), como $\bar{0}$ e $\bar{1}$ estão em $\bar{K}$, basta tomarmos $a_n = 0$ e $b_n = 1$ para todo $n \in \mathbb{N}$ e tem-se $0 = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}}$ e $1 = \lim \{b_n^{p^n}\}_{n \in \mathbb{N}}$ em S. Provamos a seguir (i): $S^p = S$. A inclusão $S^p \subseteq S$ é evidente. Suponha agora que $a = f(\alpha) \in S$ com $\alpha \in \bar{K}$. Como $\bar{K}$ é perfeito, existe $\beta \in \bar{K}$ tal que $\beta^p = \alpha$. Seja $f(\beta) = b$. Assim $f(\beta^p) = f(\beta)^p = b^p$. Por outro lado $f(\beta^p) = f(\alpha) = a$ e portanto $b^p = a$, donde $S \subseteq S^p$ e temos $S^p = S$.

(ii): Suponhamos que S' é um outro sistema de representantes e $g : \bar{K} \longrightarrow S'$ uma função tal que $g(\alpha^p) = g(\alpha)^p \ \forall \ \alpha \in \bar{K}$. Sejam $g(\alpha) = b_o$ e $g(\alpha^{p^{-n}}) = b_n \in S'$. Então

$$g(\alpha) = g((\alpha^{p^{-n}})^{p^n}) = g(\alpha^{p^{-n}})^{p^n} = b_n^{p^n} \in S'.$$

Como g é função $b_o = b_n^{p^n}$. Observe que a sequência $\{b_n^{p^n}\}_{n \in \mathbb{N}}$ define o limite $a = \lim \{b_n^{p^n}\}_{n \in \mathbb{N}}$, $a \in S$. Como $b_n^{p^n} = b_o \in S'$, tem-se $a = \lim\{b_n^{p^n}\}_{n \in \mathbb{N}} = \lim\{b_o\}_{n \in \mathbb{N}} = b_o$ e segue-se $S' \subseteq S$. Ora,

$S \subseteq S'$, pois cada $a \in S$ é da forma $a = f(\alpha)$ para algum $\alpha \in \bar{K}$. Além disso, $g(\alpha) = b_o$. Mas $\overline{f(\alpha)} = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}} = a$ e $g(\alpha) = \lim \{b_n^{p^n}\}_{n \in \mathbb{N}} = b_o$. Como $\overline{a_n^{p^n}} = \overline{b_n^{p^n}} = \alpha$, $a = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}} = \lim \{b_n^{p^n}\}_{n \in \mathbb{N}} = b_o$, $a \in S'$. Portanto $S' = S$ e $g = f$.

Finalmente, se car $K = p \neq 0$ então S é um corpo isomorfo a $\bar{K}$. De fato, se a e $b \in S$ então $a = f(\alpha)$ e $b = f(\beta)$ e digamos $a = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}}$ e $b = \lim \{b_n^{p^n}\}_{n \in \mathbb{N}}$. Então

$$a+b = \lim \{a_n^{p^n}\}_{n \in \mathbb{N}} + \lim \{b_n^{p^n}\}_{n \in \mathbb{N}} = \lim \{(a_n+b_n)^{p^n}\}_{n \in \mathbb{N}} = \lim \{c_n^{p^n}\}_{n \in \mathbb{N}}$$

onde $c_n = a_n+b_n$. Como $\bar{a}_n = \alpha^{p^{-n}}$ e $\bar{b}_n = \beta^{p^{-n}}$, $\overline{a_n+b_n} = (\alpha+\beta)^{p^{-n}}$. Logo $a+b = f(\alpha+\beta) \in S$. Assim a função f é isomorfismo de corpos e S é um corpo de representantes. Reciprocamente, se car $K = 0$ então S não pode ser fechado sob adição; se assim o fosse, como $1 \in S$, teríamos $\underbrace{1 + \ldots + 1}_{p \text{ vezes}} \in S$. Logo $p \in S$. Observe que $0 \in S$. Mas $\bar{p} = \bar{0} \in \bar{K}$ e como S é um sistema de representantes de $\bar{K}$, $p = 0$ em S, em contradição a car $K = 0$.

CAPÍTULO IV

O FECHO ALGÉBRICO DO CORPO DE SÉRIES FORMAIS k((T))

Este capítulo trata de um dos principais resultados desta tese, a saber a descrição do fecho algébrico do corpo de séries formais $k((T))$ sobre um corpo k fechado algebricamente de característica 0. Como apontamos mais adiante existem pelo menos três demonstrações tratando desta descrição e neste capítulo desenvolvemos duas delas. Estas provas usam a teoria de ramificação de valorizações. A descrição ora em questão inclui o seguinte resultado: Se k é um corpo algebricamente fechado de característica 0, então qualquer extensão algébrica finita do corpo de séries formais $k((T))$ é também um corpo de séries formais.

Consideraremos neste capítulo as seguintes notações e hipóteses: K denotará um corpo completo com relação a uma valorização discreta v_K; o anel de valorização correspondente será denotado por A_K, seu ideal maximal M_K, seu corpo de resíduos $\bar{K} = A_K/M_K$ e $U_K = A_K \setminus M_K$ o grupo de unidades de A_K.

Se L é uma extensão finita separável de K, denotaremos por A_L o fecho integral de A_K em L. Pelos resultados citados no Capítulo 1, A_L é um anel de valorização discreto completo e é o único anel de valorização de L que estende A_K. A restrição a K de qualquer valorização w de L correspondente a A_L é equi-

valente apenas a v_L. É possível mostrar então que podemos escolher $w = v_L$ de modo que $v_L/K = v_K$ e nesse caso, o grupo de valores Γ de v_L contém o grupo de valores Δ de v_K, e depois de uma identificação natural o corpo de resíduos $\bar{L}$ de v_L contém o corpo de resíduos $\bar{K}$ de v_k. Feito isso, definimos v_L, M_L e U_L como acima e vamos supor que a extensão residual $\bar{L}/\bar{K}$ seja separável.

A fim de caracterizarmos o fecho algébrico do corpo de séries formais $K = k((T))$ onde k é um corpo algebricamente fechado de característica zero, desenvolveremos a seguir um breve estudo sobre grupos de ramificação e algumas de suas propriedades. Devemos observar porém que esta não é a única maneira de fazê-lo. Existem outras demonstrações como por exemplo a que é dada por R.J. Walker em seu livro Algebraic Curves que usa o polígono de Newton e argumentos mais elementares do que aqueles que usaremos aqui. Daremos no final deste capítulo ainda uma terceira demonstração mais elementar.

Seja L/K uma extensão galoisiana satisfazendo às hipóteses acima e seja $G = G(L/K)$ o seu grupo de Galois. Note que se $s \in G$, então v_L e $v_L \circ s$ são valorizações de L estendendo v_K e pela unicidade da extensão segue que $v_L = v_L \circ s$. Daí, $s(A_L) = A_L$ e $s(M_L^i) = M_L^i$ $\forall i \geq 0$. Assim s opera sobre A_L/M_L^i com A_k/M_k^i linear e a aplicação de $G \times A_L$ em A_L que a cada par (s,y) associa o elemento $s(y)$ define uma ação do grupo G sobre o anel A_L. Além disso, pelo teorema 4 do Capítulo 1, existe um elemento

x em A_L tal que as potências $1,x,x^2,\ldots,x^{n-1}$ formam uma base de A_L sobre A_K.

LEMA 1: *Sejam* $s \in G$ *e* i *um inteiro* ≥ -1. *Então são equivalentes as seguintes condições:*

a) s *opera trivialmente no anel quociente* A_L/M_L^{i+1};

b) $v_L(s(a)-a) \geq i+1$ *para todo* $a \in A_L$;

c) $v_L(s(x)-x) \geq i+1$

DEMONSTRAÇÃO: A aplicação que a cada par $(s,\bar{a})$ de $G \times A_L/M_L^{i+1}$ associa o elemento $\overline{s(a)}$ de A_L/M_L^{i+1} define uma ação do grupo G sobre o anel quociente. Dizemos que um elemnto s de G opera trivialmente sobre A_L/M_L^{i+1} se $\overline{s(a)} = \bar{a}$ ou seja $s(a)-a \in M_L^{i+1}$. Assim (a) $\Leftrightarrow$ (b) é imediato. Mostremos agora que (a) $\Leftrightarrow$ (c). Como $1,x,\ldots,x^{n-1}$ constitui uma base de A_L sobre A_K, $\bar{1},\bar{x},\ldots,\bar{x}^{n-1}$ constitui um conjunto de geradores de A_L/M_L^{i+1} sobre A_K. Daí s opera trivialmente sobre A_L/M_L^{i+1} se e somente se $s(x^j)-x^j \in M_L^{i+1}$ para todo $j = 0,1,2,\ldots,n-1$. Mas para todo $j \geq 2$, $s(x)-x$ divide $s(x^j)-x^j$. Logo s opera trivialmente sobre A_L/M_L^{i+1} se e somente se $s(x)-x \in M_L^{i+1}$ ou seja $v_L(s(x)-x) \geq i+1$. Portanto (a) $\Leftrightarrow$ (c).

Para cada $i \geq 1$, seja G_i o conjunto dos $s \in G$ que satisfazem às condições do Lema 1.

PROPOSIÇÃO 1: *Os* G_i *formam uma sequência decrescente de subgru*

pos normais de $G : G_{-1} = G$, G_o *é o subgrupo de inércia de* G *e* $G_i = \{1\}$ *para* i *suficientemente grande.*

DEMONSTRAÇÃO: Sendo L/K uma extensão finita, G é um grupo finito. G_i é subconjunto não vazio de G pois a identidade I está em G_i. Sejam s e $t \in G_i$. Então para qualquer a em A_L, $s(a)-a$ e $t(a)-a$ estão em M_L^{i+1}. Ora, $(s \circ t)(a)-a = s(t(a)-a)+s(a)-a \in s(M_L^{i+1})+M_L^{i+1} = M_L^{i+1}+M_L^{i+1} \subseteq M_L^{i+1}$, donde $st(a)-a \in M_L^{i+1}$. Daí G_i é fechado em relação à operação de G e é portanto um subgrupo de G. Se s é um elemento qualquer de G_{i+1} então $s(a)-a$ está em M_L^{i+2} para todo a em A_L, isto é, $v_L(s(a)-a) \geq i+2 \geq i+1$. Logo $s \in G_i$. Assim, os G_i formam uma sequência decrescente de subgrupos de G. Além disso, cada G_i é normal em G. De fato, sejam $s \in G$, $t \in G_i$ e $a \in A_L$ elementos quaisquer. Então $\overline{sts^{-1}(a)} = st(\overline{s^{-1}(a)})$. Como t opera trivialmente no anel quociente A_L/M_L^{i+1}, $st(\overline{s^{-1}(a)}) = s(\overline{s^{-1}(a)}) = \overline{s(s^{-1}(a))} = \bar{a}$, ou seja, $\overline{sts^{-1}(a)} = \bar{a}$ donde $sts^{-1}(a)-a \in M_L^{i+1}$, logo $sts^{-1} \in G_i$.

Sejam $s \in G$ e $a \in A_L$. Então $v_L(a) \geq 0$ e, como $s(a) \in A_L$, $v_L(s(a)) \geq 0$. Assim $v_L(s(a)-a) \geq \min\{v_L(s(a)), v_L(a)\} \geq 0$, o que coloca $s(a)-a$ em A_L. Logo $s \in G_{-1}$ e temos $G \subseteq G_{-1}$. Como $G_{-1} \subseteq G$ segue-se a igualdade $G_{-1} = G$.

Provemos agora que G_o é o subgrupo de inércia de G. Seja $D = \{s \in G;\ s(M_L) = M_L\}$. Então, como vimos anteriormente, $D = G$. Logo o grupo de inércia de G é o núcleo do homomorfismo

$$\varepsilon : G \to G(\bar{L}/\bar{K}) \quad \text{onde} \quad \varepsilon(s) : \bar{L} \to \bar{L}$$
$$s \mapsto \varepsilon(s) \qquad\qquad \bar{x} \mapsto \overline{s(x)}$$

O núcleo de ε é $\ker \varepsilon = \{s \in G;\ \varepsilon(s) = I_{\bar{L}}\}$. Mas $\varepsilon(s) = I_{\bar{L}}$ se, e somente se, para todo $a \in A_L$ tivermos $\varepsilon(s)(\bar{a}) = \bar{a}$. Como $\varepsilon(s)(\bar{a}) = \overline{s(a)}$, isso equivale a $s(a)-a \in M_L$. Portanto $\ker\varepsilon = G_o$.

Finalmente, seja $\lambda \geq \sup\{v_L(s(x)-x);\ s \neq 1\}$. Se $s \in G_\lambda$, pela condição (2) do Lema 1, $v_L(s(x)-x) \geq \lambda+1$, logo $s(x)-x = 0$, daí $s(x) = x$, isto é, $s = 1$ e segue-se $G_\lambda = \{1\}$. □

O grupo G_i é chamado *i-ésimo grupo de ramificação de* G (ou de L/K).

PROPOSIÇÃO 2: *Seja* i *um inteiro não negativo. Para que um elemento* s *do grupo de inércia de* G_o *pertença a* G_i *é necessário e suficiente que* $\frac{s(\pi)}{\pi} \equiv 1 \bmod M_L^i$ *onde* π *é um elemento primo de* A_L.

DEMONSTRAÇÃO: Como desejamos informação sobre elementos de G_o, pode-se substituir G por G_o e K por K_r, o corpo fixo de G_o, o qual corresponde à maior extensão não-ramificada de K. Como por hipótese $\bar{L}/\bar{K}$ é separável, então L/K_r é uma extensão totalmente ramificada. Pela Proposição 4 Capítulo I, $A_L = A_K[\pi]$. Portanto $\frac{s(\pi)}{\pi} \equiv 1 \pmod{M_L^i}$ se, e somente se $v_L(\frac{s(\pi)}{\pi} - 1) \geq i \Leftrightarrow 1 + v_L(\frac{s(\pi)}{\pi} - 1) \geq i+1 \Leftrightarrow v_L(\pi) + v_L(\frac{s(\pi)}{\pi} - 1) = v(s(\pi)-\pi) \geq i+1$, se e somente se,

pelo item (3) do Lema 1, $s \in G_i$.

Definimos agora $U_L^{(0)} = U_L$ e $U_L^{(i)} = 1 + M_L^i$ para $i \geq 1$. Isso nos dá uma sequência decrescente de subgrupos fechados de U_L; esses subgrupos formam uma base de vizinhanças de 1 com relação à topologia induzida sobre U_L pela topologia de valorização de L^*. Como U_L é fechado, consequentemente completo, temos $U_L = \lim_{\leftarrow} U_L/U_L^{(i)}$.

Por simplicidade escreveremos U_L^i em vez de $U_L^{(i)}$, pois não há como confundir com potências de elementos de U_L.

PROPOSIÇÃO 3: (a) U_L^0/U_L^1 *é canonicamente isomorfo ao grupo multiplicativo* $\bar{L}^*$ *do corpo de resíduos* $\bar{L}$.
(b) *Para* $i \geq 1$, U_L^i/U_L^{i+1} *é canonicamente isomorfo a* M_L^i/M_L^{i+1} *que, por sua vez, é isomorfo não canonicamente ao grupo aditivo do corpo de resíduos* $\bar{L}$.

DEMONSTRAÇÃO: (a) Seja φ a aplicação que a cada u de U_L associa o elemento $u+M_L$ em $\bar{L}^*$. É evidente que φ é homomorfismo sobrejetor de grupos. Além disso se u está no núcleo $\ker \varphi$ de φ então $\varphi(u) = 1 + M_L$. Como $\varphi(u) = u+M_L$, $1+M_L = u+M_L$ o que implica $u \in 1+M_L$, daí $\ker \varphi \subseteq 1+M_L$. Por outro lado, para todo b em M_L, 1+b está em U_L; assim $\varphi(1+b) = 1+b+M_L = 1+M_L$, logo $1+M_L \subseteq \ker \varphi$. Das duas inclusões segue-se que $\ker \varphi = 1+M_L$ e, pelo teorema de isomorfismo, $U_L^0/U_L^1 \simeq \bar{L}^*$.

(b) Para $i \geq 1$, seja $\psi : M_L^i \to U_L^i/U_L^{i+1}$ definida por $\psi(x) = \overline{1+x}$. Então $\psi(x+y) = \overline{1+x+y}$ enquanto que $\psi(x)\psi(y) = \overline{1+x+y+xy}$. Como $1+x+y+xy = (1+x+y)\left(1 + \frac{xy}{1+x+y}\right)$ e $1 + \frac{xy}{1+x+y} \in U_L^{i+1}$ (pois $xy \in M_L^{2i} \subset M_L^{i+1}$, $1+x+y \in U_L$ e M_L^{i+1} sendo um ideal de A_L, $\frac{xy}{1+x+y} \in M_L^{i+1}$). Assim $1+x+y+xy = (1+x+y) \bmod U_L^{i+1}$. Portanto ψ é um homomorfismo. ψ é evidentemente sobrejetor e seu núcleo $\ker \psi = \{x \in M_L^i / \overline{1+x} = \bar{1}\}$. Mas $\overline{1+x} = \bar{1}$ se, e somente se, $1+x \in U_L^{i+1}$, isto é, $x \in M_L^{i+1}$. Passando ao quociente temos $M_L^i/M_L^{i+1} \simeq U_L^i/U_L^{i+1}$. Para mostrarmos que M_L^i/M_L^{i+1} é isomorfo ao grupo aditivo de $\bar{L}$, basta verificar que M_L^i/M_L^{i+1} é um espaço vetorial unidimensional sobre $\bar{L}$. De fato, se $\alpha = \pi^i + \pi^{i+1}A_L = \pi^i + M_L^{i+1}$, qualquer elemento x de M_L^i/M_L^{i+1} pode ser escrito como $c\alpha$ onde c éum elemento de $\bar{L}$. Daí a aplicação que a cada $x \in M_L^i/M_L^{i+1}$ associa $c \in \bar{L}$ tal que $x = c\alpha$ é isomorfismo. □

Vamos agora, utilizando a Proposição 4 a seguir, estabelecer a relação entre G_i/G_{i+1} e U_L^i/U_L^{i+1} reescrevendo a Proposição 2 como $s \in G_i$ se, e somente se, $\frac{s(\pi)}{\pi} \in U_L^i$. Além disso, essa proposição e seus corolários nos deixarão mais perto da caracterização que buscamos.

PROPOSIÇÃO 4: *A aplicação que a cada* $s \in G_i$ *associa* $\frac{s(\pi)}{\pi}$ *induz por passagem ao quociente um isomorfismo* θ_i *do grupo quociente* G_i/G_{i+1} *num subgrupo do grupo* U_L^i/U_L^{i+1}. *Esse isomorfismo não depende da escolha do elemento primo* π.

Explicitamente, se $s \in G_o$, então $s\pi = u\pi$ com $u \in U_L$, e $\theta_o(s) = \bar{u} \in \bar{L}^*$. Se $s \in G_i$, $i \geq 1$ então $s\pi = \pi(1+a)$ com $a \in M_L^i$, e $\theta_i(s)$ é igual à classe a em M_L^i/M_L^{i+1}.

DEMONSTRAÇÃO: Seja $\varphi : G_i \to U_L^i/U_L^{i+1}$ definido por $s \longmapsto \overline{(\frac{s(\pi)}{\pi})}$. φ é um homomorfismo de grupos. Com efeito, $\varphi(st) = \overline{(\frac{st(\pi)}{\pi})}$ e $\varphi(s)\varphi(t) = \overline{(\frac{s(\pi)}{\pi})}\,\overline{(\frac{t(\pi)}{\pi})}$. Como $\frac{st(\pi)}{\pi} = \frac{s(\pi)}{\pi}\,\frac{t(\pi)}{\pi}\,\frac{s(u)}{u}$ onde $u = \frac{t(\pi)}{\pi} \in U_L^i$. Se $s \in G_i$ então $v_L(s(u)-u) \geq i+1$. Logo $s(u)-u = m \in M_L^{i+1}$ o que implica $\frac{s(u)}{u} - 1 = m \cdot \frac{1}{u} \in M_L^{i+1}$ e tem-se $\frac{s(u)}{u} = 1 + m \cdot \frac{1}{u} \in U_L^{i+1}$. Daí $\frac{st(\pi)}{\pi} \equiv \frac{s(\pi)}{\pi}\,\frac{t(\pi)}{\pi} \bmod U_L^{i+1}$. Portanto $\varphi(st) = \varphi(s)\varphi(t)$. $\ker\varphi = \{s \in G_i;\ \overline{(\frac{s(\pi)}{\pi})} = \bar{1}\} = \{s \in G_i;\ \frac{s(\pi)}{\pi} \in U_L^{i+1}\} = G_{i+1}$. Pelo Teorema de Isomorfismo G_i/G_{i+1} é isomorfo a um subgrupo U_L^i/U_L^{i+1}.

Se π' é outro elemento primo de A_L então $\pi' = \pi u$ com $u \in U_L$. Logo $\frac{s(\pi')}{\pi'} = \frac{s(\pi u)}{\pi u} = \frac{s(\pi)}{\pi} \cdot \frac{s(u)}{u}$. Como $\frac{s(u)}{u} \equiv 1 \bmod U_L^{i+1}$, $\frac{s(\pi')}{\pi'} \equiv \frac{s(\pi)}{\pi} \bmod U_L^{i+1}$. Portanto θ_i independe da escolha do elemento primo π. □

COROLÁRIO 1: *O grupo G_o/G_1 é cíclico e é levado isomorficamente por θ_o num subgrupo do grupo das raízes da unidade contidas em $\bar{L}$. Sua ordem é prima com a característica do corpo $\bar{L}$.*

DEMONSTRAÇÃO: Como $U_L^o/U_L^1 = \bar{L}^*$ (identificando os elementos de

U_L^o/U_L^1 através do isomorfismo na Proposição 3) e L/K é extensão finita, $\theta_o(G_o/G_1)$ é subgrupo finito de $\bar{L}^*$. Se n é a ordem de $\theta_o(G_o/G_1)$ então qualquer que seja $s \in G_o$, $\theta_o(\bar{s})^n = 1$, isto é, $\theta_o(\bar{s})$ é raiz do polinômio X^n-1, portanto uma raiz n-ésima da unidade. Assim $\theta_o(G_o/G_1)$ é um subgrupo do grupo das raízes n-ésimas da unidade contidas em $\bar{L}$ e, portanto, é cíclico. Seja p a característica de $\bar{L}$. Se p divide n, então $n = pm$. Logo $x^n-1 = (x^m-1)^p = 0$ implica $x^m-1 = 0$ para qualquer x em $\theta_o(G_o/G_1)$, o que é absurdo pois $m < n$. □

COROLÁRIO 2: *Se a característica de* $\bar{L}$ *é zero, então* $G_1 = \{1\}$ *e o grupo* G_o *é cíclico.*

DEMONSTRAÇÃO: Se $i \geq 1$, U_L^i/U_L^{i+1} é isomorfo ao grupo aditivo de $\bar{L}$ que não tem subgrupos finitos não-triviais. Logo $G_i = G_{i+1}$ e, como $G_i = \{1\}$ para i suficientemente grande, temos que $G_1 = \{1\}$ e $G_o = G_o/G_1$ é cíclico pelo Corolário 1. □

Agora, usando o Corolário 2, caracterizaremos o fecho algébrico do corpo de séries formais $k((T))$.

TEOREMA 5: *Seja* k *um corpo algebricamente fechado de característica zero e seja* $K = k((T))$. *Então o fecho algébrico* K_a *do corpo* K *é a união dos corpos* $F_n = k((T^{\frac{1}{n}}))$ *para* $n \geq 1$.

DEMONSTRAÇÃO: Seja L uma extensão galoisiana finita de K de

BIBLIOTECA
IMECC

grau n e G o seu grupo de Galois. Como $\bar{K} = k$, algebricamente fechado, $G = G_o$. Pelo Corolário 2, G_o é cíclico. Seja L' uma outra extensão galoisiana finita de K cujo grau é n. Como a extensão composta L'L é galoisiana finita, L'L/K é extensão cíclica. Assim Gal (L'L/K) que é cíclico, possui apenas um subgrupo de índice n. Logo Gal (L'/K) = Gal (L/K) e L = L'. Isto mostra que para cada número natural n existe uma única extensão de K de grau n.

$T^{\frac{1}{n}}$ é raiz do polinômio $X^n - T$. Como $k[[T]]$ é anel fatorial, o polinômio $X^n - T$ é irredutível por Eisenstein. Para cada n temos portanto uma extensão $K(T^{\frac{1}{n}})$ de K de grau n.

Sejam $L_n = K(T^{\frac{1}{n}})$ e $K_n = k((T^{\frac{1}{n}}))$. Vamos provar que $L_n = K_n$; isto é, L_n é também um corpo de séries formais. Como L_n é completo, $\bar{L}_n = k$ e por hipótese car k = 0. Logo $\bar{K} = k \subset L_n$ é um corpo de representantes de $\bar{L}_n$. Como $f = [\bar{L}:\bar{K}] = 1$ pois $\bar{L} = \bar{K} = k$, temos $n = [L_n : K] = ef = e$. Seja π_K em elemento primo de K. Então $v_L(\pi_K) = e$ $v_K(\pi_K) = e \cdot 1 = n$. Tomemos $T = \pi_K$. Assim

$$v_L(T^{\frac{1}{n}}) = \frac{1}{n} v_L(T) = \frac{1}{n} v_L(\pi_K) = \frac{1}{n} \cdot n = 1$$

e $T^{\frac{1}{n}}$ é um elemento primo de L_n. Aplicando o Teorema 1 do Capítulo 2 concluímos $L_n = k((T^{\frac{1}{n}}))$. Portanto, $K_a = \bigcup_n L_n = \bigcup_n K_n$. □

Desse modo, cada extensão finita de K de grau n tem o gru-

po cíclico $\mathbb{Z}/_{n\mathbb{Z}}$ como grupo de Galois. Como $G(K_a/K) = \varprojlim G(L/K)$, onde L percorre o conjunto de extensões galoisianas finitas de K, $G(K_a/K) = \varprojlim \mathbb{Z}/_{n\mathbb{Z}} = \hat{\mathbb{Z}}$.

COROLÁRIO: *O grupo de Galois* $G(K_a/K)$ *é* $\hat{\mathbb{Z}}$.

Dissemos no início deste Capítulo que a maneira de caracterizar o fecho algébrico de $K = k((T))$ via grupos de ramificação não é a única e citamos a demonstração de Walker usando polígonos de Newton e valorizações. A proposição que mostraremos a seguir nos dá um terceiro caminho para se obter o fecho algébrico K_a de $K = k((T))$ diferente daqueles já mencionados, com uma vantagem: a de podermos analisar situações mais gerais, a saber, quando k não é de característica zero ou não é algebricamente fechado.

PROPOSIÇÃO 6: *Suponha que* L/K *é totalmente ramificada,* [L:K] = e *e* car $\bar{K} = 0$ *ou* car $\bar{K}$ *não divide* e. *Então* $L = K(\sqrt[e]{\pi})$ *onde* π *é um elemento primo de* K .

DEMONSTRAÇÃO: Observemos inicialmente que se $v' = v_L/K$ então $v' = \alpha v_K$ para algum real $\alpha > 0$. Se $\pi \in K$ é tal que $v_K(\pi) = 1$ então $v'(\pi) = \alpha \in v'(K^*)$. Logo $e = (v_L(L^*) : v'(K^*)) = (\mathbf{Z} : \alpha\mathbb{Z}) = \alpha$, em K; assim temos $v_L = e\, v_K$.

Seja π_L um elemento primo de A_L. Pela observação acima $\pi_L^e = \pi_K \mu$ onde μ é uma unidade de A_L. Como $\bar{L} = \bar{K}$, existe u,

unidade de A_K, tal que $\mu-u \in \pi_L A_L$. Escrevamos agora $\pi_L^e = \pi_K u + \pi_K(\mu-u)$. Tomemos $f(X) = X^e - \pi_K u \in L[X]$. Sejam $\alpha, \zeta\alpha, \ldots, \zeta^{e-1}\alpha$ as raízes de f onde ζ é raiz primitiva e-ésima da unidade no fecho algébrico. Se w é a extensão da valorização v_L a um fecho algébrico de L, então, para todo $i \notin \{0,e\}$, $w(\zeta^i\alpha-\alpha) = w[\alpha(\zeta^i-1)] = w(\alpha) + w(\zeta^i-1)$. Por hipótese, car $\bar{K}$ não divide e, logo X^e-1 tem raízes distintas $\zeta^0, \zeta^1, \ldots, \zeta^{e-1}$ tanto no fecho algébrico de K quanto no fecho algébrico de $\bar{K}$. Portanto $w(\zeta^i-1) = 0$ e segue-se $w(\zeta^i\alpha-\alpha) = w(\alpha)$.

Como $\pi_L^e = \pi_K u + \pi_K(\mu-u)$ tem-se $f(\pi_L) = \pi_L^e - \pi_K u = \pi_K(\mu-u)$. Como $f(X) = \prod_{i=0}^{e-1} (X-\zeta^i\alpha)$, $f(\pi_L) = \prod_{i=0}^{e-1} (\pi_L-\zeta^i\alpha)$. Aplicando w a ambos os mebros dessa igualdade, e considerando a igualdade anterior, obtemos

$$w[f(\pi_L)] = \sum_{i=0}^{e-1} w(\pi_L-\zeta^i\alpha) = w[\pi_K(\mu-u)] =$$

$$= w(\pi_K) + w(\mu-u) > w(\pi_K)$$

pois $w(\mu-u) > 0$. Assim, $\sum_{i=0}^{e-1} w(\pi_L-\zeta^i\alpha) > w(\pi_K u) = w(\alpha^e) = ew(\alpha)$, donde existe j, $0 \leq j < e$ tal que

$$w(\pi_L-\zeta^j\alpha) > w(\alpha) = \max\{w(\zeta^i\alpha-\alpha);\quad 0 < i \leq e-1\}.$$

Sendo L henseliano, pelo Lema de Krasner, Capítulo 1, $L(\zeta^j\alpha) \subset L(\pi_L) = L$. Mas $\zeta^j\alpha \in L(\zeta^j\alpha)$, logo $\zeta^j\alpha \in L$. Como f é um polinômio de Eisenstein, f é irredutível e $[K(\zeta^j\alpha) : K] = e$. Note que

$K \subset K(\zeta^j\alpha) \subset L$ e, como $[L:K] = e = \partial f$, temos $K(\zeta^j\alpha) = L$. Seja pois, $\pi = \pi_K u$. Assim $L = K(\sqrt[e]{\pi})$. □

Analisaremos agora, à luz da Proposição 6, o fecho algébrico do corpo de séries formais $K = k((T))$ onde k é um corpo algebricamente fechado e se característica zero. K é henseliano, logo para cada extensão finita L de K existe um único anel de valorização de L que estende o de K. Como $\bar{L} = \bar{K} = k$, $f = [\bar{L}:\bar{K}] = 1$ e temos varificadas as hipóteses da Proposição 6. Portanto $L = K(\sqrt[e]{\pi})$ onde π é um elemento primo de K. Sendo k algebricamente fechado, k contém as raízes e-ésimas primitivas da unidade e, consequentemente, K também as contém. Sendo car $K = 0$ segue que $K(\alpha)/K$ onde $\alpha = \sqrt[e]{\pi}$ é extensão cíclica. Se σ é um K-automorfismo de $K(\alpha)$ então $\sigma\alpha$ é também uma raiz de $X^e - \pi$. Logo $\sigma\alpha = \zeta^{i(\sigma)}\alpha$ onde $\zeta^{i(\sigma)}$ é uma raiz e-ésima da unidade, não necessariamente primitiva. A aplicação $\sigma \mapsto \zeta^{i(\sigma)}$ é obviamente um homomorfismo injetor de $G = G(K(\alpha)/K)$ num subgrupo do grupo cíclico das raízes e-ésimas da unidade. Como $\#G = [K(\alpha):K] = e$, a aplicação acima é sobre, portanto um isomorfismo. Daí $G \tilde{-} \mathbb{Z}/e\mathbb{Z}$.

Suponha agora $K(\sqrt[e]{T})$ é também uma extensão de K de grau e. Como a extensão composta $K(\sqrt[e]{T})\ K(\sqrt[e]{\pi})/K$ é finita, portanto cíclica, pelo que mostramos anteriormente, para cada divisor n da ordem do grupo de Galois dessa extensão, existe um único subgrupo de ordem n. Pelo Teorema Fundamental da Teoria de Galois existe um único subcorpo intermediário cujo grau sobre K é

e. Daí $K(\sqrt[e]{T}) = K(\sqrt[e]{\pi})$. Provamos que para cada inteiro positivo e existe uma única extensão de K de grau e. Assim, se K_a é o fecho algébrico de K então $K_a = \bigcup_e K(\sqrt[e]{T}) = \bigcup_e k((T^{\frac{1}{e}}))$, onde a última igualdade foi obtida na demonstração da Proposição 5.

Como apontamos na Introdução deste Capítulo, segue da prova do Teorema 5 o seguinte resultado interessante: Se k é um corpo algebricamente fechado de característica 0, então uma extensão finita do corpo de séries formais $k((T))$ é também um corpo de séries formais.

CAPÍTULO V

MÓDULOS FINITAMENTE GERADOS SOBRE O ANEL DE POLINÔMIOS $k[X]$ SENDO k UM CORPO

Neste capítulo desenvolvemos a estrutura de um módulo finitamente gerado sobre o anel de polinômios $k[X]$, onde k é um corpo. Pode parecer um pouco estranho inclui-lo numa tese de mestrado, já que ele faz parte de um curso comum de álgbera; aliás de muitos livros inclusive [5] e [12], fornecem um resultado ainda mais geral do que o nosso, dando assim a estrutura de módulos finitamente gerados sobre domínios principais.

Nossa abordagem via anel de polinômios $k[X]$ tem a finalidade de orientar a prova do teorema principal desta tese que consta do próximo capítulo. Este teorema trata da estrutura de módulos finitamente gerados sobre o anel de séries formais $\mathbb{Z}_p[[X]]$ onde $\mathbb{Z}_p$ é o anel de inteiros p-ádicos, sendo p um número primo.

A prova é via matrizes de relações e um componente principal da prova é o Teorema de Preparação de Weierstrass proporcionando o análogo para o anel $\mathbb{Z}_p[[X]]$ da divisão euclideana no caso do anel $k[X]$. Assim achamos interessante desenvolver uma prova da estrutura de módulos finitamente gerados sobre o anel de polinômios $k[X]$ via uma abordagem matricial.

Cabe mencionar que de modo geral esta abordagem não é de praxe nos livros comuns de álgebra. Nossa prova é tirada do livro de

Mal'cev [8]. É evidente que nossa abordagem é mais interessante do ponto de vista da álgebra linear nos estudos de formas canônicas de uma transformação linear T sobre um espaço vetorial de dimensão finita sobre o corpo k. Assim o presente capítulo torna-se mais didático e interessante.

Seja M um módulo finitamente gerado sobre o anel de polinômios $k[X]$, onde k é um corpo. Suponha que M é gerado por n elementos $u_1,\ldots,u_n$. Então existe um homomorfismo sobrejetor θ do $k[X]$-módulo livre $k[X]^n$ em M, tal que $\theta(y_i) = u_i$ para todo $i = 1,\ldots,n$, onde $y_1 = (1,0,\ldots,0)$, $y_2 = (0,1,0,\ldots,0)$,... e $y_n = (0,\ldots,0,1)$. Se $K = \ker \theta$ então, pelo Teorema Fundamental do Isomorfismo, $M \simeq k[X]^n/K$.

PROPOSIÇÃO 1: *O submódulo* K *pode ser gerado por* m *elementos com* $m \leq n$.

DEMONSTRAÇÃO: Seja $R = k[X]$. Procedemos por indução sobre n. Como K é um submódulo de R^n, temos que

$$I_1(K) = \{a \in R \,/\, \exists y \in K \text{ tal que } y - ay_1 \in Ry_2 + \ldots + Ry_n\}$$

é um ideal de R. Sendo R um domínio de ideais principais, $I_1(K) = Ra_1$ e existe $x_1 \in K$ tal que $x_1 - a_1y_1 \in Ry_2 + \ldots + Ry_n$. Seja $K_1 = K \cap (Ry_2 + \ldots + Ry_n)$. Afirmo que $K = Rx_1 + K_1$. Com efeito, se $z = b_1y_1 + \ldots + b_ny_n \in K$ então $b_1 \in I_1(K)$, daí $b = da_1$

com $d \in R$. Segue-se que $z-dx_1 = z-d(x_1-a_1y_1)-b_1y_1 \in K_1$, logo $z \in Rx_1+K_1$ e temos $K \subseteq Rx_1+K_1$. A inclusão no outro sentido é imediata. Por hipótese de indução K_1 tem m-1 geradores e $m-1 \leq n-1$. Portanto, K tem n geradores e $m \leq n$. □

Sejam $x_1,\ldots,x_m$ os geradores de K. Então $x_1 = (\lambda_{11},\ldots,\lambda_{1n})$, $x_m = (\lambda_{m1},\ldots,\lambda_{mn})$. M é conhecido a partir de K e K a partir de $x_1,\ldots,x_m$. Portanto M é conhecido pela matriz m x n

$$F = \begin{bmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & & \vdots \\ \lambda_{m1} & \cdots & \lambda_{mn} \end{bmatrix}$$

onde interpretamos as linhas do F como geradores de K. Ora cada linha dessa matriz é um elemento do núcleo do homomorfismo θ. Assim temos que para todo $i = 1,\ldots,m$, $\theta(\lambda_{i1},\lambda_{i2},\ldots,\lambda_{in}) = 0$, isto é, $\lambda_{i1}u_1 + \lambda_{i2}u_2 + \ldots + \lambda_{in}u_n = 0$. Podemos então dizer que $M = [u_1,\ldots,u_n]$ é determinado pela matriz $F = [\lambda_{ij}]_{m \times n}$ e relações

$$(*) \quad \sum_{j=1}^{n} \lambda_{ij} u_j = 0 \quad \text{com} \quad i = 1,2,\ldots,m,$$

isto é, M é gerado por $u_1,\ldots,u_n$ e relações (*). Chamamos F de matriz de relações. Assim, um módulo finitamente gerado sobre $R = k[X]$ é determinado por uma matriz de relações. Procuro então um conjunto de geradores e um conjunto de relações as mais

simples possíveis.

DEFINICÃO: *Dizemos que duas natrizes* $F_{m\,x\,n}$ *e* $F'_{m',\,x\,n'}$ *são equivalentes se* M *é gerado por* $u_1,\ldots,u_n$ *e relações dadas por* F *e, ao mesmo tempo,* M *é gerado por* $u'_1,\ldots,u'_n$ *e relações dadas por* F' .

Esta é evidentemente uma relacão de equivalência.

EXEMPLO 1: Seja M = (0) o k[X]-módulo nulo. Então $\theta : k[X]^n \to M$ é a aplicação nula. Assim, ker $\theta = k[X]^n$. Portanto M é dado pela matriz $F = I_n$ ou por qualquer outra matriz $F' = I_m$ com $m \geq 1$. Logo $F \sim F'$.

EXEMPLO 2: Seja $M = [u_1, u_2]$ dado pela matriz

$$F = \begin{bmatrix} X & X^2 \\ 1 & 1+X \end{bmatrix} \quad \text{e relações} \quad \begin{aligned} Xu_1 + X^2u_2 &= 0 \qquad (1) \\ u_1 + (1+X)u_2 &= 0 \qquad (2). \end{aligned}$$

Desse sistema obtemos, multiplicando a equação (2) por X,

$$\begin{aligned} Xu_1 + X^2u_2 &= 0 \qquad (1) \\ Xu_1 + (X+X^2)u_2 &= 0 \qquad X(2) \end{aligned}$$

X(2)-(1) nos dá $Xu_2 = 0$ e, substituindo em (1), $xu_1 = 0$. Te

mos então novas relações $Xu_1 = 0$ e $Xu_2 = 0$ que correspondem à matriz $F' = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix}$. Logo M é dado também por F' e temos $F \sim F'$. Isto significa que

$$M \simeq k[X]/_{(X)} \times k[X]/_{(X)} \simeq k \times k.$$

Nesse caso a matriz F' é mais compreensível do que a matriz F. Perguntamos então: como partindo de uma matriz F, podemos chegar a uma outra matriz de relações F'? Veremos através da proposição a seguir, que isso pode ser feito de maneira muito interessante usando operações relacionadas com matrizes, as quais chamaremos de operações elementares.

Seja F uma matriz de relações. Pela Proposição 1 podemos considerar apenas matrizes quadradas. São as seguintes as operações elementares:

(i) *Multiplicar uma linha qualquer de* F *por um escalar não nulo* $\lambda \in k$;

(ii) *Somar a uma linha qualquer de* F *uma outra linha multiplicada por* $f(X) \in k[X]$;

(iii) *Multiplicar uma coluna qualquer de* F *por um escalar não nulo* $\lambda \in k$;

(iv) *Somar a uma coluna qualquer de* F *uma outra coluna multiplicada por* $f(X) \in k[X]$.

PROPOSIÇÃO 2: *Seja* M *um módulo finitamente gerado sobre* $k[X]$ *e* $F_{n\,x\,n}$ *uma matriz de relações de* M. *Se* $F'_{n\,x\,n}$ *é uma matriz obtida de* F *por uma qualquer das operações elementares, então* $F \sim F'$.

DEMONSTRAÇÃO: (i) Sejam $M = [u_1,\ldots,u_n]$ e $F = [a_{ij}]_{n\,x\,n}$. Suponha $F' = [b_{ij}]_{n\,x\,n}$ é obtida de F pela operação (i), isto é, $b_{tj} = \lambda a_{tj}$ com $\lambda \neq 0$ e $b_{ij} = a_{ij}$ se $i \neq t$. Então

$$\sum_j b_{ij}\, u_j = \sum_j a_{ij}\, u_j = 0 \quad \text{se } i \neq t \text{ e, se } i = t,$$

$$\sum_j b_{tj}\, u_j = \sum_j \lambda a_{tj}\, u_j = \lambda \sum_j a_{tj}\, u_j = 0 .$$

Logo F' é também uma matriz de relações de M. Além disso, como $\lambda \neq 0$, partindo de relações dadas por F', podemos obter as relações dadas por F multiplicando a t-ésima relação por λ^{-1}. Assim, conhecendo-se F conhecemos F' e, reciprocamente. Logo M é também determinado pela matriz F' e, portanto $F \sim F'$.

(ii) Consideremos agora que $F' = [b_{ij}]_{n\,x\,n}$ é obtida de $F = [a_{ij}]_{n\,x\,n}$ através da operação (ii), isto é, $b_{tj} = a_{tj} + fa_{sj}$, $s \neq t$ e $b_{ij} = a_{ij}$ se $i \neq t$. Então,

$$\sum_j b_{ij}\, u_j = \sum_j a_{ij}\, u_j = 0 \quad \text{se } i \neq t \text{ e, se } i = t,$$

$$\sum_j b_{tj}\, u_j = \sum_j (a_{tj}+fa_{sj})u_j = \sum_j a_{tj}\, u_j + f \sum_j a_{sj}\, u_j = 0.$$

Logo F' é também uma matriz de relações de M. Além disso, somando à t-ésima relação dada por F' a s-ésima relação dada por F' multiplicada por $(-f)$, obtemos de F' as relações dadas pela matriz F. Portanto $F \sim F'$.

(iii) Para a operação (iii) suponha que $F' = [b_{ij}]_{n\,x\,n}$ onde $\forall\, i$ com $1 \leq i \leq n$, $b_{it} = \lambda a_{it}$ com $\lambda \neq 0$ e $b_{ij} = a_{ij}$ se $j \neq t$. Como $\lambda \neq 0$, $M = [u_1,\ldots,\lambda^{-1}u_t,\ldots,u_n]$. De fato, se $u \in M$ então

$$u = \sum_i b_i u_i \quad \text{com} \quad b_i \in k[X]$$
$$= b_1u_1+\ldots+(b_t\lambda)(\lambda^{-1}u_t)+\ldots+b_nu_n \in [u_1,\ldots,\lambda^{-1}u_t,\ldots,u_n].$$

Logo $M \subseteq [u_1,\ldots,\lambda^{-1}u_t,\ldots,u_n]$ e, evidentemente, $[u_1,\ldots,\lambda^{-1}u_t,\ldots,u_n] \subseteq M$. Segue-se que para todo $i = 1,2,\ldots,n$,

$$\sum_j a_{ij}u_j = 0 \Leftrightarrow a_{il}u_1+\ldots+(a_{it}\lambda)(\lambda^{-1}u_t)+\ldots+a_{in}u_n = 0.$$

Portanto, M é gerado por $u_1,\ldots,u_n$ e relações dadas por F e, ao mesmo tempo, M é gerado por $u_1,\ldots,\lambda^{-1}u_t,\ldots,u_n$ e relações dadas por F' e temos $F \sim F'$.

(iv) Finalmente, suponhamos que $F' = [b_{ij}]_{n\,x\,n}$ é obtida de $F = [a_{ij}]_{n\,x\,n}$ via operação (iv), isto é, $\forall\, i$ com $1 \leq i \leq n$ $b_{it} = a_{it}+fa_{is}$ com $f \in k[X]$ e $b_{ij} = a_{ij}$ se $j \neq t$. Afirmo que $M = [u_1,\ldots,u_s-fu_t,u_{s+1},\ldots,u_n]$. Com efeito, se $u \in M$ então

$$u = b_1u_1+\ldots+b_su_s+\ldots+b_tu_t+\ldots+b_nu_n$$

$$= b_1u_1+\ldots+b_s(u_s-fu_t)+\ldots+(b_t-b_sf)u_t+\ldots+b_nu_n$$

que está em $[u_1,\ldots,u_s-fu_t,\ldots,u_t,\ldots,u_n]$. Logo $M \subseteq [u_1,\ldots,u_s-fu_t,\ldots,u_t,\ldots,u_n]$. A inclusão no outro sentido é imediata. Segue-se que para todo $i = 1,2,\ldots,n$

$$\sum_j a_{ij}u_j = 0 \iff a_{i1}u_1+\ldots+a_{is}(u_s-fu_t)+\ldots+(a_{it}+fa_{is})u_t+\ldots+a_{in}u_n = 0 .$$

Portanto M é gerado por $u_1,\ldots,u_n$ e relações dadas por F e ao mesmo tempo M é gerado por $u_1,\ldots,u_s-fu_t,u_{t+1},\ldots,u_n$ e relações dadas por F' e temos $F \sim F'$. □

Com esta proposição reduzimos o estudo dos módulos finitamente gerados sobre $k[X]$ ao estudo das matrizes com entradas em $k[X]$. Passamos então a trabalhar com essas matrizes, criando condições para darmos a estrutura de $k[X]$-módulos de tipo finito. De acordo com a Proposição 1 podemos considerar apenas matrizes quadradas.

Considere as matrizes quadradas $[\lambda_{ij}]_{n\,x\,n}$ onde cada λ_{ij} é um polinômio em X com coeficientes no corpo k. Dizemos que uma matriz F é equivalente a uma matriz G se F puder ser obtida de G por uma série finita de operações elementares.

O resultado seguinte nos dá mais uma operação muito útil que é obtida a partir daquelas definidas anteriormente.

PROPOSIÇÃO 3: *Quaisquer duas linhas de uma matriz podem ser permutadas usando as operações* (i) *e* (ii); *quaisquer duas colunas podem ser permutadas usando-se* (iii) *e* (iv).

DEMONSTRAÇÃO: Suponha que queremos permutar a i-ésima linha L_i, e a j-ésima linha L_j, de uma matriz F. Isso é possível através da aplicação da seguinte série de operações elementares.

(a) some a linha L_j à linha L_i obtendo assim uma nova i-ésima linha $L_i' = L_i + L_j$;

(b) some a linha L_i' multiplicada por (-1) à linha L_j obtendo uma nova j-ésima linha L_j';

(c) multiplique a linha L_j' por (-1), obtendo L_j'';

(d) some a linha L_j'' multiplicada por (-1) à linha L_i'.

Para mermutar quaisquer duas colunas da matriz F executamos na mesma sequência operações análogas com as colunas. □

Segue desse resultado que se F difere de G apenas na ordem das linhas ou colunas então F é equivalente a G.

A relação "F é equivalente a G" definida acima, é uma relação de equivalência. Com efeito,

1. A RELAÇÃO É TRANSITIVA: Se F é equivalente a G e G é equivalente a H então F é equivalente a H. Por hipótese, G

pode ser obtida de H e F de G por uma série finita de operações elementares. Consequentemente F pode ser obtida de H por uma série finita dessas operações.

2. A RELAÇÃO É SIMÉTRICA: Se F pode ser obtida de G por uma série finita de operações elementares então G pode ser obtida de F por uma série finita de operações elementares. Mostremos primeiro que se F pode ser obtida de G por uma só operação elementar, então G também pode ser obtida de F por uma só operação elementar. Para isto consideremos cada um dos quatro tipos de operações elementares. Seja F obtida de G pela operação (i) por multiplicação da i-ésima linha de G por um escalar não-nulo λ. Então multiplicando a i-ésima linha de F por λ^{-1} obteremos G. Agora seja F obtida de G via operação (ii), por exemplo somando-se à i-ésima linha de G a j-ésima linha multiplicada por f. Nesse caso, somando-se à i-ésima linha de F a j-ésima linha multiplicada por (-f) obtemos G. Análogas afirmações são verdadeiras para operações dos tipos (iii) e (iv). Consequentemente, para cada operação elementar existe uma operação elementar inversa. Portanto, se F é obtida de G por uma série finita de operações elementares, aplicando as operações inversas na ordem oposta obteremos G de F.

3. A RELAÇÃO É REFLEXIVA: Aplicando a F duas operações que são inversas uma da outra, obteremos novamente F.

Desta forma as matrizes de polinômios podem ser divididas em classes de equivalência. Aqui surge a questão se existe ou não um certo tipo de matriz de polinômios tal que cada classe de equivalência contém uma e uma única matriz dessa forma. *Uma forma* com essa propriedade é chamada *canônica*. Mostraremos que para matrizes de polinômios, a forma diagonal com certas condições de divisibilidade é uma forma canônica no sentido acima.

É através dessa matriz que caracterizaremos os módulos finitamente gerados sobre $k[X]$.

DEFINIÇÃO: *Uma matriz de polinômios da forma*

$$\begin{bmatrix} f_1 & & & \\ & f_2 & & \\ & & \ddots & \\ & & & f_n \end{bmatrix}$$

é chamada matriz diagonal canônica se cada elemento diagonal f_i *é um divisor do seguinte* f_{i+1}, *e se todos os elementos diagonais não nulos tem coeficiente líder* 1.

É claro que se a diagonal contém polinômios nulos, eles devem ocorrer nos últimos lugares, desde que 0 não é divisor de nenhum polinômio não-nulo. Por outro lado, se a diagonal contém escalares diferentes de zero. então eles devem ser iguais a 1 e ocu

par os primeiros lugares, pois o único polinômio com coeficiente líder 1 que divide 1 é o polinômio 1. Consequentemente a matriz diagonal canônica genérica tem a forma

$$\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1 & & \\ & & & & \ddots & \\ & & & & & f_r \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{bmatrix}$$

onde cada f_i é um polinômio não constante com coeficiente lider 1 que divide o seguinte f_{i+1}.

TEOREMA 1: *Cada matriz de polinômios pode ser reduzida à forma canônica diagonal por um número finito de operações elementares.*

DEMONSTRAÇÃO: Seja G uma dada matriz de polinômios. Se $G = 0$, não há o que provar desde que 0 já está na forma desejada. Suponha portanto, que $G \neq 0$. Dentre todas as matrizes de polinômios equivalentes a G, escolha uma na qual o elemento do canto superior esquerdo é não-nulo e de grau mínimo. Seja

$$F = \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{n1} & \cdots & f_{nn} \end{bmatrix}$$

essa matriz. Mostraremos que todos os elementos da primeira linha e primeira coluna de F são divisíveis por f_{11}. Pelo Algoritmo Euclidiano, para cada $i = 2,\ldots,n$

(1) $f_{1i} = f_{11}q_i + r_i$ onde $r_i = 0$ ou $\partial r_i < \partial f_{11}$

Execute em F a seguinte operacão elementar: Some à i-ésima coluna a primeira coluna multiplicada por $-q_i$. A igualdade (1) mostra que o elemento da primeira linha e i-ésima coluna da nova matriz é r_i. Se $r_i \neq 0$, permutando a primeira e a i-ésima coluna obtemos uma matriz equivalente a F cujo elemento do canto superior esquerdo é r_i que tem grau menor do que o grau de f_{11}, o que contraria a escolha de F. Portanto $r_i = 0$. Um argumento análogo mostra que f_{11} divide todos os elementos da primeira coluna.

Com q_i como acima, execute as seguintes operações elementares em F: Some à segunda coluna a primeira multiplicada por $-q_2$; depois some à terceira coluna a primeira multiplicada por $-q_3$, e assim sucessivamente. Execute operações análogas nas linhas. Como resultado, F será transformada na matriz equivalente

$$(2) \qquad H = \begin{bmatrix} f_{11} & 0 & \cdots & 0 \\ 0 & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & h_{n2} & \cdots & h_{nn} \end{bmatrix}$$

onde h_{ij} são polinômios obviamente.

Afirmo que todos os h_{ij} são divisíveis por f_{11}. Se h_{ij} não fosse divisível por f_{11}, somando-se a i-ésima linha de H à primeira, obteríamos uma matriz $\bar{H}$ com as seguintes propriedades:

(a) $\bar{H}$ é equivalente a G;

(b) o elemento no canto superior esquerdo de $\bar{H}$ é não-nulo e de grau mínimo possível;

(c) na primeira linha de $\bar{H}$ há um elemento h_{ij} que não é divisível pelo primeiro elemento dessa linha.

Assim, pelo argumento precedente a propriedade (c) contradiz as duas primeiras, e a afirmação está provada. Demonstraremos então que para cada matriz G existe uma matriz equivalente H da forma (2), onde todos h_{ij} são divisíveis por f_{11}. Executamos agora operações elementares na matriz

BIBLIOTECA
IMECC

$$H_1 = \begin{bmatrix} h_{22} & \cdots & h_{2n} \\ \vdots & & \vdots \\ h_{n2} & \cdots & h_{nn} \end{bmatrix} .$$

Cada operação elementar de H_1 pode ser considerada uma operação elementar de H. É fácil ver que a primeira linha e a primeira coluna de H são deixadas inalteradas. Além disso, como todos os elementos de H_1 são divisíveis por f_{11}, todos os elementos da nova matriz, obtida de H_1 como resultado de operações elementares, serão também divisíveis por f_{11}.

Aplicando o resultado provado acima à matriz H_1, vemos que por operações elementares podemos obter de H_1 uma matriz da forma

$$K_1 = \begin{bmatrix} k_{22} & 0 & \cdots & 0 \\ 0 & p_{33} & \cdots & p_{3n} \\ \vdots & \vdots & & \vdots \\ 0 & p_{n3} & & p_{nn} \end{bmatrix}$$

e, consequentemente de H uma matriz da forma

$$L = \begin{bmatrix} f_{11} & 0 & 0 & \cdots & 0 \\ 0 & k_{22} & 0 & \cdots & 0 \\ 0 & 0 & p_{33} & \cdots & p_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & p_{n3} & & p_{nn} \end{bmatrix}$$

onde todos os p_{ij} são divisíveis por k_{22} e k_{22} é divisível por f_{11}. Continuando esse processo, depois de um número finito de passos obtemos a forma canônica diagonal desejada. □

Não é difícil extrair da nossa demonstração um método prático para reduzir matriz de polinômios à forma canônica diagonal. A idéia é usar operações elementares, primeiro para obter um elemento no canto superior esquerdo de grau mínimo, depois para obter zeros nos lugares restantes na primeira linha e na primeira coluna. Feito isso, aplicar o mesmo método à matriz H_1, e assim por diante.

O Teorema 1 afirma que cada classe de equivalência de matrizes contém pelo menos uma matriz canônica diagonal. A seguir, veremos um exemplo.

EXEMPLO 1: Vamos reduzir a matriz

$$\begin{bmatrix} 1-X & X^2 & X \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{bmatrix}$$

à forma canônica diagonal.

$$\begin{bmatrix} 1-X & X^2 & X \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{bmatrix} L_1 \overset{\sim}{\to} L_1+L_2 \begin{bmatrix} 1 & X^2+X & 0 \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{bmatrix} \sim$$

$$C_2 \to C_2-(X^2+X)C_1 \begin{bmatrix} 1 & 0 & 0 \\ X & -X^3-X^2+X & -X \\ 1+X^2 & -X^4-X^3-X & -X^2 \end{bmatrix} \overset{\sim}{\begin{matrix} L_2 \to L_2-XL_1 \\ L_3 \to L_3-(1+X^2)L_1 \end{matrix}}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & -X^3-X^2+X & -X \\ 0 & -X^4-X^3-X & -X^2 \end{bmatrix} C_2 \overset{\sim}{\leftrightarrow} C_3 \begin{bmatrix} 1 & 0 & 0 \\ 0 & -X & -X^3-X^2+X \\ 0 & -X^2 & -X^4-X^3-X \end{bmatrix}$$

$$L_2 \overset{\sim}{\to} -L_2 \begin{bmatrix} 1 & 0 & 0 \\ 0 & X & X^3+X^2-X \\ 0 & -X^2 & -X^4-X^3-X \end{bmatrix} C_3 \overset{\sim}{\to} C_3-(X^2+X-1)C_2 \begin{bmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & -X^2 & -X(X+1) \end{bmatrix}$$

$$\overset{\sim}{L_3 \to L_3+XL_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & -X(X+1) \end{bmatrix} \overset{\sim}{L_3 \to (-1)L_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X(X+1) \end{bmatrix}$$

O Teorema 1 de fato fornece a estrutura de um módulo M finitamente gerado sobre o anel de polinômios $k[X]$ sobre um corpo k. Como afirmamos no início deste capítulo, se M é dado por uma matriz F, então as linhas de F proporcionam relações entre geradores de F. Se F é equivalente a G e G está na forma canônica diagonal, digamos

$$\begin{bmatrix} g_1 & & 0 \\ & g_2 & \\ & & \ddots \\ 0 & & g_n \end{bmatrix}$$

com $g_i | g_{i+1}$ $\forall$ i = 1,2,...,n-1. Então M também é gerado por $u_1,u_2,\ldots,u_m$ onde $g_i u_i = 0$ $\forall$ i = 1,2,...,n e $g_i | g_{i+1}$.

Seja então $e_1,e_2,\ldots,e_n$ a base canônica de $k[X]^n$; isto é, $e_i = (0,\ldots,0,1,0,\ldots,0)$ onde 1 ocupa o i-ésimo lugar. Pode-se definir um homomorfismo de módulos $\theta : k[X]^n \to M$ por $\theta(e_i) = u_i$; então o núcleo K é dado pela matriz G; isto é, $K = \{(h_1,h_2,\ldots,h_n)$ onde g_i divide h_i, i = 1,2,...,n$\}$.

Assim M é isomorfo como $k[X]$-módulo ao produto direto

$$\frac{k[X]}{(g_1)} \times \frac{k[X]}{(g_2)} \times \ldots \times \frac{k[X]}{(g_n)}$$

onde mais ainda se tem: $g_i | g_{i+1}$, $i = 1,2,\ldots,n-1$. Note ainda mais que se $g_n = 0$ então $\frac{k[X]}{(g_n)} \simeq k[X]$ e se $g_1 = 1$, então $\frac{k[X]}{(g_1)}$ é (0).

Assim temos demonstrado o seguinte teorema, que é de suma importância:

TEOREMA 2 (TEOREMA FUNDAMENTAL PARA MÓDULOS FINITAMENTE GERADOS SOBRE $k[X]$): *Seja* M *um módulo finitamente gerado sobre* $k[X]$. *Então*

$$M \simeq k[X]^r \oplus k[X]/_{(f_1(X))} \oplus \ldots \oplus k[X]/_{(f_{n-r}(X))}$$

onde $n,r \in \mathbb{N}$, $r \leq n$ *e* $f_i | f_{i+1}$, $1 \leq i \leq n-r-1$. *Além disso os ideais* $(f_i(X))$, $1 \leq i \leq n-r$ *são unicamente determinados por* M. *De fato, os* $f_i(X)$ *são únicos, se são mônicos.*

DEMONSTRAÇÃO: Resta provar apenas a última parte do enunciado. Note que se $M \simeq \frac{k[X]}{(f_1)} \times \ldots \times \frac{k[X]}{(f_n)}$, onde os f_i, são mônicos e $f_i | f_{i+1}$ para $i = 1,2,\ldots,n-1$, então M é dado por uma matriz de relações

$$F = \begin{bmatrix} f_1 & & \\ & \ddots & \\ & & f_n \end{bmatrix}$$

na forma canônica diagonal. Logo basta mostrar que a forma canônica diagonal de uma matriz é única. Este segue do seguinte resultado como corolário.

Seja F uma matriz de polinômios de ordem n. Considere todos os menores possíveis de ordem r de F sendo $r \leq n$. Esses menores são polinômios em X. Chamaremos de máximo divisor comum desses menores e o denotaremos por $D_r(X)$ ao divisor comum de maior grau com coeficiente líder 1. Se todos os menores de ordem r são nulos, então definimos $D_r(X) = 0$. Em particular, $D_1(X)$ é o máximo divisor comum dos elementos da matriz F; $D_n(X)$ é o determinante de F dividido pelo seu coeficiente líder, a menos que $D_n(X) = 0$.

TEOREMA 3: *Se* F_1 *e* F_2 *são matrizes equivalentes de polinômios e* $D_{r1}(X)$ *e* $D_{r2}(X)$ *denotam os máximos divisores comuns dos menores de ordem* r *de* F_1 *e* F_2 *respectivamente, então* $D_{r1}(X) = D_{r2}(X)$.

DEMONSTRAÇÃO: Como F_1 e F_2 são equivalentes, F_2 pode ser obtida de F_1 por uma série de operações elementares. Suponha

inicialmente que esta série consiste de uma operação elementar . Por exemplo, seja F_2 obtida de F_1 pela multiplicação da i-ésima linha de F_1 por um escalar $\lambda \neq 0$. Os menores correspondentes de F_1 e F_2 são idênticos ou diferem por um fator λ. Como um fator constante não influencia o cálculo do máximo divisor comum, temos $D_{r1} = D_{r2}$. A situação é a mesma quando F_2 é obtida de F_1 pela multiplicação de uma coluna de F_1 por λ. Suponha agora que F_2 é obtida de F_1 por uma operação do tipo (ii) ou (iv); seja F_2 o resultado da adição da j-ésima linha multiplicada por $f(X)$ à i-ésima linha de F_1. Vamos mostrar que D_{r1} divide D_{r2}.

Os menores de F_1 e F_2 podem ser divididos em três classes. Na primeira colocamos aqueles que não contêm elementos da i-ésima linha. Nesse caso, os menores correspondentes de F_1 e F_2 são evidentemente iguais. Na segunda classe colocamos aqueles menores que contêm elementos de ambas as linhas i-ésima e j-ésima. Como um determinante não se altera se somarmos a uma linha um múltiplo de outra linha, os menores correspondentes de F_1 e F_2 são iguais também nessa classe. Finalmente, na terceira classe colocamos aqueles menores que contêm elementos da i-ésima linha mas não contêm elementos da j-ésima. Nessa classe os menores correspondentes são da forma

$$M_1 = \begin{vmatrix} \cdots\cdots\cdots \\ f_{i\nu_1} \cdots f_{i\nu_r} \\ \cdots\cdots\cdots \end{vmatrix}, \quad M_2 = \begin{vmatrix} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_{i\nu_1} + f(X).f_{j\nu_1} \cdots f_{i\nu_r} + f(X).f_{j\nu_r} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{vmatrix}$$

onde as linhas que não foram escritas são idênticas. Pela propriedade de adição de determinantes,

$$M_2 = \begin{vmatrix} \cdots\cdots\cdots \\ f_{i\nu_1} \cdots f_{i\nu_r} \\ \cdots\cdots\cdots \end{vmatrix} + f(X) \begin{vmatrix} \cdots\cdots\cdots \\ f_{j\nu_1} \cdots f_{j\nu_r} \\ \cdots\cdots\cdots \end{vmatrix} = M_1 \pm f(X) N_1 .$$

onde N_1 é algum menor da matriz F_1. Todos os menores de ordem r de F_1 são divisíveis por D_{r1}. Logo D_{r1} divide tanto M_1 como N_1. Segue-se da igualdade acima que todos os menores de ordem r de F_2 são divisíveis por D_{r1}. Isto significa que D_{r1} divide o máximo divisor comum dos menores de ordem r de F_2, isto é, D_{r1} divide D_{r2}. Aplicando a operação inversa que também é do tipo (ii) a F_2, obtemos F_1. Logo, D_{r2} divide D_{r1}, e portanto $D_{r1} = D_{r2}$. Um argumento análogo vale no caso de uma operação do tipo (iv). Desse modo o teorema fica demonstrado no caso em que F_2 é obtida de F_1 por uma operação elementar. Ora, se $D_r(X)$ não é alterado por cada operação elementar separadamente numa série, é evidente que não será alterado pela série de operações elementares. Isto prova o Teorema 2.

Consideremos os polinômios $D_1(X),\ldots,D_n(X)$ numa matriz cuja forma canônica é

$$D = \begin{bmatrix} d_1(X) & & & \\ & d_2(X) & & \\ & & \ddots & \\ & & & d_n(X) \end{bmatrix}$$

Para obter um menor de ordem r, devemos suprimir n-r linhas e n-r colunas. Se a i-ésima linha é eliminada, então a i-ésima coluna da nova matriz assim obtida contém apenas zeros. Sendo assim, para obter um menor não nulo, devemos suprimir linhas e colunas correspondentes. Logo os menores de ordem r devem ser da forma

$$\begin{vmatrix} d_{\nu_1}(X) & & & \\ & d_{\nu_2}(X) & & \\ & & \ddots & \\ & & & d_{\nu_r}(X) \end{vmatrix} = d_{\nu_1}(X)d_{\nu_2}(X)\ldots d_{\nu_r}(X), \qquad (3)$$

e $D_r(X)$ é o máximo divisor comum desses menores. Das desigualdades $1 \leq \nu_1 < \ldots < \nu_r \leq n$ segue-se que $1 \leq \nu_1$, $2 \leq \nu_2,\ldots,r \leq \nu_r$.

Assim $d_{\nu_i}(X)$ é divisível por $d_i(X)$, e isto significa que $d_{\nu_1}(X)\ldots d_{\nu_r}(X)$ é divisível por $d_1(X)\ldots d_r(X)$. Consequentemente, cada menor de ordem r da matriz D é divisível pelo menor de ordem r

$$\begin{vmatrix} d_1(X) & & \\ & \ddots & \\ & & d_r(X) \end{vmatrix} = d_1(X)\ldots d_r(X) \qquad (4)$$

Se esse menor é nulo, então todos os menores de ordem r de D são nulos e por definição $D_r(X) = 0$. Se o menor (4) é não-nulo, então os polinômios $d_1(X), \ldots, d_r(X)$ são não nulos e têm coeficientes líderes 1. Como todo menor (3) é divisível por (4), $D_r(X)$ coincide com (4). Consequentemente temos

$$D_r(X) = d_1(X)\ldots d_r(X) \qquad (5)$$

COROLÁRIO: *A forma canônica diagonal de uma matriz F é única.*

DEMONSTRAÇÃO: Sejam

$$D = \begin{bmatrix} d_1(X) & & & \\ & d_2(X) & & \\ & & \ddots & \\ & & & d_n(X) \end{bmatrix} \quad e \quad E = \begin{bmatrix} e_1(X) & & & \\ & e_2(X) & & \\ & & \ddots & \\ & & & e_n(X) \end{bmatrix}$$

duas matrizes diagonais equivalentes a F onde os $d_i(X)$ e $e_i(X)$ são mônicos e $d_i \mid d_{i+1}$ e $e_i \mid e_{i+1}$ $\forall$ i = 1,2,...,n-1. Se indicamos por $D_r(X)$ e $E_r(X)$ os máximos divisores comuns de menores de ordem r de D e E respectivamente, então $D_r = E_r$ pelo Teorema 2. Por outro lado, pela observação feita acima, $D_r = d_1 d_2 \ldots d_r$ e $E_r = e_1 e_2 \ldots e_r$. Assim $d_1 = e_1$, $d_1 d_2 = e_1 e_2, \ldots,$ $d_1 d_2 \ldots d_r = e_1 e_2 \ldots e_r$, etc. Segue-se que $d_i = e_i$, $\forall$ i = 1,2,...,n desde que todos eles são não-nulos. Assim, nesse caso, vale a unicidade da forma canônica.

Suponhamos agora que existe s, $0 \leq s \leq n-1$ tal que $d_1, d_2, \ldots, d_s \neq 0$ e $d_{s+1} = 0$. (Por definição $d_o = 1$.) Então o argumento acima mostra que $d_1 = e_1$, $d_2 = e_2, \ldots, d_s = e_s$ e $d_{s+1} = e_{s+1} = 0$. Ora, $d_{s+2} = \ldots = d_n = 0$ e $e_{s+2} = \ldots = e_n = 0$ donde segue-se que $d_i = e_i$ $\forall$ i = 1,2,...,n. Fica assim demonstrada a unicidade da forma canônica diagonal de uma matriz F. □

CAPÍTULO VI

MÓDULOS FINITAMENTE GERADOS SOBRE $\mathbf{Z}_p[[X]]$

A estrutura de módulos sobre o anel $\mathbf{Z}_p[[X]]$ se tornou importante no estudo de corpos ciclotômicos, isto é, extensões finitas e infinitas do corpo Q dos números racionais obtidas por adjunção de raízes da unidade. A adjunção de todas as raízes da unidade parece difícil de estudar. Iwasawa em 1958 iniciou o estudo de $\mathbb{Z}_p$-extensões de corpos k de números algébricos. L/k é uma $\mathbb{Z}_p$-extensão se $Gal(L/k) \tilde{=} \mathbb{Z}_p$, grupo aditivo dos inteiros p-ádicos. Se α_n é uma raiz p^n-ésima primitiva da unidade, então indique: $k_n = k(\alpha_n)$ e $k_\infty = \bigcup_{n\geq 0} k_n$. O grupo de Galois $Gal(k_\infty/k) \tilde{=} \mathbb{Z}_p \times \frac{\mathbb{Z}}{(p-1)}$. Logo existe uma extensão L/K tal que $Gal(L/k) \tilde{=} \mathbb{Z}_p$. De fato, L é o subcorpo fixo de k_∞ fixado pelo grupo $\frac{\mathbb{Z}}{(p-1)}$. Neste caso, L/K é uma $\mathbb{Z}_p$-extensão. Ora, $\mathbf{Z}_p = \lim_{\leftarrow} \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}$. $\mathbf{Z}_p \supset (p) \supset (p^2) \supset \ldots \supset (p^n) \supset \ldots \supset (0)$ e portanto temos uma cadeia ascendente de subcorpos $k = L_o \subset L_1 \subset L_2 \subset \ldots \subset L_n \subset \ldots$ $L = \cup L_n$, $Gal(L_n/k) \tilde{=} \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}$. Assim cada L_n é um Γ_n-módulo e portanto L também o é. De fato, L é um $\mathbf{Z}_p[\Gamma_n]$-módulo, onde $\mathbb{Z}_p[\Gamma_n]$ é um anel de grupo Γ_n sobre o anel $\mathbb{Z}_p$. A observação importante é que temos homomorfismos naturais $\mathbb{Z}_p[\Gamma_{n+1}] \longrightarrow \mathbb{Z}_p[\Gamma_n]$ compatíveis, de modo que $\mathbb{Z}_p[\Gamma] = \lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n]$ como anel. Como

$\mathbb{Z}_p[\Gamma] \simeq \mathbb{Z}_p[[X]]$ o anel de séries formais, via o fato $\mathbb{Z}_p[\Gamma_n] \simeq$ $\simeq \frac{\mathbb{Z}_p[X]}{(X^{p^n}-1)}$, L se torna um $\mathbb{Z}_p[[X]]$-módulo. Não é por esse fato que a estrutura de módulos finitamente gerados sobre $\mathbb{Z}_p[[X]]$ se torna interessante. O interesse real está na estrutura de uma parte (a parte p-primária) do grupo das classes de corpos L_n.

Seja F um corpo de números algébricos e H/F o corpo de classes de Hilbert; isto é, H/F é a extensão abeliana não-ramificada maximal. A Teoria de Corpos de Classes assegura que Gal(H/F) é isomorfo ao grupo de classes de ideais de F !

Agora considere apenas o p-Sylow subgrupo C_n do grupo das classes de L_n onde L/k é uma $\mathbb{Z}_p$-extensão e $k = L_o \subset L_1 \subset \ldots \subset L_n \ldots$ uma cadeia como indicada acima. Temos um homomorfismo $C_{n+1} \to C_n$ natural e portanto $C = \varprojlim C_n$ tem sentido. Um resultado de Iwasawa afirma que C é um $\mathbb{Z}_p[[X]]$-módulo finitamente gerado. A prova apresenta C como um grupo de Galois de uma p-extensão abeliana não ramificada e usa o citado resultado da Teoria de Corpos de Classes. Daí obtém-se a cardinalidade de C_n !

Assim vemos como é importante a estrutura de módulos finitamente gerados sobre o anel $\mathbb{Z}_p[[X]]$. A prova original de Iwasawa é complicada. Serre observou (Classes de Corps Cyclotomiques, d'après Iwasawa, Seminaire Bourbaki, 1958) que $\mathbb{Z}_p[[X]]$ é um anel de dimensão 2 e deduziu o resultado de Iwasawa do Teorema de estrutura de módulos finitamente gerados sobre domínios de Krull ;

este último resultado usa a teoria de divisores. Lang [6] e Washington [15] apresentam uma prova matricial e a nossa tentativa de compreender esta prova nos levou a incluir o Capítulo V. O objetivo é partir de uma matriz $m \times n$ cujas entradas são séries formais e executar operações admissíveis de maneira a conseguir uma matriz mais simples que também descreva o módulo em questão. Entram operações elementares como no Capítulo V e entram também operações "pseudo-elementares" que nos permitem omitir pedaços finitos. A justificativa para omitir esses pedaços finitos vem também da Teoria de Galois, pois o módulo em questão ao ser visto como grupo de Galois, é um grupo profinito e portanto pode ser descrito módulo grupos finitos. Topologicamente os dois são isomorfos.

No capítulo anterior usamos fortemente o algoritmo euclidiano de divisão. Na presente situação, o análogo é o Teorema de Preparação de Weierstrass que fornece um algoritmo de divisão. Apresentamos este Teorema numa situação mais geral, trabalhando com o anel de séries formais $R[[X]]$ onde R é um anél local Hausdorff completo.

1. TEOREMA DE PREPARAÇÃO DE WEIERSTRASS

Seja F um anel não-nulo. Seja $f = \sum_{i \geq 0} f_i X^i \in R[[X]]$,

$f_i \in R$. Definimos grau de f em X relativo a R e denotamos por grf como sendo grf em X se $0 \neq f \in R[X]$; $-\infty$ se $f = 0$ e ∞ se $f \notin R[X]$.

Suponha que R é um anel local cujo ideal maximal é M. Definimos *grau de Weierstrass de* $f \neq 0$ relativo a R e denotamos por $gr_w f$ como sendo o mínimo i tal que $f_i \notin M$ se $f \notin M[[X]]$; e ∞ se $f \in M[[X]]$.

Dizemos que f é R[X]-*distinguido* se, $d = gr_w f < \infty$, $f_d = 1$ e $f_i = 0$ para todo $i > d$. Note que neste caso f é um polinômio. Chamaremos f *de polinômio distinguido em* X (de grau d) com coeficientes em R.

PROPOSIÇÃO 1: *Seja* R *um anel local. Se* f, g *e* $h \in R[[X]]$ *tem-se (das definições acima) que*

(i) $gr_w fg = gr_w f + gr_w g$, *desde que* $f, g, fg \neq 0$;

(ii) $h \in M[[X]] \iff gr_w h = \infty$; $(h \neq 0)$;

(iii) h *é uma unidade em* $R[[X]] \iff gr_w h = 0$;

(iv) *Se* $f \neq 0$ *e* $g \neq 0$ *são* R[[X]]-*associados então* $gr_w f = gr_w g$;

(v) f *é distinguido* $\iff$ $grf = gr_w f < \infty$ *e* f *é mônico*;

(vi) *Se* f *é distinguido,* g *é um polinômio mônico em* X *com coeficientes em* R *e* g *divide* f *em* R[X],

então g *é distinguido.*

DEMONSTRAÇÃO: (i) Basta considerar o caso onde $gr_w f < \infty$ e $gr_w g < \infty$. Sejam $f = \Sigma f_i X^i$ e $g = \Sigma g_i X^i$. Então $fg = \Sigma h_i X^i$ onde $h_i = f_o g_i + f_1 g_{i-1} + \ldots + f_i g_o$. Suponha $gr_w f = j$ e $gr_w g = k$. Então $h_{j+k} = f_o g_{j+k} + \ldots + f_i g_k + \ldots + f_{j+k} g_o$. Como f_j e $g_k \notin M$, $f_j g_k \notin M$ e $f_\lambda g_\mu \in M$ se $(\lambda,\mu) \neq (i,k)$. Dai $h_{j+k} \notin M$. também, e para qualquer $s < j + k$, $h_s \in M$. Portanto

$$gr_w fg = j + k = gr_w f + gr_w g.$$

(ii) É a definição de $gr_w f$.

(iii) $h = \Sigma h_i X^i$ é uma unidade de $R[[X]] \Leftrightarrow h_o$ é uma unidade de $R \Leftrightarrow h_o \notin M \Leftrightarrow gr_w h = 0$.

(iv) Se f e g são $R[[X]]$-associados então $f = \delta g$ onde δ é uma unidade em $R[[X]]$. Por (i) $gr_w f = gr_w \delta g = gr_w \delta + gr_w g$. Por (ii) $gr_w \delta = 0$ e temos $gr_w f = gr_w g$.

(v) É a definição de um elemento distinguido.

(vi) Se $d = gr_w f < \infty$, $f_d = 1$ e $f_i = 0$ para todo $i > d$. Se $g|f$ em $R[X]$ então $f = rg$ com $r \in R[X]$. De $f = rg$ tem-se, $grf = grr + grg$, pois g é mônico, e $gr_w f = gr_w r + gr_w g$. Se $grg > gr_w g$ então

$$\begin{aligned} grf &> grr + gr_w g \\ &\geq gr_w r + gr_w g \\ &= gr_w f , \end{aligned}$$

uma contradição ao fato que f é distinguido. Logo $grg = gr_w g$ e sendo g mônico, g é distinguido.

TEOREMA 1: (Teorema de Preparação de Weisrstrass *Seja* (R,M) *um anel local Hausdorff completo e sejam* f *e* $g \in R[[X]]$.

(i) *Se* $gr_w f < \infty$ *então existem únicos elementos* $q \in R[[X]]$ *e* $r \in R[X]$ *tais que* $g = qf + r$ *e* $grr < gr_w f$;

(ii) *Se* f *e* g *são distinguidos então* f *e* g *são* R[[X]]*-associados se, e somente se* $f = g$;

(iii) *Se* f *é distinguido e* $g \in R[X]$ *então* $q \in R[X]$. *Se, além disso,* g *é também distinguido e* $r = 0$ *então* q *é distinguido;*

(iv) $f \notin M[[X]]$ *se, e somente se* f *é um* R[[X]]*-associado de um elemento distinguido* f^*, *isto é,* $f = \delta f^*$ *onde* δ *é uma unidade em* R[[X]]; *e nesse caso* f^* *e* δ *são unicamente determinados por* f;

(v) *Se* f *é distinguido e* $f = f_1 \ldots f_s$ *com* $f_1, \ldots, f_s$ *em* R[[X]] *então* f_i *é um* R[[X]]*-associado de um polinômio distinguido* f_i^*, $i = 1, \ldots, s$ *e* $f = f_1^* \ldots f_s^*$.

DEMONSTRAÇÃO: (i) Seja $f = \sum_{i \geq 0} f_i X^i$, $f_i \in R$ e $d = gr_w f$. Sejam $f' = \sum_{i=0}^{d-1} f_i X^i$ e $f^* = \sum_{i \geq d} f_i X^{i-d}$. Então f^* é uma unidade de

$R[[X]]$ e $f \in M[[X]]$. Daí $F = -\frac{f'}{f^*} \in [[X]]$ e $f = (X^d - F)f^*$. Sejam $Q = f^*q$ e $G = g$. Assim nossa afirmação se torna equivalente à seguinte: dados $G \in R[[X]]$ e $F \in M[[X]]$, existe único $Q \in R[[X]]$ tal que $[G-(X^d-F)Q]$ é um polinômio de grau $< d$. De fato, suponha que $g = qf+r$ e $grr < gr_w f$. Pondo-se $Q = f^*q$ temos $gr\,[G-(X^d-F)Q] = gr(g-qf) = gr\,r < d$. Reciprocamente, se existe único $Q \in R[[X]]$ com $gr\,[G-(X^d-r)Q] < \infty$, então tomando $r = G-(X^d-F)Q$ e $q = \frac{Q}{f^*}$, $qf = (X^d-F)Q$ e temos $G = g = qf+r$.

UNICIDADE DE Q: É suficiente mostrar que se $Q = \sum_{i\geq 0} Q_i X^i$, $Q_i \in R$, $gr(X^d-F)Q < d$ então $Q = 0$. Com efeito, se $Q' \in R[[XX]]$ é tal que $gr\,[G-(X^d-F)Q'] < d$ então

$$gr[G-(X^d-F)Q-(G-(X^d-F)Q')] = gr\,[(X^d-F)(Q'-Q)] < d\ .$$

Logo $Q'-Q = 0$ e daí $Q' = Q$. Ora, suponha que $Q \in M^u[[X]]$ com $u \geq 0$. Seja $e \geq 0$ um inteiro qualquer. Então o coeficiente de X^{d+e} em $(X^d-F)Q$ é zero, pois $d+e \geq d$. Por outro lado, o coeficiente de X^{d+e} em $(X^d-F)Q$ consiste de uma expressão Q_e + soma de termos da forma F_iQ_j. Como cada $Q_j \in M^u$ e cada $F_i \in M$, temos $F_iQ_j \in M^{u+1}$. Daí $Q_e \in M^{u+1}$. Como e é arbitrário segue que $Q \in M^{u+1}[[X]]$. Repetindo-se o argumento com u+1 em lugar de u, segue que $Q \in M^u[[X]]$ para todo $u \geq 0$. Isto quer dizer que para todo $i \geq 0$, os coeficientes Q_i de Q pertencem a $\bigcap_{u\geq 0} M^u$. Pelo Teorema de Krull $\bigcap_{n\geq 0} M^u = (0)$. Logo $Q = 0$.

EXISTÊNCIA: Usando o fato de que $f \in M[[X]]$, sucessivamente tentaremos encontrar $Q^{(u)} \in M^u[[X]]$ tal que $Q = Q^{(0)}+Q^{(1)}+\ldots$, isto é, Q será uma soma infinita de séries formais de maneira que Q tenha sentido. Isto é feito para garantir que $gr(G-(X^d-F)Q) < d$. Escreva $G = \sum_{i\geq 0} G_i X^i$, $F = \sum_{i\geq 0} F_i X^i$, onde $G_i \in R$ e $F_i \in M$ $\forall\, i \geq 0$. A idéia é proceder da seguinte maneira: Escrevamos $Q = Q^{(o)}+Q^{(1)}+\ldots+Q^{(u)}+\ldots$ onde os $Q^{(u)}$ são séries formais a serem definidas. Escreva $(G-(X^d-F)Q) = G-X^d(Q^{(0)}+Q^{(1)}+Q^{(2)}+\ldots)+$ $+ F(Q^{(o)}+Q^{(1)}+Q^{(2)}+\ldots)$. Note que se escolhemos $Q^{(u)} \in M^u[[X]]$, então $FQ^{(u)} \in M^{u+1}[[X]]$. Portanto $Q^{(0)}$ é escolhido tal que $gr(G-Q^{(0)}X^d) < d$, $Q^{(1)}$ escolhido tal que $gr(-Q^{(1)}X^d+FQ^{(0)}) < d$ $Q^{(2)}$ escolhido tal que $gr(-Q^{(2)}X^d+FQ^{(1)}) < d$ ... etc. e em geral uma vez escolhido $Q^{(u)}$, definimos $Q^{(u+1)}$ via $gr(-Q^{(u+1)}X^d+FQ^{(u)}) < d$. Assim se $Q^{(u)} = \sum_{e\geq 0} Q_e^{(u)} X^e$, temos:

$Q_e^{(u)} = G_{d+e}$, para todo $e \geq 0$;

$Q_e^{(u+1)} = \sum_{j=0}^{d+e} F_j\, Q_{d+e-j}^{(u)}$, para todos $u \geq 0$ e $e \geq 0$;

Isto define sucessivamente os $Q^{(u)}$ para $u \geq 0$. Assim

$$gr\,[G-Q^{(0)}X^d] < d \quad \text{e} \quad gr\,[-Q^{(u+1)}X^d+Q^{(u)}F] < d$$

para todo $u \geq 0$. Com efeito,

$$G-Q^{(0)}X^d = (G_o+G_1X+\ldots+G_{d-1}X^{d-1}+G_dX^d) - \sum_{e\geq 0} Q_e^{(0)} X^{d+e} =$$

$$= G_o+G_1X+\ldots+G_{d-1}X^{d-1}+G_dX^d+\ldots-G_dX^d-G_{d+1}X^{d+1}-\ldots = G_o+G_1X+\ldots+G_{d-1}X^{d-1} ,$$

cujo grau é menor que d . Da mesma maneira considere

$$-Q^{(u+1)}X^d+Q^{(u)}F = \sum_{e\geq 0} Q_e^{(u+1)}X^{d+e} + \left(\sum_{e\geq 0} Q_e^{(u)}X^e\right)\left(\sum_{e\geq 0} F_eX^e\right) .$$

O coeficiente de X^{d+e} deste polinômio é $Q_e^{(u+1)} + \sum_{j+k=d+e} Q_j^{(u)} F_k = 0$ da definição de $Q_e^{(u+1)}$, sempre que $e \geq 0$. Portanto $-Q^{(u+1)}X^d + Q^{(u)}F$ é um polinômio de grau menor que d . Feito isso observe que $Q^{(1)} \in M[[X]]$ e se $Q^{(u)} \in M^u[[X]]$ então $Q^{(u+1)} \in M^{u+1}[[X]]$, pois $F \in M[[X]]$ e isto vale para todo $u \geq 0$. Isto quer dizer que $Q_e^{(u)} \in M^u$ para todo $u \geq 0$ e todo $e \geq 0$. Assim para todo $e \geq 0$ a soma $\sum_{u\geq 0} Q_e^{(u)}$ existe em R, pois R é completo Hausdorff a respeito da topologia M-ádica, já que a sequência $(Q_e^{(0)} + Q_e^{(1)}+Q_e^{(2)}+\ldots+Q_e^{(u)})_u$ é uma sequência de Cauchy. Definamos $Q_e = \sum_{u\geq 0} Q_e^{(u)}$ e $Q = \sum_{e\geq 0} Q_e X^e$. Ora Q atende a nosso objetivo, pois $(G-(X^d-F)Q)$ é um polinômio de grau menor que d:

$$G-(X^d-F)Q = \lim_{u\to\infty} (G-(X^d-F)(\sum_{j=0}^{u} Q^{(j)})) = \lim_{u\to\infty} (T_u),$$

digamos, onde

$$T_{u+1} = G-(X^d-F)(\sum_{j=0}^{u+1} Q^{(j)}) = G-X^dQ^{(0)}+FQ^{(0)}-X^dQ^{(1)}+\ldots$$
$$+ FQ^{(u)}-X^dQ^{(u+1)}+FQ^{(u+1)}$$
$$= \text{um polinômio } f_{u+1} \text{ de grau menor que } d + FQ^{(u+1)}.$$

Ora, a sequência (T_u) tem um limite em $R[[X]]$ donde a sequência de polinômios (f_u) é uma sequência de Cauchy. Ela ou é eventualmente constante ou tem um polinômio f de grau menor que d como limite. De qualquer modo $(G-(X^d-F)Q)$ é um polinômio de grau menor que d. Isto mostra (i).

(ii) Suponha que f e g $R[[X]]$-associados. Então $g = \delta f$ onde δ é uma unidade em $R[[X]]$. Pela Proposição 1 $gr\ g = gr_w\ g = gr_w f = gr\ f$. Como f e g são mônicos (pois são distinguidos), temos $gr(f-g) < gr_w f$. Além disso podemos escrever $f-g = 0.f + (f-g) = (1-\delta)f+0$ (duas decomposições de f-g como em (i)). Pela unicidade em (i) segue-se que $f-g = 0$, isto é, $f = g$.

(iii) Se f é distinguido então $gr_w f = d < 0$, $f_d = 1$ e $f_i = 0$ para todo $i > d$. Tome $g \in R[X]$. Por (i) existem únicos q e $r \in R[[X]]$ tais que $g = qf+r$. Por outro lado, f é também um elemento de $R[X]$ de grau d com $f_d = 1$. Pelo algoritmo Euclidiano existem únicos q' e r' em $R[X]$ (únicos) tais que $g = q'f+r'$. Da unicidade da representação em $R[[X]]$ segue-se que $q = q' \in R[X]$. Para a segunda parte, se g é também distinguido e $r = 0$ então q divide g em $R[X]$, isto é, $g = qf$ e como q é mônico (pois g e f o são) temos da Proposição 1(vi) que q é também distinguido.

(iv) $\Leftarrow$ f* distinguido $\Leftrightarrow$ $gr_w f^* = d < \infty$. Como f e f* são $R[[X]]$-associados, pela Proposição 1(iv) $gr_w f = gr_w f^* = d < \infty$ e

portanto $f \notin M[[X]]$.

=> Suponhamos agora que $f \notin M[[X]]$. $d = gr_w f < \infty$. Seja $g = X^d$ em (i). Então $X^d = qf+r$ com $gr\ r < gr_w f = d$. Afirmamos: $r \in M[[X]]$. Caso contrário, $gr_w r < d$. Como $X^d - r = qf$,

$$gr_w qf = gr_w q + gr_w f = gr_w(X^d - r) = gr_w r < d ,$$

logo $gr_w q < 0$, um absurdo. $gr_w r$ não pode ser $\geq d$ pois $r_i = 0 \in M$ para qualquer $i \geq d$. Seja $f^* = X^d - r$. Então f^* é um polinômio distinguido de grau d e $f^* = X^d - r = qf$. Logo $gr_w f^* = d = gr_w q + gr_w f$ o que implica $gr_w q = 0$ e q é unidade.

f^* e q são unicamente determinados por f. Com efeito, se f' é outro polinômio distinguido associado a f e g uma outra unidade tais que $\delta f^* = f = gf'$, então $f^* = \delta^{-1} gf' = \delta' f'$. Por (ii) $f^* = f'$. Daí $\delta = g$.

(v) f distinguido <=> $gr\ f = gr_w f < \infty$ e f mônico. Note que nenhum $f_i \in M[[X]]$. Pela Proposição 1(i), $gr_w f = gr_w f_1 + \ldots + gr_w f_s < \infty$ o que implica $gr_w f_i < \infty$ para todo $i = 1,2,\ldots,s$. Pela Proposição 1 (ii), $f_i \notin M[[X]]$. Logo por (iv) f_i é associado a um polinômio distinguido f_1^*. Ora

$$gr(f_1^* \ldots f_j^*) = grf_1^* + \ldots + grf_s^* = gr_w f_1^* + \ldots + gr_w f_s^* = gr_w(f_1^* \ldots f_s^*) .$$

Portanto $f_1^* \ldots f_s^*$ é distinguido associado a $f = f_1 \ldots f_s$. Por (ii) segue-se que $f = f_1^* \ldots f_s^*$.

Do Teorema 1 seguem imediatamente os resultados análogos para o anel $\mathbb{Z}_p$ dos inteiros p-ádicos, sendo p um número primo $\geq$ 2. São desses que precisaremos no parágrafo seguinte.

TEOREMA 2. 1) (ALGORITMO DA DIVISÃO EM $\mathbb{Z}_p[[X]]$: *Se* $f,g \in \mathbb{Z}_p[[X]]$ *e* $p \nmid f$ *então existem* $q \in \mathbb{Z}_p[[X]]$ *e* $r \in \mathbb{Z}_p[X]$ *um polinômio, tais que* $g = qf+r$ *com* $gr\ r < gr_w f$. *Aqui, se* $n = gr_w f$, *então* $f = a_o+a_1X+\ldots+a_{n-1}X^{n-1}+a_nX^n+\ldots$ *onde* $p \nmid a_n$ *e* $p \mid a_i$, $i = 0,1,2,\ldots,n-1$.

2) TEOREMA p-ÁDICO DE PREPARAÇÃO DE WEIERSTRASS): *Seja* $f(X) = \sum_{i=0}^{\infty} a_iX^i$ *onde* $p \mid a_o,a_1,\ldots,a_{n-1}$ *e* $p \nmid a_n$ $(n \geq 0)$ *tal que* $gr_w f = n$. *Então* $f(X)$ *pode ser escrito de maneira única como* $f(X) = \varepsilon(X)P(X)$ *onde* $\varepsilon(X)$ *é uma unidade de* $\mathbb{Z}_p[[X]]$ *e* $P(X)$ *é um polinômio distinguido de* $\mathbb{Z}_p[X]$. $P(X) = X^n+b_{n-1}X^{n-1}+\ldots+b_1X+b_o$ *onde* $p \mid b_i$, $i = 0,1,\ldots,n-1$.

3) *Mais geralmente, se* $f(X) \in \mathbb{Z}_p[X]$ *com* $f \neq 0$, *então* f *pode ser escrito de maneira única como* $f(X) = p^t\varepsilon(X)P(X)$ *onde* $t \geq 0$ *e* $\varepsilon(X)$ *é uma unidade de* $\mathbb{Z}_p[[X]]$ *e* $P(X)$ *é um polinômio distinguido de* $\mathbb{Z}_p[X]$.

4) *Mais ainda se* f *é um polinômio em* 3) *então* $\varepsilon(X)$ *também é um polinômio.*

5) $\mathbb{Z}_p[[X]]$ *é um anel fatorial cujos elementos irredutíveis são*

BIBLIOTECA
IMECC

associados de p *ou de polinômios distinguidos irredutíveis.*

2. ESTRUTURA DE MÓDULOS FINITAMENTE GERADOS SOBRE $\mathbb{Z}_p[[X]]$

Vamos tratar agora da estrutura de módulos finitamente gerados sobre $\mathbb{Z}_p[[X]]$. Seja $\Lambda = \mathbb{Z}_p[[X]]$ e M um Λ-módulo finitamente gerado sobre Λ. Nossa meta é descrever a estrutura de M em termos de ideais de Λ como no caso do Teorema 2 do Capítulo V. Felizmente isto é possível módulo pedaços finitos. O pseudo-isomorfismo é o mecanismo que alcança esta descrição. O Teorema 3 descreve esta estrutura.

LEMA 1: *Suponha que* $f,g \in \Lambda$ *são relativamente primos. Então o ideal* (f,g) *é de índice finito em* Λ.

DEMONSTRAÇÃO: Considere o ideal (f,g) e seja h um elemento não nulo deste ideal de menor grau. Pelo Teorema 2, existem um inteiro $\mu \geq 0$ e um polinômio distinguido H e uma unidade $U(X) \in \Lambda$ tais que $h = p^{\mu}U(X)H(X)$. Multiplicando-se pelo inverso de $U(X)$, pode-se supor que $h = p^{\mu}(X)H(X)$. (Repare que o novo $h \in (f,g)$ e o grau do novo h não muda.) Afirmamos que $H = 1$: Se não, aplique o algoritmo de divisão a f e H. Assim, $f = Hq+r$, onde $gr\ r < gr\ H$ e $p^s f = p^s Hq + p^s r = hq + p^s r$ donde $p^s r \in (f,g)$ com $gr\ p^s r < gr\ h$. Logo $r = 0$ ou seja H divide f. Da mesma maneira H divide g. Mas f e g são primos entre si - uma contradição. Logo $H = 1$. Assim temos $h = p^s \in (f,g)$. Se $s = 0$,

então $(f,g) = \Lambda$ e a conclusão do Lema segue. Se $s > 0$ pode-se supor que p não divide ambos f e g; digamos p não divide f. Portanto $f = U_1(X)f_1(X)$ onde f_1 é um polinômio distinguido. Multiplicando-se ainda pelo inverso de $U_1(X)$, pode-se supor que f é distinguido. Assim $(p^s,f) \subseteq (f,g)$. Ora (p^s,f) é um ideal de índice finito:

$$\frac{\Lambda}{(p^s,f)} \simeq \mathbb{Z}_p[[X]]/(f) \simeq \frac{\mathbb{Z}_p[[X]/(f)}{(\bar{p}^s)}$$

Ora pelo algoritmo de divisão todo elemento de Λ é congruente módulo f a um polinômio de grau menor que o de f. Se passamos agora módulo $(\bar{p}^s)$, então um conjunto de representantes de $\frac{\mathbb{Z}_p[[X]]}{(f)} / (\bar{p}^s)$ consiste de $\{\bar{a}_o+\bar{a}_1\bar{X}+\bar{a}_2\bar{X}^2+\ldots+\bar{a}_{m-1}\bar{X}^{m-1}\}$ onde $m = gr\ f$ e $\bar{a}_i \in \mathbb{Z}_p(p^s) \simeq \frac{\mathbb{Z}}{(p^s)}$. Assim o índice de $\frac{\Lambda}{(f,p^s)}$ é $p^s m$, que é finito. Como $(f,p^s) \subseteq (f,g)$ segue que (f,g) é de índice finito.

LEMA 2: *Suponha que* $f,g \in \Lambda$ *são elementos primos entre si. Então*

(i) *A aplicação natural* $\Lambda/(fg) \longrightarrow \Lambda/(f) \oplus \Lambda/(g)$ *definida por* $\bar{c} \longmapsto (\bar{c},\bar{c})$ *onde* $c \in \Lambda$ *e barra indica classe módulo é uma injeção, cujo Cokernel é finito.*

(ii) *Existe uma injeção* $\Lambda/(f) \oplus \Lambda/(g) \longrightarrow \Lambda/(fg)$ *cujo Cokernel é finito.*

DEMONSTRAÇÃO: (i) A aplicação natural $\theta : \bar{c} \longrightarrow (\bar{c},\bar{c})$ é uma injeção pois $\theta(\bar{c}) = 0$ se e somente se f e g dividem c. Como f e g são primos entre si e Λ é um domínio fatorial, segue que $fg|c$ e logo $\bar{c} = 0$. Portanto θ é uma injeção. Para a segunda afirmativa de (i), primeiro mostremos que se $I = (f,g)$ o ideal gerado por f e g em Λ, e $(a,b) \in \Lambda \times \Lambda$. Então $(\bar{a},\bar{b}) \in \text{Im } \theta$ se e somente se $a-b \in I$. Seja $a-b \in I$. Escreva $a-b = Af+Bg$ com $A,B \in \Lambda$. Então $a-Af = b+Bg = c$, digamos e evidentemente

$$\theta(\bar{c}) = \theta(\overline{a-Af}) = \theta(\overline{b+Bg}) = (\overline{a-Af},\overline{b+Bg}) \in \frac{\Lambda}{(f)} \times \frac{\Lambda}{(g)} = (\bar{a},\bar{b}).$$

Reciprocamente, se $(\bar{a},\bar{b}) = \theta(\bar{c})$, então $c-a = fA$ e $c-b = gB$ para algum $A,B \in \Lambda$. Daí $c = a+fA = b+gB$ e $a-b \in I$. Ora pelo Lema 1, $\frac{\Lambda}{(f,g)}$ é finito. Sejam $r_1,r_2,\ldots,r_n \in \Lambda$ um sistema completo de representantes de classes módulo (f,g) de Λ. Então $\{(\bar{0},\bar{r}_i)\}_{1\leq i\leq n}$ é um sistema completo de representantes de Cokernel de θ. Com efeito, se $(\bar{a},\bar{b}) \in \frac{\Lambda}{(f)} \times \frac{\Lambda}{(g)}$, seja $r_i \in \Lambda$ tal que $a-b \equiv -r_i \pmod{(f,g)}$. Então pela nossa afirmação anterior, $(\bar{a},\overline{b-r_i}) \in \text{Im } \theta$ ou seja $(\bar{a},\bar{b}) \equiv (\bar{0},\bar{r}_i)$ (módulo Im θ) em $\frac{\Lambda}{(f)} \times \frac{\Lambda}{(g)}$. Por outro lado, $(\bar{0},\bar{r}_i) \not\equiv (\bar{0},\bar{r}_j)$ (mód. Im θ) se $i \neq j$, pois $(\bar{0},\bar{r}_i) \equiv (\bar{0},\bar{r}_j)$ (mód Cokernel θ) se e somente se $(\bar{0},\overline{r_i-r_j}) \in \text{Im } \theta$. Isto é possível se e somente se $r_i-r_j \in I$ o que não é possível se $i \neq j$. Assim θ é uma aplicação cujo Cokernel é finito.

(ii) Pela primeira parte se $M = \theta(\frac{\Lambda}{(fg)}$ e $N = \frac{\Lambda}{(f)} \oplus \frac{\Lambda}{(g)}$, en-

tão $M \subseteq N$ e $M \tilde{=} \frac{\Lambda}{(fg)}$; também N/M é finito. Seja P um polinômio distinguido (não-constante) relativamente primo em relação a fg. Mostramos que existe um inteiro positivo k tal que a multiplicação por P^k define uma injeção $N \xrightarrow{P^k} M$ cujo Cokernel é finito.

Seja $(\bar{x},\bar{y}) \in N$. Como N/M é finito e $\{P^i(\bar{x},\bar{y})\}_{i=0}^{i=\infty} \subseteq N$, existem inteiros $0 \leq i < j$ tais que $P^i(\bar{x},\bar{y}) \equiv P^j(\bar{x},\bar{y})$ (mód. M) ou seja $(1-P^{j-1})\, P^i(\bar{x},\bar{y}) \in M$. Mas $1-P^{j-1}$ é uma unidade de Λ, pois $j \neq i$ e portanto P^{j-i} é um polinômio distinguido não-constante. Assim $P^i(\bar{x},\bar{y}) \in M$. Ora, N é um Λ-módulo finitamente gerado por $(\bar{1},\bar{0})$ e $(\bar{0},\bar{1})$. Portanto existe um inteiro $k \geq 0$ tal que $P^k(\bar{1},\bar{0}) \in M$ e $P^k(\bar{0},\bar{1}) \in M$ donde $P^k N \subseteq M$. Assim $\varphi : N \xrightarrow{P^k} M$ é uma aplicação de N em M. φ é injetiva, pois se $P^k(\bar{x},\bar{y}) = 0$ em M então f divide $P^k x$ e g divide $P^k y$; como P e fg são primos entre si, f divide x e g divide y ou seja $(\bar{x},\bar{y}) = (\bar{0},\bar{0})$. Daí φ é injetiva. O composto de φ com o isomorfismo $M \tilde{=} \frac{\Lambda}{(fg)}$ define a desejada injeção ψ: $\frac{\Lambda}{(f)} \times \frac{\Lambda}{(g)} \longrightarrow \frac{\Lambda}{(fg)}$. Ora $\psi(\bar{1},\bar{1}) = \overline{P^k}$. Portanto se $J = (P^k, fg)$ o ideal gerado por P^k e fg em Λ, então $\bar{J} \subseteq \text{Im}\ \psi \subseteq \frac{\Lambda}{(fg)}$. Ora, $\text{Coker}\ \psi = \frac{\Lambda/(fg)}{\text{Im}\ \psi}$ é uma imagem homomórfica de $\frac{\Lambda/(fg)}{\bar{J}} \simeq \frac{\Lambda}{J}$ e $\frac{\Lambda}{J}$ é finito pelo Lema 1 pois fg e P^k são primos entre si. Portanto Coker ψ também é finito.

DEFINIÇÃO: *Dizemos que dois Λ-módulos de M e M' são pseudo-*

isomorfos e denotaros por $M \sim M'$, *se existe um homomorfismo* $M \longrightarrow M'$ *com núcleo e co-núcleo finitos.*

A composição de dois pseudo-isomorfismos é um pseudo-isomorfismo.

Em termos desta definição, o Lema 2 afirma que $\frac{\Lambda}{(f)} \times \frac{\Lambda}{(g)} \sim \frac{\Lambda}{(fg)}$ e $\frac{\Lambda}{(fg)} \sim \frac{\Lambda}{(f)} \times \frac{\Lambda}{(g)}$ se f,g são primos entre si. Cabe observar que em geral $\sim$ não é uma relação de equivalência; se $M \sim M'$ não decorre que $M' \sim M$!

Nossa meta é descrever a estrutura de módulos finitamente gerados sobre o anel $\mathbb{Z}_p[[X]]$. Este teorema foi primeiramente demonstrado por Iwasawa. Existe uma prova de Serre que usa o fato de que nosso anel $\mathbf{Z}_p[[X]]$ é um domínio noetheriano de Krull de dimensão 2 e usa a teoria de divisores (Ver Bourbaki, N., Algèbre Commutative, Chap. 7, Diviseurs: Hermann, Paris, 1965).

Nossa prova é baseada no livro de Lang [6], onde ele dá uma prova matricial. Esta abordagem é baseada no espírito do Capítulo V, que serve de modelo. Além de operações que ali comparecem, entram mais 3 operações aqui, uma vez que o Teorema da estrutura em questão trata de pseudo-isomorfismo e não de isomorfismo. Isto quer dizer que o módulo em questão é descrito via um homomorfismo $\theta : M \longrightarrow M'$ onde M' tem uma estrutura simples como no Capítulo V, e onde $\ker \theta$ e $\operatorname{coker} \theta$ são finitos. Portanto a informação é módulo dois pedaços finitos.

Mais uma vez a custo de repetição desenvolvemos a filosofia

que está atrás da abordagem matricial.

Seja M um módulo finitamente gerado sobre Λ com geradores $u_1,\ldots,u_n$. Então existe um homomorfismo sobrejetor θ do Λ-módulo Λ^n em M tal que $\theta(y_i) = u_i$ para todo $i = 1,\ldots,n$ onde $y_1 = (1,0,\ldots,0),\ldots,y_n = (0,\ldots,0,1)$. Seja $K = \ker \theta$. Pelo Teorema Fundamental do Isomorfismo, $M \simeq \Lambda^n/K$. Como K é submódulo do Λ-módulo Λ^n e Λ é Noetheriano, K é finitamente gerado (Lang [5]). Sejam $\lambda_1 = (\lambda_{11},\ldots,\lambda_{1n}),\ldots,\lambda_m = (\lambda_{m1},\ldots,\lambda_{mn})$ os geradores de K. Então M pode ser representado pela matriz m x n

$$F = \begin{bmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & & \vdots \\ \lambda_{m1} & \cdots & \lambda_{mn} \end{bmatrix} .$$

Como cada linha dessa matriz é um elemento do núcleo do homomorfismo θ, temos que para todo $i = 1,\ldots,m$

$$\theta(\lambda_{i1},\ldots,\lambda_{in}) = 0$$

isto é,

$$(*) \qquad \lambda_{i1}\, u_1 + \ldots + \lambda_{in}\, u_n = 0 \quad .$$

Assim $M = [u_1,\ldots,u_n]$ é determinado pela matriz $F = [\lambda_{ij}]_{m\,x\,n}$ e relações (*). Aqui a matriz F é também chamada de matriz de

relações do módulo M. Desse modo, um módulo finitamente gerado sobre Λ é determinado por uma matriz de relações.

Procuraremos, como no capítulo anterior, um conjunto de geradores e um conjunto de relações as mais simples possíveis.

Vejamos a seguir as operações básicas permitidas com linhas e colunas. Primeiro aquelas que correspondem a mudar geradores de F e M que foram usadas para $k[X]$.

OPERAÇÃO A: *Podemos permutar linhas ou permutar colunas.*

OPERAÇÃO B: *Podemos somar a uma linha (ou coluna) um múltiplo de outra linha (ou coluna). Em particular, se* $\lambda' = q\lambda + r$ *então*

$$\begin{bmatrix} \vdots & \vdots \\ \lambda & \cdots \; r \; \cdots \\ \vdots & \vdots \end{bmatrix} \xrightarrow[c_r + qc_l]{} \begin{bmatrix} \vdots & \vdots \\ \lambda & \cdots \; \lambda' \; \cdots \\ \vdots & \vdots \end{bmatrix} .$$

OPERAÇÃO C: *Podemos multiplicar uma linha ou coluna por um elemento unidade de* Λ.

Agora as operações adicionais onde entram os pseudo-isomorfismos:

OPERAÇÃO I: *Se F contém uma linha* $(\lambda_{11}, p\lambda_{12}, \ldots, p\lambda_{1n})$ *com*

$p \nmid \lambda_{11}$, *então podemos trocar* F *pela matriz* F' *cuja primeira linha é* $(\lambda_{11}, \lambda_{12}, \ldots, \lambda_{1n})$ *e as demais linhas são as de* F *com os primeiros elementos multiplicados por* p.

$$\begin{bmatrix} \lambda_{11} & p\lambda_{12} & \cdots & p\lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & & \vdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \end{bmatrix} \longrightarrow \begin{bmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ p\lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & & \vdots \\ p\lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \end{bmatrix} = F' .$$

Em particular, se $\lambda_{12} = \ldots = \lambda_{1n} = 0$ *então podemos multiplicar* $\lambda_{21}, \ldots, \lambda_{m1}$ *por uma potência arbitrária de* p.

Fornecemos uma justificativa da OPERAÇÃO 1.

DEMONSTRAÇÃO: Precisamos mostrar que existe um pseudo-isomorfismo $\theta : M \longrightarrow M'$ onde M e M' são definidos por matrizes F e F' respectivamente (tendo n geradores em cada caso). Assim M é gerado por $u_1, u_2, \ldots, u_n$ satisfazendo às relações

$$(*) \quad \begin{cases} \lambda_{11}u_1 + p\lambda_{12}u_2 + p\lambda_{13}u_3 + \ldots + p\lambda_{1n}u_n = 0 \\ \lambda_{21}u_1 + \lambda_{22}u_2 + \ldots \quad \ldots + \lambda_{2n}u_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \lambda_{m1}u_1 + \lambda_{m2}u_2 + \ldots \quad + \lambda_{mn}u_n = 0 \end{cases}$$

M' é gerado por n geradores $v_1, v_2, \ldots, v_n$ onde

$$(**) \quad \begin{cases} \lambda_{11}v_1 + \lambda_{12}v_2 + \ldots + \lambda_{1n}u_n = 0 \\ p\lambda_{21}v_1 + \lambda_{22}v_2 + \ldots + \lambda_{2n}v_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p\lambda_{m1}v_1 + \lambda_{m2}v_2 + \ldots + \lambda_{mn}v_n = 0 \end{cases}$$

Em primeiro lugar tomamos $M' = M + \Lambda v = \Lambda v_1 + \ldots + \Lambda v_n + \Lambda v$ onde os v_i satisfaçam as mesmas relações (*) dos geradores de M e

$$(***) \quad \begin{cases} -v_1 + pv = 0 \\ \lambda_{12}u_2 + \lambda_{13}u_3 + \ldots + \lambda_{1n}u_n + \lambda_{11}v = 0 \end{cases}.$$

Definimos $\theta : M \longrightarrow M'$ por $\theta(u_i) = v_i$, $\forall\, i = 1,2,\ldots,n$. θ é bem definida, pois ambos os u_i e v_i satisfazem as mesmas relações.

Afirmo que θ é uma injeção. Se $m \in M$ e $\theta(m) = 0$, então $m = \mu_1\mu_1 + \ldots + \mu_n\mu_n$ para algum $\mu_i \in \Lambda$ e $\theta(m) = \mu_1 v_1 + \ldots + \mu_n v_n$ em M'. $\theta(m) = 0$ em M' $\Rightarrow$ $\theta(m)$ é uma combinação linear de linhas de relações definidas por (*) e (***). A matriz de relações de M' usando os geradores $v_1, v_2, \ldots, v_n$ e v é uma matriz $(m+2) \times (n+1)$. Se indicamos por $r_1, r_2, \ldots, r_m$ as linhas de F então existem escalares $a_1, a_2, \ldots, a_m$, a e b $\in \Lambda$ tais que

$$\theta(m) = \left[a_1(\vec{r}_1,0) + a_2(\vec{r}_2,0) + \ldots + a_m(\vec{r}_m,0) + a(-1,0,\ldots,0,p) + b(0,\lambda_{12},\ldots,\lambda_{1n},\lambda_{11})\right] \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \\ v \end{bmatrix} .$$

Isto é simplesmente uma maneira de dizer que $\theta(m)$ pertence ao módulo de relações K' definindo M' e dado por (*) e (***). Os geradores de K' são as linhas da matriz

$$\begin{bmatrix} (\vec{r}_1,0) \\ \vdots \\ (\vec{r}_m,0) \\ (-1,0,\ldots,0,p) \\ (0,\lambda_{12},\ldots,\lambda_{1n},\lambda_{11})) \end{bmatrix} = \begin{bmatrix} \lambda_{11} & p\lambda_{12} & \cdots & p\lambda_{1n} & 0 \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} & 0 \\ -1 & 0 & \ldots & 0 & p \\ 0 & \lambda_{12} & \cdots & \lambda_{1n} & \lambda_{11} \end{bmatrix} .$$

Logo o vetor $\theta(m)$ é uma combinação linear das linhas dessa última matriz. Ora se $m = \mu_1 u_1 + \ldots + \mu_n u_n$, então $\theta(m) = \mu_1 v_1 + \ldots + \mu_n v_n$. Logo

$$(\mu_1,\mu_2,\ldots,\mu_n,0) = a_1(\vec{r}_1,0) + a_2(\vec{r}_2,0) + \ldots + a_m(\vec{r}_m,0) + a(-1,0,\ldots,0,p) + b(0,\lambda_{12},\ldots,\lambda_{1n},\lambda_{11}) .$$

Comparando-se os últimos componentes $0 = ap+b\lambda_{11}$. Como $p\nmid\lambda_{11}$, $p|b$ e $\lambda_{11}|a$. Daí $-\frac{a}{\lambda_{11}} = \frac{b}{p} = c \in \Lambda$. Substituindo-se $-a = c\lambda_{11}$ e $b = cp$ temos

$$(\mu_1,\mu_2,\ldots,\mu_n) = (a_1\vec{r}_1 + a_2\vec{r}_2+\ldots+a_m\vec{r}_m +$$

$$+ \underbrace{c(\lambda_{11},0,\ldots,0)}_{\text{n entradas}} + c(0,p\lambda_{12},p\lambda_{13},\ldots,p\lambda_{1n})$$

$$= a_1r_1 + a_2r_2+\ldots+a_mr_m + c\,r_1 \quad \text{(repare que os } r_i \text{ são vetores com n entradas)}$$

$$= (a_1+c)\vec{r}_1 + a_2\vec{r}_2+\ldots+a_m\vec{r}_m .$$

Isto mostra que $(\mu_1,\mu_2,\ldots,\mu_n)$ é uma combinação linear de linhas da matriz F que é a matriz de relações de M. Logo $m = \mu_1u_1+\mu_2u_2+\ldots+\mu_nu_n$ pertence a K, o módulo de relações de M. Logo $m = 0$ em M. Daí $\theta : M \longrightarrow M'$ é uma injeção. Portanto $\ker\theta = (0)$ é finito.

Vamos mostrar que $\operatorname{coker}\theta$ é finito.

Primeiro observe que $-v_1+pv = 0$ e $\lambda_{12}v_2 +\ldots+ \lambda_{1n}v_n+\lambda_{11}v = 0$ e $\theta(M) = [v_1,\ldots,v_n]$ (gerado por v_i). Logo $pM' \subseteq \theta(M)$ pois $(pv_i) \subseteq \theta(M)$ e $(pv)\subseteq\theta(M)$. Da mesma maneira $\lambda_{11}M' \subseteq \theta(M)$. Portanto $\frac{M'}{\theta(M)}$ é anulado pelo ideal (p,λ_{11}). Ora p e λ_{11} são primos entre si e portanto $\frac{\Lambda}{(p,\lambda_{11})}$ é finito pelo Lema 1. M' é

um módulo finitamente gerado sobre Λ por $v_1, v_2, \ldots, v_n$ e v, e portanto $\frac{M'}{\theta(M)}$ é finitamente gerado sobre $\frac{\Lambda}{(p,\lambda_{11})}$ por $\bar{v}$. Como $\frac{\Lambda}{(p,\lambda_{11})}$ é finito, então $\frac{M'}{\theta(M)} = \frac{\Lambda}{(p,\lambda_{11})}\bar{v}$ é finito. Logo coker θ é finito. Assim θ é um pseudo-isomorfismo.

Vamos mostrar agora que a matriz de relações M' pode ser dada pela matriz $m \times n$ F'.

Ora $M' = [v_1, v_2, \ldots, v_n, v]$ com relações (*) e
($(n+1)$ geradores)

$$(***) \quad \begin{cases} -v_1 + pv = 0 \\ \lambda_{12}v_2 + \ldots + \lambda_{1n}v_n + \lambda_{11}v = 0 \end{cases}$$

Logo $M' = [v_2, v_3, \ldots, v_n, v] = [v, v_2, v_3, \ldots, v_n]$.
(n geradores)

A primeira linha de (*) dá

$$\lambda_{11}v_1 + p\lambda_{12}v_2 + \ldots + p\lambda_{1n}v_n = 0 .$$

Mas $v_1 = pv$ dá

$$p(\lambda_{11}v + \lambda_{12}v_2 + \ldots + \lambda_{1n}v_n) = 0 .$$

Esta relação já está incluída na 2ª relação de (***). Portanto podemos tomar a primeira linha da matriz de relações de M' como $(\lambda_{11}, \lambda_{12}, \ldots, \lambda_{1n})$. Como $v_1 = pv$, as outras linhas de (*) são as mesmas linhas correspondentes de F com os elementos da primeira

coluna multiplicados por p. Por exemplo,

$$\lambda_{21}v_1 + \lambda_{22}v_2 + \ldots + \lambda_{2n}v_n = 0$$

se torna

$$p\lambda_{21}v + \lambda_{22}v_2 + \ldots + \lambda_{2n}v_n = 0 ,$$

dando

$$(p\lambda_{21}, \lambda_{22}, \ldots, \lambda_{2n}) .$$

Logo F' pode ser tomada como matriz de relações de M'. □

OPERAÇÃO II: *Se todos os elementos da primeira coluna de* F *são divisíveis por* p^k *e se a primeira linha* $p^k\lambda_{11}, \ldots, p^k\lambda_{1n}$ *com* $p \nmid \lambda_{11}$, *então podemos mudar para a matriz* $\begin{bmatrix} F' & 0 \\ 0 & p^k \end{bmatrix}$ *onde* F' *é obtida de* F *por substituição da primeira linha* $(p^k\lambda_{11}, \ldots, p^k\lambda_{1n})$ *por* $(\lambda_{11}, \ldots, \lambda_{1n})$. *Isto é,*

$$F = \begin{bmatrix} p^k\lambda_{11} & p^k\lambda_{12} & \cdots & p^k\lambda_{1n} \\ p^k\lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p^k\lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \end{bmatrix} \longrightarrow \begin{bmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} & 0 \\ p^k\lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p^k\lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & \ldots & 0 & p^k \end{bmatrix}$$

DEMONSTRAÇÃO da justificativa da Operação II: Seja M gerado por $u_1,u_2,\ldots,u_n$ e seja F a matriz de relações de M. Seja M' gerado por $v_1,v_2,\ldots,v_n$ e v onde G', a matriz de M' é

$$G' = \left[\begin{array}{cccc|c} & & F & & 0 \\ \hline p^k & 0,\ldots & & & -p^k \\ 0 & \lambda_{12} & \lambda_{13} \cdots & \lambda_{1n} & \lambda_{11} \end{array}\right].$$

Isto é, $v_1,\ldots,v_n$ satisfazem as mesmas relações que $u_1,u_2,\ldots,u_n$ na matriz F e, além disso,

$$(***) \quad \begin{cases} p^k v_1 - p^k v = 0 \\ \lambda_{12}v_2 + \lambda_{13}v_3 + \ldots + \lambda_{1n}v_n + \lambda_{11}v = 0 \ . \end{cases}$$

Como no caso da Operação I, definimos um homomorfismo $\theta : M \to M'$ por $\theta(u_i) = v_i$, $i = 1,2,\ldots,n$. θ é bem definido pois F faz parte de G'.

Afirmamos que θ é novamente uma injeção. De fato, seja $m = \mu_1u_1+\ldots+\mu_nu_n \in M$ tal que $\theta(m) = \mu_1v_1+\ldots+\mu_nv_n = 0$ em M'. Logo $(\mu_1,\mu_2,\ldots,\mu_n,0)$ é uma combinação linear de $(\vec{r}_1,0),(\vec{r}_2,0),\ldots,(\vec{r}_m,0)$, $(p^k,0,\ldots,0,-p^k)$ e $(0,\lambda_{12},\lambda_{13},\ldots,\lambda_{1n},\lambda_{11})$, onde r_i é a i-ésima linha de F; isto porque $(\mu_1,\ldots,\mu_n,0)$ pertence ao módulo de relações K' de M' gerado pelas linhas de G' .

Logo existem escalares $a_1,a_2,\ldots,a_m$, a e b $\in \Lambda$ tais que

$$(\mu_1,\mu_2,\ldots,\mu_n,0) = a_1(\vec{r}_1,0) + a_2(\vec{r}_2,0) +\ldots+ a_m(\vec{r}_m,0) + a(p^k,0,\ldots,0,-p^k) + b(0,\lambda_{12},\ldots,\lambda_{1n},\lambda_{11}) .$$

Daí, $0 = -ap^k+b\lambda_{11}$. Ora $p\dagger\lambda_{11} \Rightarrow p^k|b$ e $\lambda_{11}|a$. Logo $\frac{a}{\lambda_{11}} = \frac{b}{p^k} = c \in \Lambda$, donde

$$\begin{aligned}(\mu_1,\mu_2,\ldots,\mu_n) &= a_1\vec{r}_1 + a_2\vec{r}_2 +\ldots+ a_m\vec{r}_m + \\ &+ c\lambda_{11}(p^k,0,\ldots,0) + p^kc(0,\lambda_{12},\ldots,\lambda_{1n}) \\ &= (a_1+c)\vec{r}_1 + a_2\vec{r}_2 +\ldots+ a_m\vec{r}_m.\end{aligned}$$

Portanto $(\mu_1,\mu_2,\ldots,\mu_n)$ é uma combinação linear das linhas da matriz de relações F. Isto implica em $m = \mu_1u_1+\ldots+\mu_nu_n = 0$ em M. Logo θ é injetora e $\ker\theta = (0)$.

Mostremos que coker θ é finito. Ora $\theta(M) = [v_1,v_2,\ldots,v_n] \subseteq M'$. Logo $\frac{M'}{\theta(M)}$ é gerado por $\bar{v}$. Repare que $(p^kv) = (p^kv_1) \subseteq \theta(M)$ e $(p^kv_i) \subseteq \theta(M)$. Logo $p^kM' \subseteq \theta(M)$. Da mesma maneira $\lambda_{11}M' \subseteq \theta(M)$. Portanto $\frac{M'}{\theta(M)}$ é anulado por (p^k,λ_{11}) donde ele é um $\frac{\Lambda}{(p^k,\lambda_{11})}$-módulo gerado por $\bar{v}$. Ora, pelo Lema 1, $\frac{\Lambda}{(p^k,\lambda_{11})}$ é finito e portanto $\frac{M'}{\theta(M)} = \frac{\Lambda}{(p^k,\lambda_{11})}\bar{v}$ também é finito. Logo, coker θ é finito e θ é um pseudo-isomorfismo.

Para conseguir a matriz F' como relações, consideramos M"

o submódulo de M' gerado por $v, v_2, \ldots, v_n$ e M''' o submódulo de M' gerado por $v_1 - v$. Evidentemente $M' = M'' + M'''$.

Afirmamos que $M'' \cap M''' = (0)$. De fato, se $av + a_2v_2 + \ldots + a_nv_n = b(v_1 - v)$ com $a, b, a_i \in \Lambda$, então $(a+b)v - bv_1 + a_2v_2 + \ldots + a_nv_n = 0$ em M'. Daí $\beta = (-b, a_2, \ldots, a_n, a+b)$ pertence ao módulo de relações de M'. Ora, a primeira coluna de F e de G' são divisíveis por p^k. Como pertence ao subespaço gerado pelas linhas de G', tem a sua primeira entrada divisível por p^k. Daí $p^k \mid (-b)$, digamos $-b = p^k c$. Então $b(v_1 - v) = -cp^k(v_1 - v) = 0$ em M'. Logo $av + a_2v_2 + \ldots + a_nv_n = b(v_1 - v) = 0$ e $M'' \cap M''' = (0)$. Portanto $M' = M'' \oplus M'''$.

Seja $M' \xrightarrow{\varphi} M''$ a projeção $\ker\varphi = M''' = \Lambda(v_1 - v)$. Como $p^k(v_1 - v) = 0$, M'' é anulado por p^k e logo M''' é um $\frac{\Lambda}{(p^k)}$-módulo. Mas o anulador de M''' é (p^k) pois se $f(v_1 - v) = 0$ então $(f, 0, \ldots, 0, -f)$ pertence ao módulo de relações K' de M' e daí a primeira entrada é divisível por p^k. Isto mostra que $M''' \simeq \frac{\Lambda}{(p^k)}$. A matriz de relações de M' pode ser obtida de matrizes de relações G'' e G''' de M'' e M''', respectivamente. G'' é obtida de relações de $v, v_2, v_3, \ldots, v_n$ e de G''' de relações de $v_1 - v$. Portanto

$$G'' = \begin{bmatrix} \lambda_{11} & \lambda_{12} \cdots \lambda_{1n} \\ p^k\lambda_{21} & \lambda_{22} \cdots \lambda_{2n} \\ \cdots\cdots\cdots\cdots\cdots \\ p^k\lambda_{m1} & \lambda_{m2} \cdots \lambda_{mn} \end{bmatrix}$$

tais que $\lambda_{11}v+\lambda_{12}v_2+\ldots+\lambda_{1n}v_n = 0$, $p^k\lambda_{21}v+\lambda_{22}v_2+\ldots+\lambda_{2n}v_n = 0$, etc. (repare que $p^k\lambda_{12}v_1 = p^k\lambda_{12}v$) e $G''' = [p^k]$, uma matriz 1 x 1. Portanto a matriz de relações de M' é

$$\begin{bmatrix} G'' & 0 \\ 0 & G''' \end{bmatrix} = \left[\begin{array}{ccc|c} \lambda_{11} & \lambda_{12} \cdots & \lambda_{1n} & \\ p^k\lambda_{21} & \lambda_{22} \cdots & \lambda_{2n} & \\ \cdots\cdots\cdots\cdots\cdots & & & 0 \\ p^k\lambda_{m1} & \lambda_{m2} \cdots & \lambda_{mn} & \\ \hline 0 & & & p^k \end{array}\right] = F'$$

como desejamos.

OPERAÇÃO III: *Se* F *contém a primeira linha* $(p^k\lambda_{11},\ldots,p^k\lambda_{1n})$ *e para algum* λ *com* $p\nmid\lambda$, $(\lambda\lambda_{11},\ldots,\lambda\lambda_{1n})$ *é uma relação (não necessariamente contida em* F *de maneira explícita), então podemos mudar de* F *para* F' *onde* F' *é obtida de* F *por substituição de* $(p^k\lambda_{11},\ldots,p^k\lambda_{1n})$ *por* $(\lambda_{11},\ldots,\lambda_{1n})$.

DEMONSTRAÇÃO da justificativa da Operação III: Seja M gerado por $u_1, u_2, \ldots, u_n$ e a matriz de relações

$$F = \begin{bmatrix} p^k\lambda_{11} & p^k\lambda_{12} & \cdots & p^k\lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \end{bmatrix}.$$

Seja M' um módulo gerado por $v_1, v_2, \ldots, v_n$ e seja G a matriz de relações de M' definida por

$$G = \begin{bmatrix} & F & \\ \lambda_{11} & \cdots & \lambda_{1n} \end{bmatrix}$$

uma matriz $(m+1) \times n$. Existe um homomorfismo $\theta : M \to M'$ definido por $\theta(u_i) = v_i$. θ é bem definido pois os v_i satisfazem as mesmas relações que os u_i. É evidente que θ é sobrejetor, logo coker $\theta = (0)$.

Afirmamos que coker θ é anulado pelo ideal (λ, p^k) de Λ. Com efeito, se $x = a_1u_1 + \ldots + a_nu_n$ está no ker θ então $a_1v_1 + \ldots + a_nv_n = 0$ e $(a_1, a_2, \ldots, a_n) \in K'$, o submódulo de relações gerado pelas linhas de G. Logo

$$(a_1,\ldots,a_n) = t_1\vec{r}_1+t_2\vec{r}_2+\ldots+t_n\vec{r}_n+t(\lambda_{11},\lambda_{12},\ldots,\lambda_{1n})$$

onde os r_i são as linhas de F. Portanto em M

$$x = a_1u_1+\ldots+a_nu_n = t(\lambda_{11}u_1+\lambda_{12}u_2+\ldots+\lambda_{1n}u_n) .$$

Daí $\lambda x = 0$, pois $(\lambda\lambda_{11},\lambda\lambda_{12},\ldots,\lambda\lambda_{1n})$ é também uma relação de M. Da mesma maneira $p^kx = 0$ pois $(p^k\lambda_{11},p^k\lambda_{12},\ldots,p^k\lambda_{1n})$ é uma relação de M. Daí (p^k,λ) anula ker θ e ker θ é um $\frac{\Lambda}{(p^k,\lambda)}$-módulo.

Ora, ker $\theta \subseteq M$ e M é finitamente gerado. Como Λ é noetheriano, ker θ é finitamente gerado, digamos por $y_1,y_2,\ldots,y_s$. Portanto ker θ é gerado por $y_1,\ldots,y_s$ como $\frac{\Lambda}{(p^k,\lambda)}$-módulo também. Então ker θ é uma imagem homomórfica como $\frac{\Lambda}{(p^k,\lambda)}$-módulo de $(\frac{\Lambda}{(p^k,\lambda)})^s$. Esse último módulo é finito pois $\frac{\Lambda}{(p^k,\lambda)}$ é finito pelo Lema 1. Portanto ker θ é finito, sendo uma imagem homomórfica de $(\frac{\Lambda}{(p^k,\lambda)})^s$. Isto mostra que φ é um pseudo-isomorfismo.

A matriz de relações de M' pode ser tomada como

$$\begin{bmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{m1} & \lambda_{m2} & \ldots & \lambda_{mn} \end{bmatrix}$$

substituindo-se a primeira linha de F pela última linha de G .

Dadas essas operações, a estrutura de um $\mathbb{Z}_p[[X]]$-módulo M finitamente gerado pode ser expressa da seguinte maneira:

TEOREMA 3: *Seja* M *um* Λ*-módulo finitamente gerado. Então existe um pseudo-isomorfismo* $\theta : M \to M'$ onde

$$M' = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \frac{\Lambda}{(p^{n_i})} \right) \oplus \left(\bigoplus_{j=1}^{t} \frac{\Lambda}{(f_j(X))^{m_j}} \right)$$

com $r \geq 0$, $s \geq 0$, $t \geq 0$, $n_i > 0$ *(se* $s > 0$*)* *e* $m_j > 0$ *(se* $t > 0$*)* *e os* $f_j(X)$ *são polinômios distinguidos e irredutíveis.*

DEMONSTRAÇÃO: Procedemos da mesma maneira que na demonstração do Teorema 2 do Capítulo V seguindo o espírito da prova do Teorema 1 daquele capítulo. O módulo M é dado por geradores $u_1, u_2, \ldots, u_n$ e uma matriz de relações F . Pode-se mudar de F para uma matriz F' usando um número finito de operações do tipo A, B, C, I, II e III. F' define um novo módulo M' tal que $M \sim M'$ (composição de dois pseudo isomorfismos é um pseudo-isomorfismo). A meta é efetuar as operações indicadas de tal maneira que a matriz F' tenha uma forma simples.

Dizemos que $F \sim F'$ se F' é obtida de F via um número finito de operações. Observe que se F é uma matriz m x n, então

$$F' = \begin{bmatrix} G & & & & \\ & p^{k_1} & & & \\ & & p^{k_r} & & \\ & & & \ddots & \\ & & & & p^{k_n} \end{bmatrix}$$

onde G é uma matriz $m \times n$ e $k_i \in \mathbf{Z}$. O tamanho de F' é maior somente quando entram um número de operações do tipo II; caso contrário, F' tem o mesmo tamanho de F.

Se $F = 0$ então M é livre, $M \sim \Delta^n$. Portanto, suponhamos $F \neq 0$. Consideramos as matrizes F' com $F \sim F'$ (F fixa definida por M). Afirmamos que p não divide as entradas de todas as matrizes F'. Caso contrário, existe $k \geq 1$ tal que p^k divide todas as entradas e p^{k+1} não divide todas elas. Via operações do tipo A, pode-se supor que $F \sim F'$ onde

$$F' = \begin{bmatrix} p^k\lambda_{11} & p^k\lambda_{12} & \cdots & p^k\lambda_{1n} \\ p^k\lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p^k\lambda_{m1} & \lambda_{m2} & & \lambda_{mn} \end{bmatrix}$$

com $p \nmid \lambda_{11}$. Ora, via Operação II

$$F' \sim G = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} & 0 \\ p^{k}\lambda_{21} & & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p^{k}\lambda_{m1} & & & & \\ 0 & & & & p^{k} \end{bmatrix}$$

e pelo suposto p divide todas as entradas de F' enquanto $p \nmid \lambda_{11}$ - uma contradição.

Assim existe uma matriz G tal que $F \sim G$ e p não divide todas as entradas de G e portanto podemos falar no grau de Weierstrass finito de entradas não nulas de G. Então pegamos uma matriz G tal que $F \sim G$ e G possui uma entrada não-nula cujo grau de Weierstrass é o menor possível entre os graus de Weierstrass de entradas não-nulas de matrizes F' com $F \sim F'$. Via operações do tipo A sobre G, podemos supor

$$F \sim \begin{bmatrix} \lambda_{11}=\lambda & \lambda_{12} & \cdots & \lambda_{1n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & & 0 & p^{k_1} \end{bmatrix}$$

onde a última linha e a última coluna podem deixar de existir. Elas so aparecem

se a Operação II tiver sido usada na transição de F para G. Ora, λ_{11} admite uma fatoração $\lambda_{11} = \varepsilon_{11}(X)\mu_{11}(X)$ onde $\varepsilon_{11}(X)$ é uma unidade de Λ e μ_{11} um polinômio distinguido. Via Operação C, multiplicando-se a primeira linha da última matriz por ε_{11}^{-1}, temos

$$F \sim \begin{bmatrix} \mu_{11} & \lambda_{12} & \cdots & \lambda_{1n} & 0 \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & \cdots & 0 & p^{k_1} \end{bmatrix} \quad *$$

onde μ_{11} é um polinômio distinguido. Aplicando-se o algoritmo da divisão de λ_{1j} por λ_{11}, temos $\lambda_{1j} = q_{1j}\lambda_{11} + r_{1j}$ onde $r_{1j} \in \mathbb{Z}_p[X]$ e $q_{1j} \in \Lambda$.

Via operações do tipo B (somando-se q_{1j} vezes a primeira coluna à j-ésima coluna da última matriz tem-se

---

(*) Indica que aquela linha e aquela coluna podem ou não aparecer.

$$F \sim \begin{bmatrix} \mu_{11} & r_{12} & r_{13} & \cdots & r_{1n} & 0 \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & \cdots & \lambda_{2n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda_{m1} & \lambda_{m2} & \lambda_{m3} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & 0 & \cdots & 0 & p^k \end{bmatrix}^{*}_{*}.$$

Afirmamos que os $r_{1j} = 0$. Primeiro observamos que $gr_w r_{1j} = \infty$, ou seja, p divide os coeficientes de r_{1j}, $\forall$ j. Isto vale pois caso contrário .

$$gr_w r_{1j} \leq gr\ r_{1j} < gr\ \mu_{11} = gr_w \lambda_{11} = gr_w \lambda \ ,$$

contrariando a escolha de λ . Portanto p divide os coeficientes de r_{1j}. Existe um inteiro $t \geq 1$ tal que p^t divide os r_{1j}, mas $p^{t+1} \nmid r_{1j}$ para todo j , digamos $p^{t+1} \nmid r_{1s}$, $2 \leq s \leq n$. Assim

$$F \sim \begin{bmatrix} \mu_{11} & p^t x_{12} & p^t x_{13} & \cdots & p^t x_{1s} & \cdots & p^t x_{1n} & 0 \\ & & & \cdots & & & & \\ \cdot & & & & & & & \end{bmatrix}$$

onde $p \nmid \mu_{11}$. Usando operações do tipo I sucessivamente, temos

$$F = \begin{bmatrix} \mu_{11} & x_{12} & \cdots & x_{1s} & \cdots & x_{1n} & 0 \\ p^t x_{21} & x_{22} & \cdots & x_{2s} & \cdots & x_{2n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p^t x_{m1} & x_{m2} & \cdots & x_{ms} & \cdots & x_{mn} & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 & p^{k_1} \end{bmatrix}^*$$

onde $p \nmid x_{1s}$. Ora $gr_w x_{1s} \leq gr\ r_{1s} < gr\ \mu_{11} = gr_w \lambda$, contrariando a escolha de λ. Portanto $r_{ij} = 0$, $\forall\ j = 2,\ldots,n$.

Assim

$$F \sim \begin{bmatrix} \mu_{11} & 0 & \cdots & 0 & 0 \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & \cdots & 0 & p^{k_1} \end{bmatrix}^* = \begin{bmatrix} \mu_{11} & 0 & \cdots & 0 & 0 \\ \lambda_{21} & & & & \vdots \\ \cdots & & B & & \\ \lambda_{m1} & & & & 0 \\ 0 & & & 0 & p^{k_1} \end{bmatrix}^*$$

onde B é uma matriz $(m-1) \times (n-1)$. Se $B = 0$, pelo algoritmo da divisão por μ_{11}, pode-se supor que λ_{i1} é um polinômio com $gr\ \lambda_{i1} < gr\ \lambda_{11}$. Pela escolha de λ_{11}, $gr_w \lambda_{i1} = \infty$, $\forall\ i = 2,3,\ldots,n$.

Afirmamos que $\lambda_{i1} = 0$, $\forall\ i = 2,3,\ldots,n$. Caso contrário,

existe $t \geq 1$ tal que $p^t | \lambda_{i1}$ e $p^{t+1} \nmid \lambda_{s1}$ digamos com $2 \leq s \leq n$. Se $\lambda_{s1} = p^t y_{s1}$ então $(p^t y_{s1}, 0, \ldots, 0)$ é uma relação e evidentemente $(\lambda_{11} y_{s1}, 0, \ldots, 0)$ é uma relação multiplicando-se a primeira linha por y_{s1}. Pelas Operações A e III e observando o fato de $p \nmid \lambda_{11}$ concluimos que $(y_{s1}, 0, \ldots, 0)$ é uma relação. Ora $p \nmid y_{s1}$ e $gr_w y_{s1} \leq gr\ y_{s1} = gr\ \lambda_{s1} < gr\ \lambda_{11} = gr_w\ \lambda_{11}$, contrariando a escolha de λ_{11}. Logo se $B = 0$ então $\lambda_{j1} = 0$, $\forall\ j = 2, \ldots, n$ e

$$F \sim \begin{matrix} \\ \\ \\ \\ * \end{matrix} \begin{matrix} \begin{bmatrix} \lambda_{11} & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & p^{k_1} \end{bmatrix} \\ \\ \\ \\ * \end{matrix}$$

donde $M \sim \Lambda^{n-1} \oplus \frac{\Lambda}{(\lambda_{11})} \oplus \frac{\Lambda}{(p^{k_1})}$.

O caso de $B \neq 0$ vai depender dos seguintes lemas:

LEMA 3: *Se*

$$F = \begin{bmatrix} \lambda_{11} & \lambda\lambda_{12} & & \lambda\lambda_{1n} \\ \ldots & \ldots & \ldots & \ldots \end{bmatrix}$$

e λ *e* λ_{11} *são primos entre si, então* $F \sim F'$ *onde*

$$F' = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda\lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \lambda\lambda_{m1} & \lambda_{m2} & \ldots & \lambda_{mn} \end{bmatrix} .$$

DEMONSTRAÇÃO: Seja M um Λ-módulo definido por F. Sejam $M = \Lambda u_1 + \ldots + \Lambda u_n$ e $M' = \Lambda v_1 + \ldots + \Lambda v_n + \Lambda v$ onde os v_i satisfazem as mesmas relações que os u_i (*) e

$$(***) \begin{cases} -v_1 + \lambda_u = 0 \\ \lambda_{12} v_2 + \ldots + \lambda_{1n} v_n + \lambda_{11} v = 0 . \end{cases}$$

A matriz de M' pode ser

$$G = \begin{bmatrix} F & & \cdots & & 0 \\ -1 & 0 & \ldots & 0 & \lambda \\ 0 & \lambda_{12} & \cdots & \lambda_{1n} & \lambda_{11} \end{bmatrix} .$$

Definimos $\theta : M \to M'$ com $\theta(u_i) = v_i$. θ é bem definida pois F faz parte de G. Afirmo que θ é injeção. De fato, indiquemos as linhas de F por $\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_m$. Seja $m = \mu_1 u_1 + \ldots + \mu_n u_n \in M$ com $\theta(m) = \mu_1 v_1 + \ldots + \mu_n v_n = 0 \in M'$. Logo $(\mu_1, \mu_2, \ldots, \mu_n, 0) \in K'$, o módulo de relações de M'. Logo existem escalares $a_1, a_2, \ldots, a_n$, $a, b \in \Lambda$ tais que

$$(E)\quad (\mu_1,\mu_2,\ldots,\mu_n,0) = a_1(\vec{r}_1,0)+\ldots+a_n(\vec{r}_n,0) + a(-1,0,\ldots,0,\lambda) + b(0,\lambda_{12},\ldots,\lambda_{1n},\lambda_{11}).$$

Comparando-se a última entrada, $0 = a\lambda+b\lambda_{11}$

$$0 = a\lambda + b\lambda_{11}$$

donde $a\lambda = -b\lambda_{11}$. Como $(\lambda,\lambda_{11}) = 1$, $\lambda \mid b$ e $\lambda_{11} \mid a$ ou seja $-\frac{a}{\lambda_{11}} = \frac{b}{\lambda} = c \in \Lambda$. Substituindo em (E) para a e b, temos

$$\begin{aligned}(\mu_1,\mu_2,\ldots,\mu_n) &= a_1\vec{r}_1 +\ldots+ a_n\vec{r}_n + c(\lambda_{11},0,\ldots,0) + \\ &+ c(0,\lambda\lambda_{12},\ldots,\lambda\lambda_{1n}) \\ &= (a_1+c)\vec{r}_1 + a_2\vec{r}_2 +\ldots+ a_n\vec{r}_n .\end{aligned}$$

Logo $(\mu_1,\ldots,\mu_n) \in K$, o módulo de relações de F, portanto $m = \mu_1u_1+\ldots+\mu_nu_n = 0$. Assim $\ker\theta = (0)$.

Mostremos que coker θ é finito. Ora, $\theta(M) = [v_1,\ldots,v_n]$. Logo $\frac{M'}{\theta(M)} = [\bar{v}]$. De (***) $\lambda M' \subseteq \theta(M)$ e $\lambda_{11}M' \subseteq \theta(M)$. Logo $\frac{M'}{\theta(M)}$ é anulado pelo ideal (λ,λ_{11}) de Λ. Assim $\frac{M'}{\theta(M)}$ é um $\frac{\Lambda}{(\lambda,\lambda_{11})}$-módulo. Como $\frac{\Lambda}{(\lambda,\lambda_{11})}$ é finito pelo Lema 1, pois λ e λ_{11} são primos entre si, decorre que $\frac{M'}{\theta(M)}$ que é gerado sobre $\frac{\Lambda}{(\lambda,\lambda_{11})}$ por $\bar{v}$ é finito. Assim coker θ é finito. Olhamos agora para a matriz de relações de M'. Ora $M' = [v_1,\ldots,v_n,v] = [v_2,\ldots,v_n,v] = [v,v_2,\ldots,v_n]$, pois $\lambda v = v_1$. Se usamos

$v_1 = \lambda v$, a primeira linha de G passa para

$$\lambda\lambda_{11}v + \lambda\lambda_{12}v_2 + \ldots + \lambda\lambda_{1n}v_n = 0$$

o que decorre da 2ª relação de (***),

$$\lambda_{11}v + \lambda_{12}v_2 + \ldots + \lambda_{1n}v_n = 0 .$$

Portanto M' é dado por

$$\begin{bmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda\lambda_{21} & \lambda_{22} & & \lambda_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda\lambda_{m1} & \lambda_{m2} & & \lambda_{mn} \end{bmatrix} .$$

LEMA 4: *Se*

$$F = \begin{bmatrix} \lambda_{11} & 0 & \ldots & 0 & 0 \\ \lambda_{21} & & & & \\ \vdots & & B & & \vdots \\ \lambda_{m1} & & & & 0 \\ 0 & & & 0 & p^{k_1} \end{bmatrix} \begin{matrix} \\ \\ \\ \\ * \end{matrix}$$

Se $B \neq 0$ *e* $B \sim B'$ *então*

$$F \sim \begin{bmatrix} \lambda_{11} & 0 & \cdots & 0 & \overset{*}{0} \\ \lambda'_{21} & & & & \\ \vdots & & B' & & \\ \lambda'_{m1} & & & & \\ \overset{*}{0} & & \cdots & 0 & p^{k_1} \end{bmatrix}$$

desde que não se use operação do tipo III.

DEMONSTRAÇÃO: É suficiente considerar o caso onde B' é obtida de B via uma operação do tipo A, B, C ou I ou II, pois no caso geral o argumento se repete. Se B' é obtido de B via uma operação A ela não envolve a primeira linha e a primeira coluna de F e portanto F ~ F' via mesmo tipo de operação efetuada sobre F e a primeira linha de F' permanece igual à de F. Se R' usa uma operação do tipo B, então a mesma operação efetuada sobre F leva a F', sem afetar a primeira linha (os elementos nulos da primeira linha ajudam esta permanência). A mesma observação vale no caso do tipo C. Se B' usa uma operação do tipo I, digamos

$$B = \begin{bmatrix} \lambda_{22} & p\lambda_{23} & p\lambda_{24} & \cdots & p\lambda_{2n} & 0 \\ \lambda_{32} & \lambda_{33} & \lambda_{34} & \cdots & \lambda_{3n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda_{m2} & \lambda_{m3} & \lambda_{m4} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & 0 & \cdots & 0 & p^{k_1} \end{bmatrix}$$

onde $p \nmid \lambda_{22}$.

Se $B \sim B'$ onde

$$B' = \begin{bmatrix} \lambda_{22} & \lambda_{23} & \lambda_{24} & \cdots & \lambda_{2n} & 0 \\ \lambda p_{32} & \lambda_{33} & \lambda_{34} & & \lambda_{3n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p\lambda_{m2} & \lambda_{m3} & \lambda_{m4} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & 0 & \cdots & 0 & p^{k_1} \end{bmatrix}.$$

Então $F \sim F'$ via a seguinte sequência de operações:

$$F = \begin{bmatrix} \lambda_{11} & 0 & 0 & \dots & 0 \\ \lambda_{21} & & & & \\ \vdots & & B & & \\ \lambda_{m1} & \dots & & & \\ 0 & & & & p^{k_1} \end{bmatrix}$$

$\sim$ via caso particular da Operação I, pois a primeira linha tem um único elemento não-nulo com $p \nmid \lambda_{11}$.

$$\sim \begin{bmatrix} \lambda_{11} & 0 & 0 & \dots & 0 \\ p\lambda'_{21} & & & & \\ \vdots & & B & & \\ p\lambda'_{m1} & & & & \\ 0 & 0 & 0 & \dots & p^{k_1} \end{bmatrix}$$

$\sim$ (via duas operações do tipo A troca 2a. e 1a. linhas e depois 2a. e 1a. colunas).

$$\sim \begin{bmatrix} \lambda_{22} & p\lambda'_{21} & p\lambda_{23} & p\lambda_{24} & \dots & p\lambda_{2n} & 0 \\ 0 & \lambda_{11} & 0 & 0 & \dots & 0 & 0 \\ \lambda_{32} & p\lambda'_{31} & \lambda_{33} & \lambda_{34} & \dots & \lambda_{3n} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \lambda_{m2} & \lambda_{m1} & \lambda_{m3} & \lambda_{m4} & \dots & \lambda_{mn} & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & p^{k_1} \end{bmatrix}$$

$\sim$ via operação do tipo I.

$$\sim \begin{bmatrix} \lambda_{22} & \lambda'_{21} & \lambda_{23} & \cdots & \lambda_{2n} & 0 \\ p.0 & \lambda_{11} & 0 & \cdots & 0 & 0 \\ p\lambda_{32} & p\lambda'_{31} & \lambda_{33} & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p\lambda_{m2} & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & p^{k_1} \end{bmatrix}$$

$\sim$ via duas operações do tipo A: troque as primeiras duas linhas e depois as primeiras colunas.

$$\sim \begin{bmatrix} \lambda_{11} & 0 & 0 & \cdots & 0 & 0 \\ \lambda'_{21} & \lambda_{22} & \lambda_{23} & \cdots & \lambda_{2n} & 0 \\ p\lambda'_{31} & p\lambda_{32} & \lambda_{33} & \cdots & \lambda_{3n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p\lambda'_{m1} & p\lambda_{m2} & \lambda_{m3} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & 0 & \cdots & 0 & p^{k_1} \end{bmatrix} = F' .$$

Se B' é obtida de B via uma operação do tipo II, digamos

$$B = \begin{bmatrix} p^{k_{\lambda_{22}}} & p^{k_{\lambda_{23}}} & \cdots & p^{k_{\lambda_{2n}}} & 0 \\ p^{k_{\lambda_{32}}} & & & & \\ \vdots & & \cdots & & \\ p^{k_{\lambda_{m2}}} & & & & \\ 0 & & & & p^{k_1} \end{bmatrix} \sim$$

com $p \nmid \lambda_{22}$.

$$B' = \begin{bmatrix} \lambda_{22} & \lambda_{23} & \cdots & \lambda_{2n} & 0 \\ p^{k_{\lambda_{32}}} & \lambda_{33} & \cdots & \lambda_{3n} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p^{k_{\lambda_{m2}}} & \lambda_{m3} & \cdots & \lambda_{mn} & 0 \\ 0 & 0 & \cdots & 0 & p^{k_1} \end{bmatrix}$$

então $F \sim F'$ via a seguinte sequência de transições.

$$F = \begin{bmatrix} \lambda_{11} & 0 & \cdots & 0 \\ \lambda_{21} & & & \\ \vdots & & B & \\ \lambda_{m1} & & & \\ 0 & & & p^{k_1} \end{bmatrix} \sim$$

via caso especial da Operação I

$$\sim \begin{bmatrix} \lambda_{11} & 0 & \cdots & 0 \\ p^{k}\lambda'_{21} & & & \\ \vdots & & B & \\ p^{k}\lambda'_{m1} & & & \\ 0 & & & p^{k_1} \end{bmatrix} \sim$$

via troca das duas las. linhas depois troca das duas las. colunas e depois Operação II

$$\sim \begin{bmatrix} \lambda_{22} & \lambda'_{21} & \lambda_{23} & \cdots & \lambda_{2n} & 0 \\ 0 & \lambda_{11} & 0 & \cdots & 0 & 0 \\ p^{k}\lambda_{32} & p^{k}\lambda'_{31} & \text{parte de B} & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p^{k}\lambda_{m2} & p^{k}\lambda'_{m1} & & & & \vdots \\ 0 & & & & & p^{k_1} \end{bmatrix} \sim$$

via troca de linhas e colunas

$$\sim \begin{bmatrix} \lambda_{11} & 0 & 0 & \cdots & 0 & 0 \\ \lambda'_{21} & \lambda_{22} & \lambda_{23} & \cdots & \lambda_{2n} & 0 \\ p^k\lambda'_{31} & p^k\lambda_{32} & \lambda_{33} & \cdots & \lambda_{3n} & 0 \\ \vdots & \vdots & \text{parte de B} & & & \vdots \\ p^k\lambda'_{m1} & p^k\lambda_{m2} & & & & \\ 0 & 0 & & \cdots & & p^{k_1} \end{bmatrix} = F' .$$

O Lema 4 é rotineiro e deixou de tratar de operações do tipo III. O seguinte lema toma conta disto e é original e a chave de nossa simplificação da prova do Teorema 3 de Iwasava.

LEMA 5: *Seja*

$$F = \begin{bmatrix} \lambda_{11} & 0 & \cdots & 0 \\ \lambda_{21} & & & \\ \vdots & & B & \\ \lambda_{m1} & & & \end{bmatrix}$$

onde λ_{11} *é distinguido e seja* $B \sim B'$ *via uma operação do tipo* III. *Então*

$$F \sim \begin{bmatrix} \lambda_{11} & 0 & \cdots & 0 \\ \lambda'_{21} & & & \\ \vdots & & B' & \\ \lambda'_{m1} & & & \end{bmatrix}, \quad \lambda'_{i1} \in \Lambda .$$

DEMONSTRAÇÃO: Sem perda de generalidade pode-se supor que

$$B = \begin{bmatrix} p^k\lambda_{22} & p^k\lambda_{23} & \cdots & p^k\lambda_{2n} \\ \lambda_{32} & \lambda_{33} & \cdots & \lambda_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{m2} & \lambda_{m3} & \cdots & \lambda_{mn} \end{bmatrix}$$

onde existe λ tal que $p \nmid \lambda$ e $(\lambda\lambda_{22}, \lambda\lambda_{23}, \ldots, \lambda\lambda_{2n})$ e também uma relação oriunda de B e que

$$B' = \begin{bmatrix} \lambda_{22} & \lambda_{23} & \cdots & \lambda_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{m2} & \lambda_{m3} & \cdots & \lambda_{mn} \end{bmatrix}$$

uma vez que a transição de B para B' é via uma operação do tipo III. Ainda com o emprego do caso especial da Operação I, pode-

se supor que p^k divide λ_{i1} para $i = 2,3,\ldots,m$. Assim $\lambda_{21} = p^k\lambda'_{21}$.

Seja M um módulo tendo F como matriz de relações - digamos, $M = Au_1+\ldots+Au_n$. Seja $M' = \frac{M}{Au_1}$, então $M' = A\bar{u}_2+\ldots+A\bar{u}_n$ e B é a matriz de relações de M'. Seja $x = \lambda'_{21}u_1+\lambda_{22}u_2+\ldots+\lambda_{2n}u_n \in M$. Então $p^k\bar{x} = \bar{0}$ e $\lambda\bar{x} = \bar{0}$ em M'. Se θ é o homomorfismo canônico: $\theta : M \to M'$, então $\theta(\lambda x) = 0$. Daí $\lambda x \in \ker\theta = Au_1$. Ora $\lambda_{11}u_1 = 0$ em M implica $\lambda\lambda_{11}x \in A\lambda_{11}u_1 = (0)$. Portanto $(\lambda\lambda_{11}\lambda'_{21}, \lambda\lambda_{11}\lambda_{22}, \ldots, \lambda\lambda_{11}\lambda_{2n})$ é uma relação definida por F. Como $p \nmid \lambda\lambda_{11}$ e como a segunda linha de F é $(p^k\lambda'_{21}, p^k\lambda_{22}, \ldots, p^k\lambda_{2n})$, pode-se aplicar a Operação III a F para concluir $F \sim F'$.

Dado o Lema 5, podemos terminar a prova do Teorema 3 por um eficiente emprego de indução.

DEMONSTRAÇÃO DO TEOREMA 3 (Prosseguindo): Pode-se supor que

$$F = \begin{bmatrix} \lambda_{11} & 0 & \ldots & 0 \\ \lambda_{21} & & & \\ \vdots & & & \\ \lambda_{m1} & & & B \end{bmatrix}$$

é de tamanho $m \times n$ onde λ_{11} é distinguido e satisfaz a escolha já indicada. Note que se $F \sim F'$ o tamanho de F' não muda efe-

tivamente, pois

$$F' = \begin{bmatrix} \text{matriz } m \times n & & 0 \\ & \ddots & \\ 0 & & T \end{bmatrix}$$

onde T é uma matriz da forma

$$\begin{bmatrix} p^{k_1} & & & 0 \\ & p^{k_2} & & \\ & & \ddots & \\ 0 & & & p^{k_t} \end{bmatrix}$$

que surge com o emprego de operações do tipo II. Como T já está na forma diagonal desejada, trabalhamos somente com a matriz m x n que faz parte de F'. Empregamos indução sobre m. Se m=1 não há nada a fazer.

Consideramos a afirmativa: G de tamanho m x n é $\sim$ a G' com

$$G' = \begin{bmatrix} \mu_{11} & & & & & & \\ & \mu_{22} & & & & & \\ & & \ddots & & & & \\ & & & \mu_{rr} & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

onde os μ_{ii} ,são polinômios distinguidos e admitimos como hipótese de indução que esta afirmativa vale para matrizes $(m-1) \times n'$. Então B é uma matriz $(m-1)(n-1)$ e $B \sim B'$, onde B' tem a forma diagonal desejada. Aplicando Lema 4 e Lema 5 um número finito de vezes, concluímos que

$$F \sim \begin{bmatrix} \lambda_{11} & 0 & & & 0 \\ \lambda'_{21} & \lambda_{22} & & & \\ \lambda'_{31} & & \ddots & & \\ & & & \lambda_{rr} & \\ \vdots & 0 & & & 0 \\ & & & & \ddots \\ \lambda'_{m1} & & & & 0 \end{bmatrix}$$

Falta-nos apenas encher a primeira coluna com elementos nulos para λ'_{i1}, $i = 2,3,\ldots,m$. Ora, pode-se aplicar o algoritmo da divisão por λ_{11} a λ'_{i1}, $i = 2,3,\ldots,m$ e, via operações do tipo B, pode-se ainda supor que λ'_{i1} são polinômios de grau menor que o de λ_{11}. Aplicação da Operação I garante ainda que $p|\lambda'_{i1}$, $i = 2,3,\ldots,n$.

Afirmamos que $\lambda'_{i1} = 0$, $\forall\ i = 2,3,\ldots,r$. Caso contrário, digamos $\lambda'_{j1} \neq 0$, $2 \leq j \leq r$, existe ℓ tal que $p^{\ell}|\lambda'_{j1}$ e $p^{\ell+1}\nmid\lambda'_{j1}$. Ora $p\nmid\lambda_{jj}$ e p^{ℓ} divide $\lambda'_{ji} = 0$, $\forall\ i \neq 1$ e j. Assim, via operações dos tipos I e A aplicados ℓ vezes, concluímos que

$$F \sim F' = \begin{bmatrix} \lambda_{11} & \cdots \\ \vdots & \\ \mu_{j1} & \\ \vdots & \end{bmatrix}$$

donde $p^{\ell}\mu_{j1} = \lambda'_{j1}$ e $p\nmid\mu_{j1}$. Ora

$$gr_w\mu_{j1} \leq gr\ \mu_{j1} = gr\lambda'_{j1} < gr\ \lambda_{11},$$

contrariando a escolha de λ_{11}. Logo $\lambda'_{i1} = 0$ $\forall\ i = 2,3,\ldots,r$. Assim

$$F \sim H = \begin{bmatrix} \lambda_{11} & & & & 0 \\ 0 & \lambda_{22} & & & \\ \vdots & & \ddots & & \\ 0 & & & \lambda_{rr} & \\ \lambda'_{r+1,1} & & & 0 & \\ \vdots & & 0 & & \ddots \\ \lambda'_{m,1} & & & & 0 \end{bmatrix} .$$

Se $\lambda'_{i1} = 0$ para todo $i = r+1,\ldots,m$ então acabamos. Caso contrário, seja $j = r+1$ e $\lambda'_{j1} \neq 0$. Escreva $\lambda'_{j1} = p^t\mu_{j1}$, $t \geq 1$. Então a j-ésima linha de F é $(p^t\mu_{j1}, p^t.0, p^t0, \ldots, p^t0)$. Também $(\lambda_{11}\mu_{j1}, \lambda_{11}0, \ldots, \lambda_{11}0)$ é uma relação definida por H, pois $\lambda_{11}\mu_{j1}u_1 = \mu_{j1}\lambda_{11}u_1 = 0$ pela primeira linha (F define $M = \Lambda u_1 + \ldots + \Lambda u_n$). Ora $p \nmid \lambda_{11}$ e Operação III permite que

$$F \sim \begin{bmatrix} \lambda_{11} & & 0 & & 0 \\ & \ddots & & & \\ 0 & & \lambda_{rr} & & \\ 0 & & 0 & & \\ \lambda'_{r+2,1} & & & \ddots & \\ \vdots & & 0 & & \\ \lambda'_{m,1} & & & & 0 \end{bmatrix} .$$

Aplicando este último processo no máximo m-r vezes, conclui mos que

$$F \sim \begin{bmatrix} \lambda_{11} & & & & & & 0 \\ & \lambda_{22} & & & & & \\ & & \ddots & & & & \\ & & & \lambda_{rr} & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{bmatrix}$$

Acrescentamos agora a F' a matriz T acima mencionada. Assim

$$F \sim \begin{bmatrix} \lambda_{11} & & & & & & \\ & \lambda_{22} & & & & & \\ & & \ddots & & & & \\ & & & \lambda_{rr} & & & \\ & & & & p^{k_1} & & \\ & & & & & \ddots & \\ & & & & & & 0 \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

Agora, considerando a decomposição de cada λ_{ii} em fatores irredutíveis e usando Lema 2 concluimos a demonstração do Teorema 3.

BIBLIOGRAFIA

[1] ABHYANKAR, S.S.: *Local Analytic Geometry*. Academic Press, New York, 1964.

[2] ARTIN, E.: *Algebraic Numbers and Algebraic Functions*. Gordon and Breach, 1967.

[3] COHEN, I.: *On the Structure and Ideal Theory of Complete Local Rings*. Trans. Amer. Math. Soc., 1946.

[4] ENDLER, O.: *Valuation Theory*. Springer-Varlag, Berlin, 1972.

[5] LANG, S.: *Algebra*. Addison-Wesley Publishing Co., Massachusetts, 1965.

[6] LANG, S.: *Ciclotomic Fields*. Springer-Verlag, New York, 1978.

[7] McCARTHY, P.J.: *Algebraic Extensions of Fields*. Blaisdell Publishing Co., Waltham, 1966.

[8] MAL'CEV: *Foundations of Linear Algebra*. W.H. Freeman. San Francisco, 1963.

[9] RIBENBOIM, P.: *L'Arithmétique des Corps*. Hermann, Paris, 1972.

[10] RIBES, L.: *Introduction to Profinite Groups and Galois Cohomology*. Queen's Papers in Pure and Applied Mathematics, nº 24. Queen's University Kingston.