Universidade Federal do Rio Grande do Sul
Instituto de Matemática
Programa de Pós-Graduação em Matemática

Ideais Primos em Skew Anéis de Polinômios

por

LUCIANE GOBBI

Porto Alegre, março de 2007

Dissertação submetida por Luciane Gobbi* como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Dr. Wagner de Oliveira Cortes

Banca Examinadora:
Dr. Miguel Angel Alberto Ferrero
Dr. Antônio Paques
Dr. Orlando Stanley Juriaans (USP)

Data de Defesa: 23 de março de 2007

*Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.

Juarez, Marinês,

Paulo, Viviane

e a meu noivo e eterno amigo, Bruno.

Agradecimentos

Primeiramente, agradeço a Deus pela oportunidade de estar realizando este sonho.

Agradeço ao professor Wagner pela orientação e paciência fundamentais para tornar este presente trabalho possível.

Meus agradecimentos aos amigos Lucinéia, Daiane, Cleber, Cícero, Flavinha, Edite, Jairo, Rosane, Rosane (secretária) e todos os demais colegas e professores da pós-graduação pelo companheirismo dedicado.

Agradeço aos professores Dotto, Helena e Marília, da graduação, pelo apoio e auxílio prestados.

Em especial, quero agradecer a Tânia pela sua amizade incondicional.

Aos meus pais, irmãos, Michele, Fernando, tia Zélia e vovó Maria, muito obrigada pelo incentivo e apoio que me ajudaram a chegar até aqui. Agradeço também ao meu noivo, Bruno, pelas palavras de incentivo, carinho e paciência distribuídos ao longo de tantos anos. Sem vocês, minha caminhada teria sido muito mais difícil.

Resumo

Sejam R um anel, ρ um automorfismo e d uma derivação de R. Este trabalho tem por objetivo estudar os ideais primos em skew anel de Laurent $R < x; \rho >$, skew anel de polinômios do tipo automorfismo $R[x; \rho]$ e skew anel de polinômios do tipo derivação $R[x; d]$. Para os casos $R < x; \rho >$ e $R[x; d]$ obtemos uma descrição completa dos ideais primos R-disjuntos. Em $R[x; \rho]$ obtemos uma caracterização dos ideais R-disjuntos fortemente ρ-primos. Além disto, quando R é um anel primo, obtemos uma caracterização dos ideais primos R-disjuntos de $R[x; \rho]$.

Abstract

Let R be a ring, ρ an automorphism and d a derivation of R. The purpose of this dissertation is to study prime ideals in skew Laurent polynomial rings $R < x; \rho >$, skew polynomial ring of automorphism type $R[x; \rho]$ and skew polynomial ring of derivation type $R[x; d]$. We obtained a full description of R-disjoint prime ideals in $R < x; \rho >$ and $R[x; d]$. In the case of $R[x; \rho]$ we obtained a characterization of strongly ρ-prime R-disjoint ideals. Furthermore, when R is a prime ring, we obtain a characterization of the R-disjoint prime ideals of $R[x; \rho]$.

Sumário

Introdução

Neste trabalho, o principal objetivo é o estudo de ideais primos em skew anel de polinômios sobre anéis não necessariamente comutativos. As principais referências são os trabalhos [3] e [8], cuja motivação dos autores foi a extensão dos resultados de M. Ferrero em [5].

Para realizarem estes estudos os autores estenderam o conceito de ideais fechados definidos em [5] para skew anel de polinômios.

A maioria das demonstrações aqui apresentadas segue a argumentação dada em [3] e [8], com algumas exceções relativas principalmente aos resultados do capítulo 1 que segue [12].

No capítulo 1, colocamos os pré-requisitos necessários ao desenvolvimento do texto. Ali aparecem as definições dos objetos abordados nos capítulos seguintes, bem como o estudo do centro do skew anel de polinômios.

No capítulo 2, estudamos ideais primos em skew anel de Laurent e skew anel de polinômios de tipo automorfismo. Na primeira seção deste capítulo, o principal resultado é o Teorema 2.1.18, onde estudamos condições necessárias e suficientes para que um ideal R-disjunto de $R < x; \rho >$ seja primo, com ρ automorfismo de R e R anel ρ-primo. Como principal conseqüência deste teorema temos o Corolário 2.1.20 onde caracterizamos os ideais primos R-disjuntos através de extensão e contração de ideais primos R-disjuntos de $R < x; \rho >$, de ideais primos $Q_\rho(R)$-disjuntos de $Q_\rho(R) < x; \rho >$ e do conjunto dos ideais maximais de Z, onde $Q_\rho(R)$ é o anel de

ρ-quocientes à esquerda de Martindale de R e Z é o centro de $Q_\rho(R) < x; \rho >$.

Na segunda seção, caracterizamos os ideais fortemente ρ-primos em skew anel de polinômios de tipo automorfismo. O principal resultado desta seção é o Corolário 2.2.11, onde estudamos condições necessárias e suficientes para que um ideal R-disjunto de $R[x; \rho]$ seja fortemente ρ-primo. Além disso, obtemos uma correspondência dos ideais primos R-disjuntos de $R < x; \rho >$ e dos ideais fortemente ρ-primos R-disjuntos de $R[x; \rho]$ que não contém x, onde R é um anel fortemente ρ-primo. Na terceira seção, quando R é um anel primo, obtemos como conseqüência a descrição dos ideais primos R-disjuntos do skew anel de polinômios do tipo automorfismo.

Finalmente no capítulo 3, estudamos os ideais primos em skew anel de polinômios de tipo derivação. Nele consideraremos R um anel d-primo, $C_d(R)$ o d-centróide estendido de R e $Q_d(R)$ o anel de d-quocientes à esquerda de Martindale de R, onde d é uma derivação de R. Então, no Teorema 3.1.7, obtemos uma condição necessária e suficiente para que um ideal R-disjunto de $R[x; d]$ seja primo e neste caso, é mostrado que todo ideal primo R-disjunto P de $R[x; d]$ é da forma $P = Q_d(R)[x; d]f_0 \cap R[x; d]$, onde f_0 é um polinômio irredutível de $Z = C_d(R)[z]$, o centro de $Q_d(R)[x; d]$. Como conseqüência do Teorema 3.1.7, obtemos uma correspondência via contração entre os ideais primos R-disjuntos de $R[x; d]$, os ideais primos $Q_d(R)$-disjuntos de $Q_d(R)[x; d]$ e os polinômios irredutíveis de $Z = C_d(R)[z]$. Além disto, no Corolário 3.1.16, estudamos uma caracterização intrínseca para que um ideal R-disjunto de $R[x; d]$ seja primo.

Capítulo 1

Pré-requisitos

Este capítulo contém alguns pré-requisitos necessários à compreensão do que segue.

1.1 Anéis de Quocientes de Martindale

Sejam R um anel qualquer e P um ideal de R. Dizemos que P é um ideal primo, se para quaisquer ideais A e B de R tais que $AB \subseteq P$ tem-se que $A \subseteq P$ ou $B \subseteq P$. Um anel R é dito primo se (0) é um ideal primo de R.

Seja R um anel primo não necessariamente com unidade. Se I é um ideal de R diremos que uma aplicação $f : I \to R$ é um R-homomorfismo à esquerda se f é aditiva e $f(ra) = rf(a)$, para todo $a \in I$ e $r \in R$. Analogamente, dizemos que f é um R-homomorfismo à direita se f é aditiva e $f(ar) = f(a)r$, para todo $a \in I$ e $r \in R$. Além disso, f é um homomorfismo de R-bimódulos se f é um R-homomorfismo à direita e à esquerda. No que segue, consideramos ideais não-nulos I de R e R-homomorfismos à esquerda $f : I \to R$. O conjunto dos ideais não-nulos de R será denotado por $\mathcal{I}$. Note que, se $I, J \in \mathcal{I}$, então $IJ \in \mathcal{I}$ e $I \cap J \in \mathcal{I}$.

Seja Ω o conjunto de todos os pares (I, f), onde $I \in \mathcal{I}$ e $f : I \to R$ é um homomorfismo de R-módulos à esquerda e consideremos $(I, f), (J, g) \in \Omega$. Dizemos que (I, f) é equivalente a (J, g) ($(I, f) \sim (J, g)$) se existir $H \in \mathcal{I}$ tal que $H \subseteq I \cap J$ e $f|_H = g|_H$. Podemos facilmente verificar que esta é uma relação de equivalência e que pode ser definida equivalentemente como segue: $(I, f) \sim (J, g)$ se, e somente se, $f|_{I\cap J} = g|_{I\cap J}$.

Denotamos por Q o conjunto quociente $\Omega/\sim$ e por $[I, f]$ a classe de equivalência de $(I, f) \in \Omega$. No que se segue, damos a Q uma estrutura de anel de modo a podermos considerar $R \subseteq Q$. Sejam $[I, f], [J, g] \in Q$. Definimos a adição e a multiplicação em Q por:

i) $[I, f] + [J, g] = [I \cap J, f + g]$, onde $f + g : I \cap J \to R$ é definido por $(f + g)(a) = f(a) + g(a)$, para todo $a \in I \cap J$.

ii) $[I, f].[J, g] = [IJ, f \circ g]$, onde $f \circ g : IJ \to R$ é definido por $(f \circ g)(a) = f(g(a))$, para todo $a \in IJ$.

É fácil verificar que estas operações estão bem definidas em Q e provar o seguinte teorema.

Teorema 1.1.1. $(Q, +, .)$ *é um anel com unidade.*

O anel Q do teorema acima é denominado o *anel de quocientes à esquerda de Martindale* de R.

Seja R um anel qualquer não necessariamente com unidade e ρ um automorfismo de R. Dizemos que um ideal I de R é um *ρ-ideal* (*ideal ρ-invariante*) se $\rho(I) \subseteq I$ ($\rho(I) = I$). Um elemento $a \in R$ é dito ρ-invariante se $\rho(a) = a$.

Um ideal ρ-invariante P de R é dito *ρ-primo* se para quaisquer ideais ρ-invariantes L e K de R tais que $LK \subseteq P$ implica $L \subseteq P$ ou $K \subseteq P$. Um anel R é dito *ρ-primo* se (0) é um ideal ρ-primo de R. Além disto, um ideal ρ-invariante P de R é dito *fortemente ρ-primo* se para quaisquer ρ-ideal J de R e um ideal K de R tais que $JK \subseteq P$ tem-se que $J \subseteq P$ ou $K \subseteq P$. Um anel R é dito *fortemente ρ-primo* se (0)

é um ideal fortemente ρ-primo de R. Se um ideal I de R é fortemente ρ-primo então I é um ideal ρ-primo. A recíproca não é verdadeira, ver ([2], Example 3.4).

Seja R um anel ρ-primo. Denotamos por $\mathcal{I}_\rho$ o conjunto dos ideais ρ-invariantes não-nulos de R. Note que se $I, J \in \mathcal{I}_\rho$, então $IJ \in \mathcal{I}_\rho$ e $I \cap J \in \mathcal{I}_\rho$. A construção do anel de ρ-quocientes à esquerda de Martindale $Q_\rho(R)$ de R segue análoga a construção do anel de quocientes à esquerda de Martindale de R.

Sejam $Z(Q_\rho(R))$ o centro de $Q_\rho(R)$ e

$$C_\rho(R) = \{c \in Z(Q_\rho(R)) : \rho(c) = c\}$$

o *ρ-centróide estendido* de R. O seguinte lema nos dá algumas propriedades importantes de $Q_\rho(R)$.

Lema 1.1.2. *Seja R um anel ρ-primo. As seguintes condições são válidas:*

i) $R \subset Q_\rho(R)$.

ii) Se I é um ideal ρ-invariante não-nulo de R e $f : I \to R$ é homomorfismo de R-módulos à esquerda, então existe $q \in Q_\rho(R)$ tal que $f(r) = rq$ para todo $r \in I$. Além disso, $q \in Z(Q_\rho(R))$ se, e somente se, f é um homomorfismo de R-bimódulos.

iii) Para todo $q_1, q_2, \cdots, q_n$ em $Q_\rho(R)$, existe um ideal ρ-invariante não-nulo I de R tal que $Iq_i \subseteq R$ para todo $i \in \{1, \cdots, n\}$.

iv) Se $Iq = 0$ para algum ideal ρ-invariante não-nulo I de R então $q = 0$.

v) $Q_\rho(R)$ é um anel ρ-primo.

Lema 1.1.3. *Seja R um anel ρ-primo e $Q_\rho(R)$ o anel de ρ-quocientes à esquerda de Martindale de R. Então ρ se estende unicamente a $Q_\rho(R)$.*

Demonstração. Seja $q \in Q_\rho(R)$. Pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo J de R tal que $qJ \subseteq R$. Definamos $f : J \to R$ por $f(x) = \rho(q\rho^{-1}(x))$ para todo $x \in J$. Claramente, f é um homomorfismo de R-módulos à direita e com isto, $[J, f] \in Q_\rho(R)$.

Sejam $q, t \in Q_\rho(R)$. Pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo K de R tal que $tqK \subseteq R$, $qK \subseteq R$ e $tK \subseteq R$. Logo, $(q+t)K \subseteq R$. Definimos $\rho' : Q_\rho(R) \to Q_\rho(R)$ por $\rho'(q) = \rho(q\rho^{-1}(x))$ para todo $x \in K$. Claramente, $\rho'(qx) = \rho'(q)\rho(x)$. Denotaremos ρ' por ρ e com isto, $\rho(qx) = \rho(q)\rho(x)$.

Por sua vez, para todo $x \in K$,

$$\rho(tq)\rho(x) = \rho((tq)x) = \rho(t)\rho(qx) = \rho(t)\rho(q)\rho(x)$$

e com isto, $[\rho(tq) - \rho(t)\rho(q)]K = 0$. Segue do Lema 1.1.2 que $\rho(tq) = \rho(t)\rho(q)$. Aplicando o mesmo raciocínio para ρ^{-1}, concluímos que ρ é inversível e assim, ρ é automorfismo de $Q_\rho(R)$. □

Lema 1.1.4. *Sejam R um anel ρ-primo e $q \in Q_\rho(R)$ tal que $qR = Rq$ e $q = \rho(q)$. Então q é inversível em $Q_\rho(R)$. Em particular, $C_\rho(R)$ é um corpo.*

Demonstração. Seja $I = Rq \cap R$ e observemos que I é um ideal não-nulo tal que $\rho(I) = I$. Iremos mostrar que, se $qr = 0$ para algum $r \in R$, então $r = 0$. De fato, $i \in I$ então, $i = qr'$ para algum $r' \in R$. Logo $ir = (qr')r \in Ir$. Como $qR = Rq$, existe $r'' \in R$ tal que $qr' = r''q$ e com isto,

$$(qr')r = (r''q)r = r''(qr) = 0.$$

Assim, $Ir = 0$ e, pelo Lema 1.1.2 (iv), temos que $r = 0$.

Pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo U de R tal que $Uq \subseteq R$. Note que Uq é um ideal de R. Definimos $f : Uq \to R$ por $f(uq) = u$, para todo $u \in U$. Não é difícil ver que f é um homomorfismo de R-módulos à esquerda bem definido. Mostraremos que $d = [Uq, f] \in Q_\rho(R)$ é o inverso de q. Com efeito, seja

$u \in U$. Então, $u = f(uq) = uqd$ e com isto, $u(1 - qd) = 0$. Pelo Lema 1.1.2, segue que $qd = 1$. Note que para cada $y \in l_{Q_\rho(R)}(q) = \{m \in Q_\rho(R) : mq = 0\}$, temos que $0 = (yq)d = y(qd) = y$.

Seja $x \in r_{Q_\rho(R)}(q)$. Pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo J de R tal que $Jx \subseteq R$. Então, $qjx = j'qx = 0$, para todo $j \in J$ e assim, $IJx = 0$.

Como $IJ \in \mathcal{I}_\rho$ então, segue do Lema 1.1.2 que $x = 0$. Logo q não é divisor de zero à esquerda e, pelo exercício 4 item (b) da página 24 de [9], q é inversível. $\square$

Seja d uma derivação de R, isto é, d é uma aplicação aditiva e $d(ab) = d(a)b + ad(b)$. Um ideal J de R é dito um *d-ideal* de R se $d(J) \subseteq J$ e um elemento $a \in R$ é dito *d-invariante* se $d(a) = 0$.

Seja P um ideal de R. Dizemos que P é um ideal *d-primo* se P é um d-ideal e se dados quaisquer d-ideais J, K de R tais que $JK \subseteq P$ implica $J \subseteq P$ ou $K \subseteq P$. Um anel R é dito *d-primo* se (0) é um ideal d-primo de R.

Suponhamos que R é um anel d-primo. A construção do anel de d-quocientes à esquerda de Martindale $Q_d(R)$ de R segue análoga a construção do anel de quocientes à esquerda de Martindale, onde neste caso, consideramos $\mathcal{I}_d$ o conjunto dos d-ideais não-nulos de R.

Lema 1.1.5. *Seja R um anel d-primo e $Q_d(R)$ o anel de d-quocientes à esquerda de Martindale de R. Então d se estende unicamente a $Q_d(R)$.*

Demonstração. Seja $q \in Q_d(R)$. Então, pelo Lema 1.1.6, existe um d-ideal não-nulo J de R tal que $Jq \subseteq R$. Definimos $f : J \to R$ por $f(x) = d(xq) - d(x)q$, para todo $x \in J$. Claramente, f é um homomorfismo de R-módulos à esquerda. Seja $d(q) = [J, f]$ e com isto, d é estendida unicamente a um elemento de $END_{\mathbb{Z}}(Q_d(R))$ tal que

$$ad(q) = f(a) = d(aq) - d(a)q.$$

Para cada $p, q \in Q_d(R)$, existe um d-ideal não-nulo I de R tal que $Ip \subseteq R, Iq \subseteq R$ e $Ipq \subseteq R$. Assim, para todo $x, y \in I \cap J$,

$$xyd(pq) = d(xypq) - d(xy)pq = xypd(q) + d(xyp)q - d(xy)pq =$$
$$xypd(q) + [d(xy)p + xyd(p)]q - d(xy)pq = xy[pd(q) + d(p)q].$$

Logo, $xy[d(pq) - d(p)q - pd(q)] = 0$ e com isto, $(I \cap J)^2[d(pq) - d(p)q - pd(q)] = 0$. Como $I \cap J \in \mathcal{I}_d$ então, pelo Lema 1.1.6, temos que $d(pq) = d(p)q + pd(q)$. $\square$

Sejam C o centro de $Q_d(R)$ e $C_d(R) = \{a \in C; d(a) = 0\}$ o d-centróide estendido de R. O seguinte lema nos dá algumas propriedades básicas de $Q_d(R)$.

Lema 1.1.6. *Seja R um anel d-primo. As seguintes condições são válidas:*

i) $R \subset Q_d(R)$.

ii) *Se I é um d-ideal não-nulo de R e $f : I \to R$ é homomorfismo de R-módulos à esquerda, então existe $q \in Q_d(R)$ tal que $f(r) = rq$ para todo $r \in I$. Além disso, $q \in C$ se, e somente se, f é um homomorfismo de R-bimódulos.*

iii) *Para todo $q_1, q_2, \cdots, q_n$ em $Q_d(R)$, existe um d-ideal não-nulo I de R tal que $Iq_i \subseteq R$ para todo $i \in \{1, \cdots, n\}$.*

iv) *Se $Iq = 0$ para algum d-ideal não-nulo I de R então $q = 0$.*

O próximo resultado nos dá uma propriedade de $C_d(R)$ e a prova é análoga a feita no Lema 1.1.4.

Lema 1.1.7. *Seja $q \in Q_d(R)$ tal que $qR = Rq$ e $d(q) = 0$. Então q é invertível em $Q_d(R)$ e em particular, $C_d(R)$ é um corpo.*

Os resultados apresentados nesta seção estão nos artigos [3], [5] e [8].

1.2 Determinação do centro de $Q_\rho(R)[x;\rho]$

Nesta seção, R é um anel com unidade e ρ é um automorfismo de R. Todos os resultados que serão aqui apresentados são do artigo [12].

O skew anel de Laurent $R < x;\rho >$ é definido como o conjunto de elementos da forma $\sum_{i=r}^{s} a_i x^i$ com $a_i \in R$, $r, s \in \mathbb{Z}$, onde a adição é a usual e a multiplicação é definida por $xa = \rho(a)x$ e $x^{-1}a = \rho^{-1}(a)x^{-1}$. O skew anel de polinômios do tipo automorfismo $R[x;\rho]$ é um subanel de $R < x;\rho >$ cujos elementos são polinômios da forma $\sum_{i=j}^{s} a_i x^i$, com $a_i \in R$ e $j, s \in \mathbb{N}$, onde a multiplicação e a adição são definidas como anteriormente.

O grau de um polinômio f de $R[x;\rho]$ se define como usualmente e se denotará por $\delta(f)$.

Seja σ um automorfismo de um anel com unidade S. Dizemos que σ é um automorfismo interno de S se existe $b \in S$ tal que $\sigma(s) = b^{-1}sb$ para todo $s \in S$. Denotaremos por σ_b o automorfismo interno de S determinado por b.

Para o que se segue, R é um anel ρ-primo com unidade e $Q_\rho(R)$ é o *anel de ρ-quocientes à esquerda de Martindale* de R.

Lema 1.2.1. *Seja $f = \sum_{i=0}^{n} a_i x^i \in Z(Q_\rho(R)[x;\rho])$. Então*

i) $\rho(a_i) = a_i$ para todo $i \in \{0, 1, \cdots, n\}$.

ii) Se $a_i \neq 0$ para algum $i \in \{0, 1, \cdots, n\}$, então a_i é invertível em $Q_\rho(R)$ e ρ^i é um automorfismo interno determinado pelo elemento invertível a_i.

iii) $a_i x^i \in Z(Q_\rho(R)[x;\rho])$, para todo $i \in \{0, 1, \cdots, n\}$.

Demonstração. (i) Como $f \in Z(Q_\rho(R)[x;\rho])$, então $fx = xf$ e com isto $\sum_{i=0}^{n} a_i x^{i+1} = \sum_{i=0}^{n} \rho(a_i) x^{i+1}$. Logo $a_i = \rho(a_i)$, para todo $i \in \{0, 1, \cdots, n\}$.

(ii) Por hipótese, para todo $q \in Q_\rho(R)$, temos que $qf = fq$. Então, $\sum_{i=0}^{n} q a_i x^i =$

$\sum_{i=0}^{n} a_i\rho^i(q)x^i$ e desta forma, $qa_i = a_i\rho^i(q)$. Assim, pelo Lema 1.1.4, se $a_i \neq 0$, então a_i é invertível em $Q_\rho(R)$. Logo, $a_i^{-1}qa_i = \rho^i(q)$, para todo $q \in Q_\rho(R)$ e $i \in \{0, 1, \cdots, n\}$.

(iii) Se $a_i = 0$ o resultado segue trivialmente. Suponhamos que $a_i \neq 0$. Para todo $q \in Q_\rho(R)$, temos que

$$(a_ix^i)q = a_i(\rho^i(q)x^i) = a_i(a_i^{-1}qa_i)x^i = q(a_ix^i).$$

Além disto,

$$x(a_ix^i) = \rho(a_i)x^{i+1} = a_ix^{i+1} = (a_ix^i)x.$$

Logo $a_ix^i \in Z(Q_\rho(R)[x;\rho])$. □

Teorema 1.2.2. *Seja* $C_\rho(R) = \{c \in Z(Q_\rho(R)); \rho(c) = c\}$.

i) Se ρ^k *não é um automorfismo interno de* $Q_\rho(R)$ *para todo* $k \geq 1$, *então* $Z(Q_\rho(R)[x;\rho]) = C_\rho(R)$.

ii) Se ρ^k *é um automorfismo interno de* $Q_\rho(R)$ *para algum* $k \geq 1$, *então*

$$Z(Q_\rho(R)[x;\rho]) = C_\rho(R)[bx^m],$$

onde m *é o menor número natural não-nulo tal que* ρ^m *é um automorfismo interno de* $Q_\rho(R)$ *determinado pelo elemento* ρ*-invariante* $b \in Q_\rho(R)$.

Demonstração. Suponhamos que ρ^k não seja um automorfismo interno de $Q_\rho(R)$ para todo $k \geq 1$. É fácil ver que $C_\rho(R) \subseteq Z(Q_\rho(R)[x;\rho])$. Por outro lado, consideremos $g \in Z(Q_\rho(R)[x;\rho])$ tal que $g = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, com $a_i \in Q_\rho(R)$ para todo $i \in \{0, 1, \cdots, n\}$.

Se $a_i \neq 0$ para algum $i \in \{1, 2, \cdots, n\}$ então, pelo Lema 1.2.1, ρ^i é um automorfismo interno de $Q_\rho(R)$ determinado por a_i, o que contradiz a hipótese. Assim, $a_i = 0$ para todo $i \in \{1, 2, \cdots, n\}$ e segue que, $g = a_0 \in C_\rho(R)$. Logo, $Z(Q_\rho(R)[x;\rho]) \subseteq C_\rho(R)$ e isto conclui a primeira parte da demonstração.

Suponhamos que ρ^k seja um automorfismo interno de $Q_\rho(R)$ determinado por um elemento $q \in Q_\rho(R)$, para algum $k \geq 1$. Note que, para $i \geq 0$

$$\rho^k(a) = \rho^i\rho^k\rho^{-i}(a) = \rho^i(\rho^k(\rho^{-i}(a))) = \rho^i(q^{-1}\rho^{-i}(a)q) = \rho^i(q^{-1})a\rho^i(q) = (\rho^i(q))^{-1}a\rho^i(q) = \rho_{\rho^i(q)}(a).$$

Assim, para $i \in \{0, 1, \cdots, k-1\}$,

$$\rho_{\rho^{k-1}(q)}\rho_{\rho^{k-2}(q)} \cdots \rho_{\rho(q)}\rho_q = \rho^k\rho^k \cdots \rho^k\rho^k = (\rho^k)^k = \rho^{k^2}.$$

Iremos mostrar que $\rho_{\rho^{k-1}(q)}\rho_{\rho^{k-2}(q)} \cdots \rho_{\rho(q)}\rho_q = \rho_{q\rho(q)\cdots\rho^{k-1}(q)}$. De fato, para $k = 2$, temos que,

$$\rho_{q\rho(q)}(a) = (q\rho(q))^{-1}aq\rho(q) = (\rho(q))^{-1}q^{-1}aq\rho(q) = (\rho(q))^{-1}\rho_q(a)\rho(q) = \rho_{\rho(q)}(\rho_q(a)).$$

Logo, $\rho_{q\rho(q)} = \rho_{\rho(q)}\rho_q$. Suponhamos que a igualdade seja verdadeira para $k-2$, isto é,

$$\rho_{\rho^{k-2}(q)}\rho_{\rho^{k-3}(q)} \cdots \rho_{\rho(q)}\rho_q = \rho_{q\rho(q)\cdots\rho^{k-2}(q)}.$$

Pela hipótese de indução,

$$\rho_{\rho^{k-1}(q)}\rho_{\rho^{k-2}(q)} \cdots \rho_{\rho(q)}\rho_q = \rho_{\rho^{k-1}(q)}(\rho_{q\rho(q)\cdots\rho^{k-2}(q)})$$

e, usando o caso $k = 2$, obtemos que

$$\rho_{\rho^{k-1}(q)}\rho_{\rho^{k-2}(q)} \cdots \rho_{\rho(q)}\rho_q = \rho_{q\rho(q)\cdots\rho^{k-2}(q)\rho^{k-1}(q)}.$$

Com isto,

$$\rho^{k^2} = \rho_{\rho^{k-1}(q)}\rho_{\rho^{k-2}(q)} \cdots \rho_{\rho(q)}\rho_q = \rho_{q\rho(q)\cdots\rho^{k-2}(q)\rho^{k-1}(q)}.$$

Seja $a = q\rho(q)\cdots\rho^{k-1}(q)$. Desde que $\rho^k(q) = q$, então

$$\rho^k(a) = \rho^k(q\rho(q)\cdots\rho^{k-1}(q)) = \rho^k(q)\rho^k(\rho(q))\cdots\rho^k(\rho^{k-1}(q)) = \rho^k(q)\rho(\rho^k(q))\cdots\rho^{k-1}(\rho^k(q)) = q\rho(q)\cdots\rho^{k-1}(q) = a$$

e segue que,

$$\rho(a) = \rho(q)\rho^2(q)\cdots\rho^{k-1}(q)\rho^k(q) = q^{-1}q\rho(q)\rho^2(q)\cdots\rho^{k-1}(q)q =$$
$$q^{-1}[q\rho(q)\rho^2(q)\cdots\rho^{k-1}(q)]q = q^{-1}aq = \rho_q(a) = \rho^k(a) = a.$$

Assim, $\rho^{k^2} = \rho_a$ é um automorfismo interno de $Q_\rho(R)$ determinado pelo elemento ρ-invariante $a \in Q_\rho(R)$.

Seja m o menor número natural tal que ρ^m é um automorfismo interno de $Q_\rho(R)$ determinado por um elemento ρ-invariante $b \in Q_\rho(R)$, isto é, $\rho^m(a) = b^{-1}ab$, para todo $a \in Q_\rho(R)$. Desta maneira, para qualquer $ax^k \in Q_\rho(R)[x;\rho]$,

$$(bx^m)(ax^k) = b(x^m a)x^k = b(\rho^m(a)x^m)x^k = bb^{-1}abx^m x^k = abx^k x^m = (ax^k)(bx^m)$$

e com isto, $bx^m \in Z(Q_\rho(R)[x;\rho])$ é um polinômio de grau mínimo em $Z(Q_\rho(R)[x;\rho])$.

Iremos mostrar que $Z(Q_\rho(R)[x;\rho]) = C_\rho(R)[bx^m]$. De fato, como $C_\rho(R) \subseteq Z(Q_\rho(R)[x;\rho])$ e $bx^m \in Z(Q_\rho(R)[x;\rho])$, segue que $C_\rho(R)[bx^m] \subseteq Z(Q_\rho(R)[x;\rho])$.

Por outro lado, seja $cx^k \in Z(Q_\rho(R)[x;\rho])$, para algum $c \in Q_\rho(R)$. Pelo Lema 1.2.1, $\rho(c) = c$ e com isto, $c \in C_\rho(R)$. Se $k < m$ então, pela minimalidade de m, $k = 0$ e temos que, $cx^k \in C_\rho(R)[bx^m]$.

Suponhamos que $k \geq m$ e que todo monômio com potência menor que k esteja em $C_\rho(R)[bx^m]$. Note que,

$$cb^{-1}x^{k-m}bx^m = cb^{-1}x^{k-m}x^m\rho^{-m}(b) = cb^{-1}x^k x^{-m}x^m\rho^{-m}(b) = cb^{-1}x^k\rho^{-m}(b) =$$
$$cx^k\rho^{-k}(b^{-1})\rho^{-m}(b) = cx^k.$$

Como, para todo $l \in Q_\rho(R)$,

$$cb^{-1}x^{k-m}l = cb^{-1}\rho^{k-m}(l)x^{k-m} = c\rho^k(l)b^{-1}x^{k-m} = l(cb^{-1}x^{k-m})$$

e

$$(cb^{-1}x^{k-m})x = cb^{-1}xx^{k-m} = cx\rho^{-1}(b^{-1})x^{k-m} = x\rho^{-1}(c)\rho^{-1}(b^{-1})x^{k-m} = x(cb^{-1}x^{k-m})$$

então, $cb^{-1}x^{k-m} \in Z(Q_\rho(R)[x;\rho])$. Assim, por hipótese de indução, $cb^{-1}x^{k-m} \in C_\rho(R)[bx^m]$. Logo, $cx^k = cb^{-1}x^{k-m}bx^m \in C_\rho(R)[bx^m]$ e, usando o Lema 1.2.1, temos que $Z(Q_\rho(R)[x;\rho]) \subseteq C_\rho(R)[bx^m]$. $\square$

As provas dos próximos resultados são similares as provas dos Lemas 1.2.1 e 1.2.2, respectivamente e por isso iremos omiti-las.

Lema 1.2.3. *Seja* $f = \sum_{i=-q}^{n} a_i x^i \in Z(Q_\rho(R) < x; \rho >)$. *Então*

i) $\rho(a_i) = a_i$ *para todo* $i \in \{-t, -t+1, \cdots, 0, 1, \cdots, n\}$.

ii) Se $a_i \neq 0$ *para algum* $i \in \{-t, -t+1, \cdots, 0, 1, \cdots, n\}$ *então* a_i *é invertível em* $Q_\rho(R)$ *e* ρ^i *é um automorfismo interno determinado pelo elemento invertível* a_i.

iii) $a_i x^i \in Z(Q_\rho(R) < x; \rho >)$, *para todo* $i \in \{-t, -t+1, \cdots, 0, 1, \cdots, n\}$.

Teorema 1.2.4. *Seja* $C_\rho(R) = \{c \in Z(Q_\rho(R)); \rho(c) = c\}$.

i) Se ρ^k *não é um automorfismo interno de* $Q_\rho(R)$ *para todo* $k \geq 1$ *então* $Z(Q_\rho(R) < x; \rho >) = C_\rho(R)$.

ii) Se ρ^k *é um automorfismo interno de* $Q_\rho(R)$ *para algum* $k \geq 1$ *então*

$$Z(Q_\rho(R) < x; \rho >) = C_\rho(R) < bx^m >,$$

onde m *é o menor número natural não-nulo tal que* ρ^m *é um automorfismo interno de* $Q_\rho(R)$ *determinado por um elemento* ρ*-invariante* $b \in Q_\rho(R)$.

1.3 Determinação do centro de $Q_d(R)[x; d]$

Nesta seção, R é um anel com unidade, d é uma derivação de R e todos os resultados apresentados são do artigo [12].

O skew anel de polinômios do tipo derivação $R[x; d]$ é definido como o conjunto de polinômios da forma $\sum_{i=j}^{n} a_i x^i$ com $a_i \in R$ e $j, n \in \mathbb{N}$, onde a adição é a usual e a multiplicação é definida por $xa = ax + d(a)$, $a \in R$.

Seja $f = \sum_{i=0}^{n} a_i x^i \in R[x; d]$. Assim,

$$d(f) = xf - fx = x(\sum_{i=0}^{n} a_i x^i) - (\sum_{i=0}^{n} a_i x^i)x = \sum_{i=0}^{n}(xa_i)x^i - \sum_{i=0}^{n} a_i x^{i+1} = \sum_{i=0}^{n}(a_i x + d(a_i))x^i - \sum_{i=0}^{n} a_i x^{i+1} = \sum_{i=0}^{n} d(a_i)x^i.$$

Desta forma, a derivação d pode ser estendida a uma derivação de $R[x; d]$. Denotaremos esta extensão por d novamente.

Seja f um polinômio em $R[x; d]$. Denotaremos por $\delta(f)$ e $lc(f)$ o grau e o coeficiente líder de f, respectivamente e denotaremos por Z o centro do anel $Q_d(R)[x; d]$.

Lema 1.3.1. *Seja R um anel d-primo. Então, $char(R) = 0$ ou $pR = 0$, para algum número primo $p \in \mathbb{Z}$.*

Demonstração. Suponhamos que $char(R) = n \neq 0$ e que n não é um número primo. Assim, $n = ab$, com $a, b \in \mathbb{N}$ primos e com isto, $(aR)(bR) = a(Rb)R = (ab)R = 0$.

Note que aR e bR são d-ideais de R e como R é um anel d-primo, então $aR = 0$ ou $bR = 0$, o que contradiz a escolha de n. Logo, n é primo. □

Lema 1.3.2. *Sejam R um anel d-primo, d uma derivação de R, $Q_d(R)$ o anel de d-quocientes à esquerda de Martindale de R e $C_d(R)$ o d-centróide estendido de R. Então $Z = C_d(R)$ ou $Z = C_d(R)[z]$, onde z tem uma das seguintes formas:*

i) $z = x - a$ *se* $char(R) = 0$ *e* $d(q) = aq - qa$, *para algum* $a \in Q_d(R)$.

ii) Existem $c_i \in C_d(R)$ *tais que* $z = x^{p^m} + \sum_{i=0}^{m-1} c_i x^{p^i} - a$, *se* $char(R) = p \neq 0$, *onde* $d(a) = 0$ *e* $(d^{p^m} + \sum_{i=0}^{m-1} c_i d^{p^i})(q) = aq - qa$.

Demonstração. Suponhamos que $C_d(R) \neq Z$ e seja $f = \sum_{i=j}^{l} a_i x^i \in Z$ um polinômio de grau minimal não-nulo. Para cada $j \in \{1, 2, \cdots, l\}$, consideremos $f_j = \sum_{i=j}^{l} \begin{pmatrix} i \\ j \end{pmatrix} a_i x^{i-j}$. Como $f \in Z$, então $xf = fx$ e com isto, $d(a_i) = 0$, para todo $i \in \{j, j+1, \cdots, l\}$. Deste modo,

$$f_jx = \sum_{i=j}^{l} \begin{pmatrix} i \\ j \end{pmatrix} a_i x^{i-j} x = \sum_{i=j}^{l} \begin{pmatrix} i \\ j \end{pmatrix} (a_i x) x^{i-j} = \sum_{i=j}^{l} \begin{pmatrix} i \\ j \end{pmatrix} (xa_i - d(a_i)) x^{i-j} =$$

$$\sum_{i=j}^{l} \begin{pmatrix} i \\ j \end{pmatrix} (xa_i) x^{i-j} = x \sum_{i=j}^{l} \begin{pmatrix} i \\ j \end{pmatrix} a_i x^{i-j} = xf_j$$

para todo $j \in \{1, 2, \cdots, l\}$.

Desde que $cf = fc$ para todo $c \in Q_d(R)$, então

$$c \sum_{i=j}^{l} a_i x^i = \sum_{i=j}^{l} a_i x^i c = \sum_{i=j}^{l} a_i (x^i c) = \sum_{i=j}^{l} a_i \sum_{r=0}^{i} \begin{pmatrix} i \\ r \end{pmatrix} d^r(c) x^{i-r}.$$

Usando a igualdade de polinômios, obtemos

$$ca_k x^k = a_k c x^k + \begin{pmatrix} k+1 \\ 1 \end{pmatrix} a_{k+1} d(c) x^k + \cdots + \begin{pmatrix} l \\ l-k \end{pmatrix} a_l d^{l-k}(c) x^k =$$

$$\sum_{i=k}^{l} \begin{pmatrix} i \\ i-k \end{pmatrix} a_i d^{i-k}(c) x^k$$

onde $k \in \{j, j+1, \cdots, l\}$ e com isto,

$$b_k = ca_k - \sum_{i=k}^{l} \begin{pmatrix} i \\ i-k \end{pmatrix} a_i d^{i-k}(c) = 0.$$

Note que,

$$f_j c = \left(\sum_{i=j}^{l} \begin{pmatrix} i \\ j \end{pmatrix} a_i x^{i-j} \right) c = \sum_{i=0}^{l-j} \begin{pmatrix} i+j \\ j \end{pmatrix} a_{i+j} (x^i c) =$$

$$\sum_{i=0}^{l-j} \begin{pmatrix} i+j \\ j \end{pmatrix} a_{i+j} \sum_{r=0}^{i} \begin{pmatrix} i \\ r \end{pmatrix} d^{i-r}(c) x^r =$$

$$\sum_{r=0}^{l-j} \left(\sum_{i=r}^{l-j} \begin{pmatrix} i+j \\ j \end{pmatrix} \begin{pmatrix} i \\ r \end{pmatrix} a_{i+j} d^{i-r}(c) x^r \right)$$

e desta forma,

$$cf_j - f_j c = \sum_{i=0}^{l-j} \begin{pmatrix} i+j \\ j \end{pmatrix} c a_{i+j} x^i - \sum_{r=0}^{l-j} \left(\sum_{i=r}^{l-j} \begin{pmatrix} i+j \\ j \end{pmatrix} \begin{pmatrix} i \\ r \end{pmatrix} a_{i+j} d^{i-r}(c) x^r \right).$$

Suponhamos que $i+j=k$ e $r=i=k-j$. Assim,

$$cf_j - f_jc =$$
$$\sum_{k=j}^{l} \begin{pmatrix} k \\ j \end{pmatrix} ca_k x^{k-j} - \sum_{k=j}^{l} \left(\sum_{i=k-j}^{l-j} \begin{pmatrix} i+j \\ j \end{pmatrix} \begin{pmatrix} i \\ k-j \end{pmatrix} a_{i+j} d^{i-k+j}(c) x^{k-j} \right) =$$
$$\sum_{k=j}^{l} \left(\begin{pmatrix} k \\ j \end{pmatrix} ca_k - \sum_{i=k-j}^{l-j} \begin{pmatrix} i+j \\ j \end{pmatrix} \begin{pmatrix} i \\ k-j \end{pmatrix} a_{i+j} d^{i-k+j}(c) \right) x^{k-j}.$$

Definimos $s_k = \begin{pmatrix} k \\ j \end{pmatrix} ca_k - \sum_{i=k}^{l} \begin{pmatrix} i \\ j \end{pmatrix} \begin{pmatrix} i-j \\ k-j \end{pmatrix} a_i d^{i-k}(c)$. Como $\begin{pmatrix} i \\ j \end{pmatrix} \begin{pmatrix} i-j \\ k-j \end{pmatrix} = \begin{pmatrix} k \\ j \end{pmatrix} \begin{pmatrix} i \\ i-k \end{pmatrix}$, então

$$s_k = \begin{pmatrix} k \\ j \end{pmatrix} ca_k - \sum_{i=k}^{l} \begin{pmatrix} k \\ j \end{pmatrix} \begin{pmatrix} i \\ i-k \end{pmatrix} a_i d^{i-k}(c) =$$
$$\begin{pmatrix} k \\ j \end{pmatrix} \left[ca_k - \sum_{i=k}^{l} \begin{pmatrix} i \\ i-k \end{pmatrix} a_i d^{i-k}(c) \right] = \begin{pmatrix} k \\ j \end{pmatrix} b_k = 0.$$

Desta maneira, $cf_j = f_jc$ e segue que $f_j \in Z$.

Como, para cada $j \in \{1, 2, \cdots, l\}$, $\delta(f_j) < \delta(f)$ então, pela minimalidade do grau de f, obtemos $\delta(f_j) = 0$. Conseqüentemente, $f_j = a_j \in C_d(R)$.

Suponhamos que $1 \leq j < i \leq l$. Desde que $\delta(f_j) = 0$, então $\begin{pmatrix} i \\ j \end{pmatrix} a_i = 0$, para todo $i \in \{j+1, j+2, \cdots, l\}$.

Se $char(R) = p < \infty$, então $\begin{pmatrix} i \\ j \end{pmatrix} \equiv 0(mod p)$ para todo $0 < j < i$ e com isto, $i = p, p^2, \cdots$. Assim, se i não é potência de p então $a_i = 0$. Desta maneira, $f = \sum_{i=j}^{l} a_i x^i = \sum_{k=0}^{m} a_{p^k} x^{p^k} + a_0$, onde $a_{p^m} = lc(f)$.

Claramente $f = a_{p^m}[x^{p^m} + \cdots + a_{p^m}^{-1} a_p x^p + a_{p^m}^{-1} a_{p^0} x^{p^0} + a_{p^m}^{-1} a_0]$. Consideremos $c_k = a_{p^m}^{-1} a_{p^k}$ e $-a = a_{p^m}^{-1} a_0$. Com isto, $f = a_l z \in C_d(R)[z]$, com z como descrito no enunciado.

Desde que $fc = cf$, para todo $c \in Q_d(R)$, então,

$$0 = ca_0 - a_0c - \sum_{k=0}^{m} a_{p^k} d^{p^k}(c),$$

ou seja,

$$\sum_{k=0}^{m} a_{p^k} d^{p^k}(c) = ca_0 - a_0c.$$

Definimos $b = -a_0$ e com isto, $\sum_{k=0}^{m} a_{p^k} d^{p^k}(c) = bc - cb$ é uma derivação interna de $Q_d(R)$ adjunta a b. Multiplicando a última igualdade por $a_{p^m}^{-1}$ obtemos

$$\sum_{k=0}^{m} c_k d^{p^k}(c) = (a_{p^m}^{-1}b)c - c(a_{p^m}^{-1}b) = ac - ca$$

para todo $c \in Q_d(R)$.

Suponhamos que $char(R) = 0$. Como $\begin{pmatrix} i \\ j \end{pmatrix} a_i = 0$, então $a_i = 0$, para todo $1 \leq j < i \leq l$ e deste modo, para $j = 1$ obtemos

$$f_1 = \sum_{i=1}^{l} \begin{pmatrix} i \\ 1 \end{pmatrix} a_i x^{i-1} = a_1 + \sum_{i=2}^{l} \begin{pmatrix} i \\ 1 \end{pmatrix} a_i x^{i-1} = a_1 \neq 0.$$

Assim, $f = a_0 + a_1x$ e desta maneira,

$$f = a_1(x + a_1^{-1}a_0) = a_1(x - a) = a_1 z,$$

onde $-a = a_1^{-1}a_0$ e z é como descrito no enunciado.

Observemos que $x - a = z \in Z$. Logo, para todo $q \in Q_d(R)$, $q(x - a) = (x - a)q$ e com isto, $d(q) = aq - qa$, o que implica que d é uma derivação interna de $Q_d(R)$ adjunta a a. Evidentemente, $f \in C_d(R)[z]$.

Seja $g \in Z$ e suponhamos que $\delta(g) < \delta(z)$. Então, $\delta(g) = 0$ e desta maneira, $g \in C_d(R) \subseteq C_d(R)[z]$. Suponhamos agora que $\delta(g) \geq \delta(z)$.

Por hipótese de indução, assumiremos que todo polinômio em Z com grau menor que $\delta(g)$ esteja em $C_d(R)[z]$ e seja $t \in Z$ tal que $\delta(t) \geq \delta(z)$. Sendo z mônico, existem $h, r \in Q_d(R)[x; d]$ tais que $t = zh + r$, onde $r = 0$ ou $\delta(r) < \delta(z) = Min(Z)$.

Denotamos por $[a, b] = ab - ba$ o comutador dos elementos a e b. Desde que $t \in Z$ então, para todo $q \in Q_d(R)$

$$0 = tq - qt = [t, q] = [zh + r, q] = (zh + r)q - q(zh + r) = zhq + rq - qzh - qr =$$
$$zhq - zqh + rq - qr = z[h, q] + [r, q]$$

e analogamente, $0 = [t, x] = z[h, x] + [r, x]$. Assim,

$$z[h, q] = -[r, q] = [q, r] \text{ e}$$
$$z[h, x] = -[r, x] = [x, r].$$

É fácil ver que $\delta([r, x]) \leq \delta(r) < \delta(z)$ e segue que, $\delta(z[h, x]) = \delta([x, r]) < \delta(z)$. Deste modo, $[x, r] = z[h, x] = 0$ e de maneira análoga, mostramos que $[q, r] = z[h, q] = 0$, para todo $q \in Q_d(R)$ e conseqüentemente $r \in Z$.

Como z é mônico, então $z[h, x] = 0$ e $z[h, q] = 0$ o que implica $[h, x] = 0$ e $[h, q] = 0$, respectivamente. Assim, $h \in Z$ e usando a hipótese de indução, temos que $h, r \in C_d(R)[z]$. Logo, $t \in C_d(R)[z]$ e portanto, $Z \subseteq C_d(R)[z]$. A outra inclusão é clara. $\square$

Capítulo 2

Ideais Primos em Skew Anel de Polinômios

O objetivo deste capítulo é estudar os ideais primos R-disjuntos no skew anel de Laurent $R < x; \rho >$ e no skew anel de polinômios do tipo automorfismo $R[x; \rho]$. Todos os resultados que serão apresentados neste capítulo são do artigo [3].

2.1 Ideais Primos em Skew Anel de Laurent

Durante esta seção, R é um anel com unidade e ρ é um automorfismo de R.

Seja $f = \sum_{i=-s}^{n} a_i x^i \in R < x; \rho >$. Então $\rho(f) = xfx^{-1}$, isto é,

$$\rho(f) = x(\sum_{i=-s}^{n} a_i x^i)x^{-1} = \sum_{i=-s}^{n} \rho(a_i)xx^i x^{-1} = \sum_{i=-s}^{n} \rho(a_i)x^i.$$

Assim, o automorfismo ρ pode ser estendido a um automorfismo de $R < x; \rho >$. Denotaremos esta extensão por ρ novamente e de maneira análoga podemos estender ρ a um automorfismo de $R[x; \rho]$.

Lema 2.1.1. *Seja I um ideal de $R < x;\rho >$. Então $I \cap R$ é um ideal ρ-invariante de R.*

Demonstração. Claramente $I \cap R$ é um ideal de R. Seja $a \in I \cap R$. Então, $\rho(a) = xax^{-1} \in I$ e com isto, $\rho(a) \in I \cap R$. De maneira análoga, se mostra que $\rho^{-1}(a) \in I \cap R$. Logo, $I \cap R$ é um ideal ρ-invariante de R. □

Lema 2.1.2. *Sejam K e L ideais ρ-invariantes de R. Então,*

$$KL < x;\rho >= K < x;\rho > L < x;\rho >.$$

Demonstração. Consideremos $ax^l \in K < x;\rho >$ e $bx^k \in L < x;\rho >$. Então, $(ax^l)(bx^k) = a\rho^l(b)x^{l+k} \in KL < x;\rho >$, desde que $\rho^l(b) \in L$. Logo, $K < x;\rho > L < x;\rho > \subseteq KL < x;\rho >$.

Por outro lado, seja $cdx^t \in KL < x;\rho >$. Assim,

$$cdx^t = (cx^0)(dx^t) \in K < x;\rho > L < x;\rho >$$

e com isto, $KL < x;\rho > \subseteq K < x;\rho > L < x;\rho >$. □

Lema 2.1.3. *Seja P um ideal primo de $R < x;\rho >$. Então $P \cap R$ é um ideal ρ-primo de R.*

Demonstração. Sejam K e L ideais ρ-invariantes de R tais que $KL \subseteq P \cap R$. Então, pelo Lema 2.1.2,

$$K < x;\rho > L < x;\rho >= KL < x;\rho > \subseteq (P \cap R) < x;\rho > \subseteq P.$$

Como P é um ideal primo de $R < x;\rho >$, então $K < x;\rho > \subseteq P$ ou $L < x;\rho > \subseteq P$. Logo, $K \subseteq P \cap R$ ou $L \subseteq P \cap R$ e portanto, $P \cap R$ é um ideal ρ-primo de R. □

Dizemos que um ideal I de $R < x;\rho >$ ($R[x;\rho]$) é *R-disjunto* se $I \cap R = 0$. Um polinômio $f \in R[x;\rho]$ é chamado *próprio* se seu termo independente for não-nulo. No caso em que f é um polinômio próprio, o grau e o coeficiente líder de f são definidos de maneira óbvia e denotados por $\delta(f)$ e $lc(f)$, respectivamente.

Seja I um ideal não-nulo R-disjunto de $R < x; \rho >$. Então existe um polinômio próprio de grau mínimo n em I e este inteiro n é dito a *minimalidade* de I, o qual será denotado por $Min(I)$.

Denotaremos por $\tau(I)$ o ideal ρ-invariante de R que consiste de todos os coeficientes líderes dos polinômios próprios de grau mínimo n em I, juntamente com o zero.

Seja P um ideal primo de $R < x; \rho >$. Então, fatorando $P \cap R$ e $(P \cap R) < x; \rho >$ de R e $R < x; \rho >$ respectivamente, podemos assumir que R é um anel ρ-primo e P é R-disjunto.

No decorrer desta seção, assumiremos que R é um anel ρ-primo, $Q_\rho(R)$ é o anel ρ-quociente à esquerda de Martindale de R e Z é o centro do anel $Q_\rho(R) < x; \rho >$.

Lema 2.1.4. *Seja I um ideal não-nulo R-disjunto de $R < x; \rho >$ tal que $Min(I) = n$. Então existe um único polinômio mônico próprio $f_I \in Q_\rho(R) < x; \rho >$ tal que, para todo $f \in I$ com grau n, temos que $f = lc(f)f_I$. Além disto, $f_I x^{-n} \in Z$.*

Demonstração. Seja I um ideal não-nulo R-disjunto de $R < x; \rho >$ tal que $Min(I) = n$. Para cada $a \in \tau(I)$ existe um único polinômio $f \in I$ tal que $lc(f) = a$ e $\delta(f) = n$. De fato, suponhamos que exista $g \in I$ tal que $lc(g) = a$ e $\delta(g) = n$. Então, $f - g$ é um polinômio em I tal que $\delta(f - g) < n$. Logo, $f = g$ e com isto f é único. Consideremos $f = ax^n + a_{n-1}x^{n-1} + \cdots + a_0$.

Definimos $\beta_i : \tau(I) \to R$ por $\beta_i(a) = a_i$ para todo $i \in \{0, 1, \cdots, n\}$, onde $a_n = a$. Mostraremos que β_i é um homomorfismo de R-módulos à esquerda. Com efeito, como para cada $a \in \tau(I)$ existe um único polinômio $f \in I$ com $\delta(f) = n$ e $lc(f) = a$ temos que β_i está bem definida, para cada $i \in \{0, 1, \cdots, n\}$.

Para todo $a, b \in \tau(I)$ e $r \in R$ existem $f, g \in I$ tais que $f = ax^n + a_{n-1}x^{n-1} + \cdots + a_0$ e $g = bx^n + b_{n-1}x^{n-1} + \cdots + b_0$. Assim, $f + g = (a + b)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + a_0 + b_0 \in I$ e $rf = rax^n + ra_{n-1}x^{n-1} + \cdots + ra_0$. Desta maneira, $\beta_i(a + b) = a_i + b_i = \beta_i(a) + \beta_i(b)$ e $\beta_i(ra) = ra_i = r\beta_i(a)$

Deste modo, pelo Lema 1.1.2, existem $q_n = 1, q_{n-1}, \cdots, q_0 \in Q_\rho(R)$ tais que $\beta_i(a) = aq_i$, para todo $i \in \{0, 1, \cdots, n\}$.

Definimos $f_I = x^n + q_{n-1}x^{n-1} + \cdots + q_0 \in Q_\rho(R) < x; \rho >$. Claramente f_I é o único polinômio próprio de $Q_\rho(R) < x; \rho >$ tal que $f = lc(f)f_I$, para todo $f \in I$ com $\delta(f) = n$. Afirmamos que $f_I x^{-n} \in Z$. De fato, para cada $a \in \tau(I)$, temos que $\rho(a)f_I - \rho(af_I) \in I$ e $\delta(\rho(a)f_I - \rho(af_I)) < n$. Como $Min(I) = n$, então $\rho(a)(f_I - \rho(f_I)) = 0$ e conseqüentemente, $\tau(I)[f_I - \rho(f_I)] = 0$.

Por sua vez, $f_I - \rho(f_I) = (q_{n-1} - \rho(q_{n-1}))x^{n-1} + \cdots + q_0 - \rho(q_0)$ e com isto, $\tau(I)[q_i - \rho(q_i)] = 0$, para todo $i \in \{0, 1, \cdots, n-1\}$. Pelo Lema 1.1.2, $q_i = \rho(q_i)$, para todo $i \in \{0, 1, \cdots, n-1\}$ e segue que, $f_I = \rho(f_I)$. Logo,

$$f_I x = x f_I. \tag{2.1}$$

Para cada $a \in \tau(I)$ e $b \in R$, $a(f_I b - \rho^n(b)f_I) \in I$ é tal que $\delta(a(f_I b - \rho^n(b)f_I)) < n$. Deste modo, $a(f_I b - \rho^n(b)f_I) = 0$ e segue que, $\tau(I)(f_I b - \rho^n(b)f_I) = 0$. Assim, usando o Lema 1.1.2,

$$f_I b = \rho^n(b) f_I. \tag{2.2}$$

Para cada $c \in R$, temos que

$$c(f_I x^{-n}) = (cf_I)x^{-n} = (f_I \rho^{-n}(c))x^{-n} = f_I(\rho^{-n}(c)x^{-n}) = f_I(x^{-n}c) = (f_I x^{-n})c.$$

Seja $q \in Q_\rho(R)$. Então, pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo J de R tal que $Jq \subseteq R$. Desta maneira, para todo $\gamma \in J$ temos que,

$$\gamma q(f_I x^{-n}) = (f_I x^{-n})\gamma q = (f_I x^{-n}\gamma)q = \gamma(f_I x^{-n})q$$

e com isto, $\gamma[q(f_I x^{-n}) - (f_I x^{-n})q] = 0$. Logo, pelo Lema 1.1.2,

$$q(f_I x^{-n}) = (f_I x^{-n})q.$$

Além disto,

$$x(f_I x^{-n}) = (xf_I)x^{-n} = (f_I x)x^{-n} = f_I(xx^{-n}) = (f_I x^{-n})x.$$

Portanto, $f_I x^{-n} \in Z$. $\square$

O polinômio f_I construído no Lema 2.1.4 será chamado de *polinômio canônico* do ideal não-nulo R-disjunto I de $R < x; \rho >$.

Corolário 2.1.5. *Sejam I um ideal R-disjunto de $R < x; \rho >$ e f_I o polinômio canônico de I. Então, $I \subseteq Q_\rho(R) < x; \rho > f_I \cap R < x; \rho >$.*

Demonstração. Seja $f \in I \cap R[x; \rho]$ e suponhamos que $Min(I) = n$. Pelo algoritmo da divisão, existem $h, r \in Q_\rho(R)[x; \rho]$ tais que $f = hf_I + r$, onde $r = 0$ ou $\delta(r) < \delta(f_I) = Min(I)$.

Pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo J de R tal que $Jh \subseteq R[x; \rho]$ e $Jr \subseteq R[x; \rho]$.

Sejam $j \in J$ e $c \in \tau(I)$. Então,

$$cjr = cj(f - hf_I) = cjf - cjhf_I = cjf - cf_I\rho^{-n}(jh).$$

Claramente $cjf \in I$. Como $cf_I \in I$ e $jh \in Jh \subseteq R[x; \rho]$, então $cf_I\rho^{-n}(jh) \in I$ e segue que $cjr \in I$. Observando que $\delta(cjr) \leq \delta(r) < Min(I)$, temos que $cjr = 0$ e, com isto, $\tau(I)Jr = 0$. Desde que $\tau(I)J \in \mathcal{I}_\rho$ então, pelo Lema 1.1.2, $r = 0$. Assim, $f = hf_I \in Q_\rho(R)[x; \rho]f_I \cap R[x; \rho] \subseteq Q_\rho(R) < x; \rho > f_I \cap R < x; \rho >$.

Para cada $f \in I$, existe $t \in \mathbb{N}$ tal que $fx^t \in I \cap R[x; \rho]$. Pelo mesmo raciocínio desenvolvido anteriormente, $fx^t \in Q_\rho(R) < x; \rho > f_I \cap R < x; \rho >$ e segue que $f \in Q_\rho(R) < x; \rho > f_I \cap R < x; \rho >$. Logo, $I \subseteq Q_\rho(R) < x; \rho > f_I \cap R < x; \rho >$. $\square$

Definição 2.1.6. *Sejam I um ideal não-nulo R-disjunto de $R < x; \rho >$ e f_I o polinômio canônico de I. Definimos o fecho $[I]$ de I por*

$$[I] = Q_\rho(R) < x; \rho > f_I \cap R < x; \rho >.$$

O ideal I é dito fechado se $[I] = I$ e, no Corolário 2.1.12, mostraremos que $[[I]] = [I]$.

Iremos obter uma caracterização intrínseca de um ideal fechado de $R < x; \rho >$. Sejam I um ideal R-disjunto de $R < x; \rho >$, $f = ax^n + a_{n-1}x^{n-1} + \cdots + a_0$ um polinômio próprio de grau mínimo n em I e $g = \rho^j(f)ra - \rho^j(a)\rho^n(rf) \in I$, para todo $r \in R$ e $j \in \mathbb{Z}$.

Como $\delta(g) < n$ então,

$$\rho^j(f)ra = \rho^j(a)\rho^n(rf) \tag{2.3}$$

para todo $r \in R$ e $j \in \mathbb{Z}$.

Seja Γ o conjunto de todos os polinômios próprios em $R < x; \rho >$ que satisfaçam a condição 2.3. Para $f \in \Gamma$ com $lc(f) = a$, consideremos

$$[f] = \{g \in R < x; \rho >\text{: existe um ideal } \rho\text{-invariante não-nulo } J \text{ de } R \text{ tal que } aJ\rho^i(g) \subseteq fR < x; \rho >, \text{ para todo } i \in \mathbb{Z}.\}$$

Analogamente, denotaremos por $\Gamma_{Q_\rho(R)}$ e $[f]_{Q_\rho(R)}$ os correspondentes subconjuntos de $Q_\rho(R) < x; \rho >$.

Observação 2.1.7. *Sejam I um ideal R-disjunto de $R < x; \rho >$ e f_I o polinômio canônico de I. Note que $\Gamma^0_{Q_\rho(R)} = \{f_0 \in \Gamma_{Q_\rho(R)} : f_0$ é mônico$\}$ é o conjunto de todos os polinômios $g \in Q_\rho(R) < x; \rho >$ tais que g é mônico, próprio e $gx^{-\delta(g)} \in Z$. Logo, f_I está em $\Gamma^0_{Q_\rho(R)}$ pois, pelo Lema 2.1.4, $f_I x^{-\delta(f_I)} \in Z$.*

Lema 2.1.8. *Seja $f \in \Gamma$. Então $[f]$ é um ideal R-disjunto de $R < x; \rho >$ que contém f como polinômio próprio de grau mínimo.*

Demonstração. Seja $f \in \Gamma$ tal que $f = ax^n + a_{n-1}x^{n-1} + \cdots + a_0$. Mostraremos que $[f]$ é um ideal de $R < x; \rho >$. De fato, note que $0 \in [f]$, pois sendo $J = R$ temos que $aR\rho^i(0) = 0 \in fR < x; \rho >$, para todo $i \in \mathbb{Z}$.

Sejam $g, h \in [f]$ e $r \in R < x; \rho >$. Então existem ideais ρ-invariantes não-nulos J e K de R tais que $aJ\rho^i(g) \subseteq fR < x; \rho >$ e $aK\rho^i(h) \subseteq fR < x; \rho >$, para todo $i \in \mathbb{Z}$.

Como $J \cap K \in \mathcal{I}_\rho$ então, para cada $y \in J \cap K$

$$ay\rho^i(g+h) = ay[\rho^i(g) + \rho^i(h)] = ay\rho^i(g) + ay\rho^i(h) \in fR < x; \rho >.$$

Além disto, para cada $r \in R$, temos que

$$aJ\rho^i(gr) = aJ\rho^i(g)\rho^i(r) \subseteq fR < x; \rho > \rho^i(r) \subseteq fR < x; \rho >.$$

Assim, $g + h \in [f]$ e $gr \in [f]$.

Consideremos que $r = r_n x^n + r_{n-1}x^{n-1} + \cdots + r_0$. Como para cada $j \in J$, $b \in R$ e $k \in \{0, 1, \cdots, n\}$, $ajbx^k\rho^i(g) = ajb\rho^{i+k}(g)x^k \in aJ\rho^{i+k}(g)x^k \subseteq fR < x; \rho > x^k \subseteq fR < x; \rho >$ então, $aj\rho^i(rg) = aj\rho^i(r)\rho^i(g) = aj\rho^i(r_n)x^n\rho^i(g) + \cdots + aj\rho^i(r_0)\rho^i(g) \in fR < x; \rho >$, para todo $i \in \mathbb{Z}$. Desta maneira, $aJ\rho^i(rg) \subseteq fR < x; \rho >$ e segue que, $rg \in [f]$. Logo, $[f]$ é um ideal de $R < x; \rho >$.

Seja $j = n - i$ na equação 2.3. Então,

$$\rho^{n-i}(f)ra = \rho^{n-i}(a)\rho^n(r)\rho^n(f)$$

e segue que,

$$a\rho^i(r)\rho^i(f) = f\rho^{i-n}(r)\rho^{i-n}(a).$$

Conseqüentemente, $a\rho^i(r)\rho^i(f) \in fR < x; \rho >$, para todo $r \in R$ e, com isto, $aR\rho^i(f) \subseteq fR < x; \rho >$, para todo $i \in \mathbb{Z}$. Logo, $f \in [f]$.

Afirmamos que f é um polinômio próprio de grau mínimo em $[f]$. Com efeito, suponhamos que exista um polinômio próprio não-nulo $h \in [f]$ tal que $lc(h) = m$ e $\delta(h) < \delta(f)$. Assim, existe um ideal ρ-invariante não-nulo J de R tal que $aJ\rho^i(h) \subseteq fR < x; \rho >$, para todo $i \in \mathbb{Z}$.

Se $aJ\rho^i(h) = 0$ para todo $i \in \mathbb{Z}$ então, em particular, $aJ\rho^i(m) = 0$ para todo $i \in \mathbb{Z}$. Deste modo, $a(\sum_{i\in\mathbb{Z}} J\rho^i(m)J) = 0$.

Como $\sum_{i\in\mathbb{Z}} J\rho^i(m)J \neq 0$ então, pelo Lema 1.1.2, $a = 0$ o que contradiz o fato de $a = lc(f) \neq 0$. Desta maneira, existem $k \in \mathbb{Z}$ e $b \in J$ tais que $0 \neq ab\rho^k(h) \in$

$aJ\rho^k(h) \subseteq fR < x;\rho >$. Seja $g = \sum_{i=s}^{m} b_i x^i \in R < x;\rho >$ tal que $ab\rho^k(h) = fg$, com $m - s$ minimal e $s < m$.

Suponhamos que $m \geq 0$ e $lc(fg) = a\rho^n(b_m) \neq 0$. Então, $\delta(h) \geq \delta(ab\rho^j(h)) = \delta(fg) = n+m \geq n = \delta(f)$, o que contradiz o fato que $\delta(h) < \delta(f)$. Assim, $a\rho^n(b_m) = 0$.

Considerando $j = 0$ na equação 2.3, temos que

$$a\rho^n(b_m r f) = f b_m r a = 0.$$

Usando a equação 2.3 novamente, obtemos que $\rho^j(fb_m)ra = 0$, para todo $j \in \mathbb{Z}$ e $r \in R$. O termo de grau $n-1$ da última igualdade é $\rho^{j+1-n}(a_{n-1})\rho^j(b_m)ra = 0$, para todo $r \in R$ e $j \in \mathbb{Z}$.

Consideremos $I = \sum_{j\in\mathbb{Z}} R\rho^j(\rho^{1-n}(a_{n-1})b_m)R$ e suponhamos que $I \neq 0$. Pela igualdade anterior, temos que $Ia = 0$ e com isto, $a = 0$, o que contradiz que $a = lc(f) \neq 0$. Deste modo, $I = 0$ e segue que $\rho^{1-n}(a_{n-1})b_m = 0$.

Repetindo este processo um número suficiente de vezes obtemos que $\rho^{-i}(a_i)b_m = 0$, para todo $i \in \{0, 1, \cdots, n-1\}$. Deste modo, $fb_m = 0$ e com isto, $fg = f(g - b_m x^m)$, o que contradiz a escolha de g .

Se $s < m < 0$, então repetindo o mesmo raciocínio anterior para $-s > 0$, obtemos que $fg = f(g - b_{-s}x^{-s})$, o que contradiz a escolha de g novamente.

Logo, f é um polinômio de grau mínimo em $[f]$ e portanto, $[f]$ é um ideal R-disjunto de $R < x;\rho >$. $\square$

Lema 2.1.9. *Sejam I um ideal não-nulo R-disjunto de $R < x;\rho >$ e f_I o polinômio canônico de I. Suponhamos que $Min(I) = n$. Então, para todo $g \in Q_\rho(R) < x;\rho >$, $gf_I = f_I\rho^{-n}(g)$.*

Demonstração. Seja $g = \sum_{i=p}^{q} b_i x^i$. Então, usando as igualdades 2.1 e 2.2, obtemos que $gf_I = (\sum_{i=p}^{q} b_i x^i)f_I = \sum_{i=p}^{q} b_i f_I x^i = \sum_{i=p}^{q} f_I \rho^{-n}(b_i)x^i = f_I\rho^{-n}(g)$. $\square$

Lema 2.1.10. *Sejam I um ideal R-disjunto de $R < x;\rho >$ e f_I o polinômio canônico de I. Então, $Min(f_I Q_\rho(R) < x;\rho >) = \delta(f_I) = Min(I)$.*

Demonstração. Suponhamos que existe $h = f_I g \in f_I Q_\rho(R) < x;\rho >$ não-nulo tal que $\delta(h) < Min(I)$, para algum $g \in Q_\rho(R) < x;\rho >$. Pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo L de R tal que $Lh \subseteq R < x;\rho >$ e $Lg \subseteq R < x;\rho >$. Seja $J = L \cap \tau(I)$ um ideal ρ-invariante não-nulo de R.

Para todo $a, b \in J$, temos que

$$abh = abf_I g = af_I \rho^{-\delta(f_I)}(b)g.$$

Como $\rho^{-\delta(f_I)}(b)g \in Lg \subseteq R < x;\rho >$ e $af_I \in I$, então $abh \in I$. Desde que $\delta(abh) \leq \delta(h) < Min(I)$, então $abh = 0$ e conseqüentemente, $J^2 h = 0$. Logo, pelo Lema 1.1.2, $h = 0$ e portanto, $Min(f_I Q_\rho(R) < x;\rho >) = Min(I)$. □

Teorema 2.1.11. *Sejam I um ideal R-disjunto de $R < x;\rho >$ e f um polinômio de grau mínimo n em I. Então, $f \in \Gamma$ e $[I] = [f]$.*

Demonstração. Seja f um polinômio de grau mínimo n em I tal que $lc(f) = a$. Para cada $j \in \mathbb{Z}$ e $r \in R$, $\rho^j(f)ra - \rho^j(a)\rho^n(rf) \in I$ é tal que $\delta(\rho^j(f)ra - \rho^j(a)\rho^n(rf)) < n$. Desta maneira, f satisfaz a condição 2.3 e com isto, $f \in \Gamma$.

Consideremos $h \in [I] = Q_\rho(R) < x;\rho > f_I \cap R < x;\rho >$, onde f_I é o polinômio canônico de I. Então, existe $g \in Q_\rho(R) < x;\rho >$ tal que $h = gf_I$.

Pelo Lema 1.1.2, existe $J \in \mathcal{I}_\rho$ tal que $Jg \subseteq R < x;\rho >$. Assim, para todo $j \in J$ e $i \in \mathbb{Z}$

$$aj\rho^i(h) = aj\rho^i(gf_I) = aj\rho^i(g)f_I.$$

Usando o Lema 2.1.9, $j\rho^i(g)f_I = f_I\rho^{-n}(j\rho^i(g))$ e com isto, $aj\rho^i(h) = af_I\rho^{-n}(j\rho^i(g)) \in fR < x;\rho >$. Deste modo, $aJ\rho^i(h) \subseteq fR < x;\rho >$ e segue que, $h \in [f]$.

Por outro lado, seja $g = \sum_{i=q}^{s} c_i x^i \in [f]$ e suponhamos que $q < 0$. Pelo algoritmo da divisão, existem $h, r \in Q_\rho(R)[x;\rho]$ tais que $gx^{-q} = hf_I + r \in R[x;\rho]$, onde $r = 0$

ou $\delta(r) < \delta(f_I)$. Como $gx^{-q} \in [f]$, então existe um ideal ρ-invariante não-nulo L de R tal que $aL\rho^i(gx^{-q}) \subseteq fR < x;\rho >$, para todo $i \in \mathbb{Z}$ e, pelo Lema 1.1.2, existe um ideal ρ-invariante não-nulo K de R tal que $Kr \subseteq R[x;\rho]$ e $Kh \subseteq R[x;\rho]$.

Assim, para cada $l \in K \cap L$ e $i \in \mathbb{Z}$

$$al\rho^i(r) = al\rho^i(g)x^{-q} - al\rho^i(h)f_I = al\rho^i(g)x^{-q} - af_I\rho^{-n}(l\rho^i(h)).$$

Note que $al\rho^i(g)x^{-q} \in fR < x;\rho >= af_IR < x;\rho > \subseteq f_IR < x;\rho >$ e $af_I\rho^{-n}(l\rho^i(h)) \in I \subseteq f_IQ_\rho(R) < x;\rho >$. Desta maneira, $al\rho^i(r) \in f_IQ_\rho(R) < x;\rho >$.

Por sua vez, segue do Lema 2.1.10, que $Min(I) = Min(f_IQ_\rho(R) < x;\rho >)$ e com isto, $\delta(al\rho^i(r)) \leq \delta(r) < Min(f_IQ_\rho(R) < x;\rho >)$. Conseqüentemente, $al\rho^i(r) = 0$.

Consideremos $r = a_sx^s + a_{s-1}x^{s-1} + \cdots + a_0$. Desta forma,

$$\begin{gathered}0 = al\rho^i(r) = al\rho^i(a_sx^s + a_{s-1}x^{s-1} + \cdots + a_0) = \\ al\rho^i(a_s)x^s + al\rho^i(a_{s-1})x^{s-1} + \cdots + al\rho^i(a_0)\end{gathered}$$

e obtemos, $a(K \cap L)\rho^i(a_0) = 0$ para todo $i \in \mathbb{Z}$. Assim, $a\sum_{i\in\mathbb{Z}}(K \cap L)\rho^i(a_0)(K \cap L) = 0$. Como R é um anel ρ-primo e $a \neq 0$ então $\sum_{i\in\mathbb{Z}}(K \cap L)\rho^i(a_0)(K \cap L) = 0$ e desta maneira, $a_0 = 0$.

Repetindo esse processo aos demais coeficientes de r obtemos que $r = 0$ e segue que $gx^{-q} = hf_I$. Logo $g \in Q_\rho(R) < x;\rho > f_I \cap R < x;\rho >= [I]$. Procedendo de maneira análoga para o caso $q > 0$, obtemos o mesmo resultado. Portanto, $[f] = [I]$. $\square$

Corolário 2.1.12. *Seja I um ideal não-nulo R-disjunto de $R < x;\rho >$. Então $[I]$ é o maior ideal de $R < x;\rho >$ que contém I e satisfaz $Min([I]) = Min(I)$. Em particular, $[[I]] = [I]$.*

Demonstração. Sejam I um ideal não-nulo R-disjunto de $R < x;\rho >$ e f um polinômio de grau mínimo n em I. Pela Proposição 2.1.11 e Lema 2.1.8, $f \in \Gamma$ e $[I] = [f]$ é um ideal R-disjunto de $R < x;\rho >$ que contém f como polinômio de grau mínimo. Assim,

$$Min([I]) = Min([f]) = \delta(f) = Min(I).$$

Por sua vez, pelo Corolário 2.1.5, temos que $I \subseteq [I]$. Deste modo, $[I]$ é um ideal de $R < x;\rho >$ que contém I e satisfaz $Min([I]) = Min(I)$.

Seja J um ideal R-disjunto de $R < x;\rho >$ tal que $I \subseteq J$ e $Min(J) = Min(I)$. Como f é um polinômio em J de grau minimal então, pela Proposição 2.1.11, $[J] = [f]$ e com isto, $J \subseteq [J] = [f] = [I]$. Conseqüentemente, $[I]$ é o maior ideal de $R < x;\rho >$ que contém I e satisfaz $Min([I]) = Min(I)$.

Consideremos $f_{[I]}$ o polinômio canônico do ideal R-disjunto $[I]$ de $R < x;\rho >$. Pelo Corolário 2.1.5,

$$[I] \subseteq Q_\rho(R) < x;\rho > f_{[I]} \cap R < x;\rho >= [[I]].$$

De maneira análoga ao raciocínio anterior, obtemos $Min([[I]]) = Min(I)$ e $I \subseteq [I] \subseteq [[I]]$. Logo, $[I] = [[I]]$. $\square$

Lema 2.1.13. *Seja $f_0 \in \Gamma^0_{Q_\rho(R)}$ um polinômio próprio. Então, $Q_\rho(R) < x;\rho > f_0$ é um ideal de $Q_\rho(R) < x;\rho >$.*

Demonstração. Claramente $0 \in Q_\rho(R) < x;\rho > f_0$. Sejam $f, g \in Q_\rho(R) < x;\rho > f_0$ e $r \in Q_\rho(R) < x;\rho >$, tais que $f = f'f_0$ e $g = g'f_0$. Como $f_0 \in \Gamma^0_{Q_\rho(R)}$ então, pela Observação 2.1.7, $f_0x^{-n} \in Z$, onde $n = \delta(f_0)$. Logo,

$$f + g = f'f_0 + g'f_0 = (f' + g')f_0 \in Q_\rho(R) < x;\rho > f_0,$$
$$rf = r(f'f_0) = (rf')f_0 \in Q_\rho(R) < x;\rho > f_0$$
$$\text{e } fr = (f'f_0)r = (f'f_0)x^{-n}\rho^n(r)x^n = f'(f_0x^{-n})\rho^n(r)x^n = f'\rho^n(r)(f_0x^{-n})x^n =$$
$$(f'\rho^n(r))f_0 \in Q_\rho(R) < x;\rho > f_0.$$

Portanto, $Q_\rho(R) < x;\rho > f_0$ é um ideal de $Q_\rho(R) < x;\rho >$. $\square$

Lema 2.1.14. *Um ideal $Q_\rho(R)$-disjunto J de $Q_\rho(R) < x;\rho >$ é fechado se, e somente se, $J = Q_\rho(R) < x;\rho > f_0$ para algum polinômio próprio $f_0 \in \Gamma^0_{Q_\rho(R)}$.*

Demonstração. Suponhamos que $J = Q_\rho(R) < x;\rho > f_0$ para algum polinômio próprio $f_0 \in \Gamma^0_{Q_\rho(R)}$ tal que $\delta(f_0) = n$. Pela Observação 2.1.7, $f_0x^{-n} \in Z$ e, pelo Lema 2.1.13, J é um ideal de $Q_\rho(R) < x;\rho >$.

Sejam I um ideal de $Q_\rho(R) < x;\rho >$ tal que $J \subseteq I$ e $Min(I) = n$ e $g \in I$. Então, existe $t \in \mathbb{N}$ tal que $gx^t \in I \cap Q_\rho(R)[x;\rho]$

Pelo algoritmo da divisão, existem $h, r \in Q_\rho(R)[x;\rho]$ tais que $gx^t = hf_0 + r$, onde $r = 0$ ou $\delta(r) < \delta(f_0)$. Claramente, temos $r = gx^t - hf_0 \in I$. No entanto, $\delta(r) < Min(I)$, e com isto, $r = 0$. Assim, $gx^t = hf_0 \in J$ e segue que, $g \in J$. Logo, $I = J$ e portanto, J é fechado.

Reciprocamente, consideremos J um ideal não-nulo fechado $Q_\rho(R)$-disjunto de $Q_\rho(R) < x;\rho >$. Assim, $I = J \cap R < x;\rho >$ é um ideal não-nulo R-disjunto de $R < x;\rho >$. Seja f_I o polinômio canônico de I e suponhamos que $Min(J) < Min(I)$.

Seja $f \in J$ um polinômio não-nulo tal que $\delta(f) = Min(J)$. Pelo Lema 1.1.2, existe um ρ-ideal invariante não-nulo L de R tal que $Lf \subseteq R < x;\rho >$.

Como, para todo $l \in L$, $lf \in I$ é tal que $\delta(lf) \leq \delta(f) = Min(J) < Min(I)$ então, $Lf = 0$. Pelo Lema 1.1.2, obtemos que $f = 0$, o que contradiz o fato que f não é nulo. Logo, $Min(J) = Min(I) = \delta(f_I)$.

Sejam $f \in J$ e $t \in \mathbb{N}$ tais que $fx^t \in Q_\rho(R)[x;\rho]$. Pelo algoritmo da divisão, existem $h, r \in Q_\rho(R)[x;\rho]$ tais que $fx^t = hf_I + r$, onde $r = 0$ ou $\delta(r) < \delta(f_I)$. Usando um processo semelhante a prova do Corolário 2.1.5, temos que $r = 0$ e com isto, $f = hf_Ix^{-t} \in Q_\rho(R) < x;\rho > f_I$. Assim, $J \subseteq Q_\rho(R) < x;\rho > f_I$.

Como $Q_\rho(R) < x;\rho > f_I$ é um ideal de $Q_\rho(R) < x;\rho >$ que contém J e satisfaz $Min(Q_\rho(R) < x;\rho > f_I) = Min(I) = Min(J)$ então, pelo Corolário 2.1.12, concluímos que $Q_\rho(R) < x;\rho > f_I = [J]$. Por hipótese, J é fechado e desta maneira, $J = Q_\rho(R) < x;\rho > f_I$. □

Definimos R_m como sendo o conjunto de todos os polinômios $f \in R[x;\rho]$ tais que $\delta(f) \leq m$ juntamente com o zero. Seja I um ideal não-nulo de $R < x;\rho >$. Definimos

$I \cap R_m$ como sendo o conjunto dos polinômios $f \in I \cap R[x;\rho]$ tais que $\delta(f) \leq m$.

Lema 2.1.15. *Sejam I um ideal não-nulo de $R < x;\rho >$ e $f \in I$ um polinômio não-nulo de grau mínimo n em I tal que $lc(f) = a$. Suponhamos que $m \geq n$ e que $g \in I \cap R_m$. Se $a_j \in R$ e i_j são inteiros não-negativos para todo $j \in \{1, 2, \cdots, m-n\}$, então existe $h \in R_{m-n}$ tal que*

$$ha_0\rho^{i_0}(f) = g \prod_{j=0}^{m-n} \rho^{-n}(a_{m-n-j}\rho^{i_{m-n-j}}(a)) \tag{2.4}$$

para todo $a_0 \in R$ e $i_0 \in \mathbb{Z}$.

Demonstração. Suponhamos que $m = n$ e seja $g \in I \cap R_m$ tal que $lc(g) = b$. Se $\delta(g) < m$, então $g = 0$ e com isto, existe $h = 0 \in R_0$ de modo que

$$ha_0\rho^{i_0}(f) = g\rho^{-n}(a_0\rho^{i_0}(a))$$

para todo $a_0 \in R$ e $i_0 \in \mathbb{Z}$.

Suponhamos que $\delta(g) = m$ e seja $p = ba_0\rho^{i_0}(f) - g\rho^{-n}(a_0\rho^{i_0}(a)) \in I$. Como $\delta(p) < Min(I)$, então $p = 0$. Deste modo,

$$ba_0\rho^{i_0}(f) = g\rho^{-n}(a_0\rho^{i_0}(a)) \tag{2.5}$$

para todo $a_0 \in R$ e $i_0 \in \mathbb{Z}$. Logo, a igualdade 2.4 está satisfeita para o caso $m = n$. Suponhamos que $m > n$ e consideremos

$$g' = g\rho^{-n}(a_{m-n}\rho^{i_{m-n}}(a)) - x^{m-n}ba_{m-n}\rho^{i_{m-n}}(f).$$

Desta maneira,

$$g\rho^{-n}(a_{m-n}\rho^{i_{m-n}}(a)) = g' + x^{m-n}ba_{m-n}\rho^{i_{m-n}}(f). \tag{2.6}$$

Se $m - n = 1$ então

$$g\prod_{j=0}^{1}\rho^{-n}(a_{1-j}\rho^{i_{1-j}}(a)) = g\rho^{-n}(a_1\rho^{i_1}(a))\rho^{-n}(a_0\rho^{i_0}(a)).$$

Da igualdade 2.6, segue que

$$g\rho^{-n}(a_1\rho^{i_1}(a)) = g' + xba_1\rho^{i_1}(f)$$

e com isto,

$$g\prod_{j=0}^{1}\rho^{-n}(a_{1-j}\rho^{i_{1-j}}(a)) = g'\rho^{-n}(a_0\rho^{i_0}(a)) + xba_1\rho^{i_1}(f)\rho^{-n}(a_0\rho^{i_0}(a)). \tag{2.7}$$

Como $g', \rho^{i_1}(f) \in I \cap R_m$ então, segue da igualdade 2.5 que

$$g'\rho^{-n}(a_0\rho^{i_0}(a)) = lc(g')a_0\rho^{i_0}(f) \text{ e}$$
$$xba_1\rho^{i_1}(f)\rho^{-n}(a_0\rho^{i_0}(a)) = xba_1lc(\rho^{i_1}(f))a_0\rho^{i_0}(f).$$

Usando a igualdade 2.7, temos que

$$g\prod_{j=0}^{1}\rho^{-n}(a_{1-j}\rho^{i_{1-j}}(a)) = [lc(g') + xba_1lc(\rho^{i_1}(f))]a_0\rho^{i_0}(f)$$

onde $lc(g') + xba_1lc(\rho^{i_1}(f)) \in R_1$ e com isto, a igualdade 2.4 está satisfeita para o caso $m - n = 1$. Suponhamos, por hipótese de indução, que existe $t \in R_k$ tal que $ta_0\rho^{i_0}(f) = g\prod_{j=0}^{k}\rho^{-n}(a_{k-j}\rho^{i_{k-j}}(a))$, para todo $k < m - n$. Note que

$$g\prod_{j=0}^{m-n}\rho^{-n}(a_{m-n-j}\rho^{i_{m-n-j}}(a)) =$$
$$g\rho^{-n}(a_{m-n}\rho^{i_{m-n}}(a))\prod_{j=0}^{m-n-1}\rho^{-n}(a_{m-n-j-1}\rho^{i_{m-n-j-1}}(a)).$$

Pela igualdade 2.6,

$$g\prod_{j=0}^{m-n}\rho^{-n}(a_{m-n-j}\rho^{i_{m-n-j}}(a)) = g'\prod_{j=0}^{m-n-1}\rho^{-n}(a_{m-n-j-1}\rho^{i_{m-n-j-1}}(a)) +$$
$$x^{m-n}ba_{m-n}\rho^{i_{m-n}}(f)\prod_{j=0}^{m-n-1}\rho^{-n}(a_{m-n-j-1}\rho^{i_{m-n-j-1}}(a)).$$

Como $g', x^{m-n}ba_{m-n}\rho^{i_{m-n}}(f) \in I \cap R_m$ então, por hipótese de indução, existem $t_1, t_2 \in R_{m-n-1}$ tais que

$$g\prod_{j=0}^{m-n}\rho^{-n}(a_{m-n-j}\rho^{i_{m-n-j}}(a)) = (t_1 + t_2)a_0\rho^{i_0}(f)$$

com $t_1 + t_2 \in R_{m-n}$. A prova está completa. $\square$

O próximo lema é fundamental na prova do principal teorema desta seção.

Lema 2.1.16. *Seja P um ideal não-nulo R-disjunto de $R < x; \rho >$. Então P é primo se, e somente se, R é ρ-primo e P é maximal com relação a propriedade de ser R-disjunto.*

Demonstração. Suponhamos que R é um anel ρ-primo e P é maximal com relação a propriedade de ser R-disjunto. Sejam J e K ideais de $R < x; \rho >$ tais que $JK \subseteq P$, $J \nsubseteq P$ e $K \nsubseteq P$. Deste modo $P \subsetneqq (J+P)$ e $P \subsetneqq (K+P)$ e com isto, $(J+P) \cap R \neq 0$ e $(K+P) \cap R \neq 0$.

Como R é um anel ρ-primo, $(J+P) \cap R$ e $(K+P) \cap R$ são ideais ρ-invariantes não-nulos de R, então

$$[(J+P) \cap R][(K+P) \cap R] \neq 0.$$

Desta forma, $0 \neq [(J+P) \cap R][(K+P) \cap R] \subseteq P \cap R$ e isto contradiz o fato de P ser R-disjunto. Logo, P é primo.

Reciprocamente, suponhamos que P seja um ideal primo não-nulo R-disjunto de $R < x; \rho >$ e consideremos J e K ideais ρ-invariantes de R tais que $JK = 0$. Assim, pelo Lema 2.1.2,

$$0 = JK < x; \rho >= J < x; \rho > K < x; \rho > \subseteq P.$$

Desde que P é primo, então $J \subseteq J < x; \rho > \subseteq P$ ou $K \subseteq K < x; \rho > \subseteq P$. Logo, $J \subseteq (P \cap R) = 0$ ou $K \subseteq (P \cap R) = 0$ e segue que, R é um anel ρ-primo.

Provaremos que P é fechado. De fato, seja $f \in P$ um polinômio de grau mínimo em P com $a = lc(f)$. Pela Proposição 2.1.11, $f \in \Gamma$ e $[P] = [f]$.

Seja $g \in [P]$. Então, existe um ideal ρ-invariante não-nulo H de R tal que $aH\rho^s(g) \subseteq fR < x; \rho > \subseteq P$, para todo $s \in \mathbb{Z}$.

Por sua vez,

$$aHRx^jg = aHR\rho^j(g)x^j \subseteq Px^j \subseteq P$$

e concluímos que $aHR < x; \rho > g \subseteq P$. Como P é primo, então $aH \subseteq P$ ou $g \in P$. Se $aH \subseteq P$, então $aH \subseteq P \cap R = 0$. Logo, pelo Lema 1.1.2, $a = 0$, o que contradiz o fato que $a \neq 0$. Assim, $g \in P$ e com isto, $[P] \subseteq P$. Desta maneira, $P = [P]$.

Seja I um ideal R-disjunto de $R < x; \rho >$ tal que $P \subseteq I$. Consideremos $f \in I$ um polinômio não-nulo de grau mínimo n em I tal que $lc(f) = a$ e $g \in P$ um polinômio não-nulo de grau mínimo m em P tal que $lc(g) = b$. Suponhamos que $m > n$. Para cada $g \in P \cap R_m \subseteq I \cap R_m$ temos, pelo Lema 2.1.15, que existe $h \in R_{m-n}$ tal que

$$ha_0\rho^{i_0}(f) = g \prod_{j=0}^{m-n} \rho^{-n}(a_{m-n-j}\rho^{i_{m-n-j}}(a))$$

para todo $a_0 \in R$ e $i_0 \in \mathbb{Z}$. Deste modo,

$$ha_0\rho^{i_0}(f) = g\rho^{-n}(a_{m-n}\rho^{i_{m-n}}(a) \cdots a_1\rho^{i_1}(a)a_0\rho^{i_0}(a)).$$

Como para todo $j \in \{0, 1, \cdots, m-n\}$, $a_j\rho^{i_j}(a) \in \tau(I)$ então, $\rho^{-n}(a_j\rho^{i_j}(a)) \in \tau(I)$ e, conseqüentemente, $ha_0\rho^{i_0}(f) = g \prod_{j=0}^{m-n} \rho^{-n}(a_{m-n-j}\rho^{i_{m-n-j}}(a)) \in g\tau(I) \subseteq gR \subseteq P$, para todo $a_0 \in R$ e $i_0 \in \mathbb{Z}$. Assim, $hR\rho^{i_0}(f) \subseteq P$, para todo $i_0 \in \mathbb{Z}$.

Para cada $rx^k \in R < x; \rho >$, temos que $hrx^kf = hr\rho^k(f)x^k \in P$ e com isto, $hR < x; \rho > f \subseteq P$. Desde que P é um ideal primo então $f \in P$ ou $h \in P$ e, segue que, $f = 0$ ou $h = 0$, o que contradiz o fato que h e f são não-nulos. Deste modo, $m = n$.

Sejam $f \in I$ e $g \in P$ tais que $\delta(f) = n + 1$ e $\delta(g) = n$. Definimos $l = axr\rho^i(g) - f\rho^{-n}(r\rho^i(b))$, para todo $i \in \mathbb{Z}$ e $r \in R$. Claramente $l \in I \cap R_n = P \cap R_n$ e com isto $fR\rho^{i-n}(b) \subseteq P$.

De maneira análoga ao feito anteriormente, obtemos que $fR < x; \rho > \rho^{i-n}(b) \subseteq P$, para todo $i \in \mathbb{Z}$. Em particular, para $i = n$, temos que $fR < x; \rho > b \subseteq P$ e com isto, $f \in P$. Assim, $I \cap R_{n+1} = P \cap R_{n+1}$.

Suponhamos, por hipótese de indução, que $I \cap R_\kappa = P \cap R_\kappa$, para todo $\kappa < t$. Sejam $f \in I$ e $g \in P$ tais que $\delta(f) = t$ e $\delta(g) = n$. Consideremos $l = ax^{t-n}r\rho^i(g) - f\rho^{-n}(r\rho^i(b))$, para todo $i \in \mathbb{Z}$ e $r \in R$.

Claramente $l \in I \cap R_{t-1}$ e, pela hipótese de indução, $l \in P \cap R_{t-1}$. Usando métodos similares ao desenvolvido anteriormente, obtemos $I \cap R_t = P \cap R_t$, para todo $t \geq 0$. Logo, $f \in P \cap R_t$, para todo $t \geq 0$ e portanto, $I \subseteq P$. $\square$

Definição 2.1.17. *Seja f um polinômio próprio em Γ. Dizemos que f é irredutível em Γ se, dados $g \in \Gamma$ e $h \in R < x; \rho >$ tais que $f = hg$, então $\delta(f) = \delta(g)$. De maneira análoga se define a irredutibilidade de um polinômio próprio $f \in \Gamma_{Q_\rho(R)}$ em $\Gamma_{Q_\rho(R)}$.*

Estamos em condições de provar o principal resultado desta seção.

Teorema 2.1.18. *Sejam R um anel ρ-primo e P um ideal R-disjunto não-nulo de $R < x; \rho >$. Então, as seguintes condições são equivalentes:*

i) P é primo.

ii) P é fechado e cada $f \in P$ com $\delta(f) = Min(P)$ é irredutível em Γ.

iii) $P = Q_\rho(R) < x; \rho > f_0 \cap R < x; \rho >$, onde f_0 é um polinômio mônico próprio em $\Gamma_{Q_\rho(R)}$ que é irredutível em $\Gamma_{Q_\rho(R)}$.

Demonstração. $(i) \Rightarrow (ii)$ Seja $f \in P$ um polinômio de grau mínimo em P.

Pela Proposição 2.1.11 e Lema 2.1.8, $f \in \Gamma$ e $[P] = [f]$ é um ideal R-disjunto de $R < x; \rho >$. Pelo Corolário 2.1.5, $P \subseteq [P]$ e, por sua vez, segue do Lema 2.1.16 que P é fechado.

Suponhamos que existam $g \in \Gamma$ e $h \in R < x; \rho >$ tais que $f = hg \in R < x; \rho > g$. Pelo Lema 2.1.8, $[g]$ é um ideal R-disjunto de $R < x; \rho >$ que contém g como polinômio próprio de grau mínimo e com isto $f = hg \in [g]$. Assim $[f] = P \subseteq [g]$ e, novamente pelo Lema 2.1.16, $P = [g]$. Deste modo, $\delta(f) = Min(P) = Min([g]) = \delta(g)$ e segue que, f é irredutível em Γ.

$(ii) \Rightarrow (iii)$ Sejam P um ideal fechado não-nulo R-disjunto de $R < x;\rho >$ e f_P o polinômio canônico de P. Então, $P = [P] = Q_\rho(R) < x;\rho > f_P \cap R < x;\rho >$ onde, pela Observação 2.1.7, $f_P \in \Gamma^0_{Q_\rho(R)}$. Consideremos $g \in \Gamma_{Q_\rho(R)}$ com $\delta(g) = s$ e $h \in Q_\rho(R) < x;\rho >$ tais que $f_P = hg$.

Pelo Lema 2.1.8, $[g]$ é um ideal $Q_\rho(R)$-disjunto de $Q_\rho(R) < x;\rho >$ que contém g como polinômio próprio de grau mínimo. Seja $f_{[g]}$ o polinômio canônico de $[g]$.

Usando o Lema 1.1.2, existe um ideal ρ-invariante não-nulo J de R tal que $Jf_{[g]} \subseteq R < x;\rho >$. Como $f_P \in [g] = Q_\rho(R) < x;\rho > f_{[g]}$ então, existe $h' \in Q_\rho(R) < x;\rho >$ tal que $f_P = h'f_{[g]}$. Usando novamente o Lema 1.1.2, existe um ideal ρ-invariante não-nulo K de R tal que $Kh' \subseteq R < x;\rho >$.

Seja $L = K \cap J \cap \tau(P)$ e consideremos $f \in P$ um polinômio com grau mínimo em P, $lc(f) = a$ e $b_1, b_2 \in L$ tais que $a = b_2\rho^n(b_1) \neq 0$. Com isto,

$$f = af_P = (b_2\rho^n(b_1))f_P = b_2 f_P b_1 = b_2(h'f_{[g]})b_1 = (b_2h')(\rho^s(b_1)f_{[g]}).$$

Desde que $\delta(\rho^s(b_1)f_{[g]}) = \delta(g)$, então $\rho^s(b_1)f_{[g]} \in \Gamma_{Q_\rho(R)}$ e como $Jf_{[g]} \subseteq R < x;\rho >$, temos $\rho^s(b_1)f_{[g]} \in \Gamma_R$. Por hipótese, $\delta(f) = \delta(af_P) = \delta(f_P) = \delta(\rho^s(b_1)f_{[g]}) = \delta(f_{[g]}) = \delta(g)$. Logo, f_P é irredutível em $\Gamma_{Q_\rho(R)}$.

$(iii) \Rightarrow (i)$ Suponhamos que $P = Q_\rho(R) < x;\rho > f_0 \cap R < x;\rho >$, onde $f_0 \in \Gamma^0_{Q_\rho(R)}$ é um polinômio próprio irredutível em $\Gamma_{Q_\rho(R)}$ e seja L um ideal R-disjunto de $R < x;\rho >$ tal que $P \subseteq L$. Podemos assumir que L é fechado, isto é, $L = [L] = Q_\rho(R) < x;\rho > h_L \cap R < x;\rho >$, onde h_L é o polinômio canônico de L. Pela observação 2.1.7, $h_L \in \Gamma^0_{Q_\rho(R)}$.

Pelo algoritmo da divisão, existem $g, r \in Q_\rho(R)[x;\rho]$ tais que $f_0 = gh_L + r$, onde $r = 0$ ou $\delta(r) < \delta(h_L)$. Analogamente a prova do Corolário 2.1.5, segue que $r = 0$ e, com isto, $f_0 = gh_L$.

Por hipótese, f_0 é irredutível em $\Gamma_{Q_\rho(R)}$ e desta maneira, $\delta(f_0) = \delta(h_L)$. Assim, $\delta(g) = 0$ e, desde que f_0 e h_L são mônicos, temos que $g = 1$. Deste modo,

$$P = Q_\rho(R) < x; \rho > f_0 \cap R < x; \rho >= Q_\rho(R) < x; \rho > h_L \cap R < x; \rho >= L$$

e, pelo Lema 2.1.16, P é primo. □

Seja I um ideal não-nulo R-disjunto de $R < x; \rho >$ tal que $Min(I) = n$. Pelo Lema 2.1.4, existe um único polinômio mônico próprio $f_I \in Q_\rho(R) < x; \rho >$ tal que, para todo $f \in I$ com $\delta(f) = Min(I)$, $f = lc(f) f_I$ e $f_I x^{-n} \in Z$.

Sejam $Z(Q_\rho(R))$ o centro de $Q_\rho(R)$, Z o centro de $Q_\rho(R) < x; \rho >$ e

$$C_\rho(R) = \{a \in Z(Q_\rho(R)); \rho(a) = a\}.$$

Consideremos $k \in C_\rho(R)$. Assim, $\rho(k) = k$ e $kc = ck$, para todo $c \in Q_\rho(R)$ e com isto, para todo $j \in \mathbb{Z}$, $x^j k = \rho^j(k) x^j = k x^j$. Conseqüentemente, $k \in Z$ e deste modo, $C_\rho(R) \subseteq Z$.

Note que $f_I x^{-n} \in Z$ e no entanto, $f_I x^{-n} \in C_\rho(R)$ se, e somente se, $f_I = x^n$, o que contradiz o fato de que f_I é próprio. Assim, $C_\rho(R) \neq Z$ e segue do Lema 1.2.4 que ρ^k é um automorfismo interno de $Q_\rho(R)$ para algum $k \geq 1$. Com isto, novamente pelo Lema 1.2.4, $Z = C_\rho(R) < bx^m >$, onde m é o menor número natural não-nulo tal que ρ^m é um automorfismo interno de $Q_\rho(R)$ determinado por um elemento não-nulo ρ-invariante $b \in Q_\rho(R)$.

Corolário 2.1.19. *Seja P um ideal não-nulo R-disjunto de $R < x; \rho >$. Então, as seguintes condições são equivalentes:*

i) P é primo.

ii) $P = Q_\rho(R) < x; \rho > g_0 \cap R < x; \rho >$, para algum polinômio mônico próprio $g_0 \in C_\rho(R)[z]$ irredutível em $C_\rho(R)[z]$ e distinto de z.

Demonstração. $(i) \Rightarrow (ii)$ Seja f_P o polinômio canônico de P tal que $\delta(f_P) = n$. Pelo Teorema 2.1.18 temos que P é fechado e com isto,

$$P = Q_\rho(R) < x; \rho > f_P \cap R < x; \rho >.$$

Além disto, pelo Lema 2.1.4, $f_P x^{-n} \in Z$. Por sua vez, da Observação 2.1.7 e do Teorema 2.1.18, temos que $f_P \in \Gamma^0_{Q_\rho(R)}$ é irredutível em $\Gamma_{Q_\rho(R)}$.

Como $Z = C_\rho(R) < bx^m >$, onde m é o menor número natural não-nulo tal que ρ^m é um automorfismo interno de $Q_\rho(R)$ determinado por um elemento não-nulo ρ-invariante $b \in Q_\rho(R)$ então, $f_P x^{-n} \in C_\rho(R) < bx^m >$ e com isto, $n = ms$, para algum $s \geq 1$.

Para cada $y \in Q_\rho(R)$, $\rho^{ms}(y) = b^{-s} y b^s$, onde $\rho^m(y) = b^{-1} y b$. Assim,

$$y(b^s f_P) = (yb^s) f_P = (b^s \rho^{ms}(y)) f_P = b^s(\rho^{ms}(y) f_P) = b^s(f_P y) = (b^s f_P) y$$

e como

$$x(b^s f_P) = b^s x f_P = (b^s f_P) x$$

temos que $b^s f_P \in Z(Q_\rho(R)[x; \rho]) = C_\rho(R)[bx^m]$.

Seja $h \in C_\rho(R)[bx^m]$ tal que $lc(h) = c_t b^t$. Como, $\rho^{mt}(q) = b^{-t} q b^t$ então, $qb^t = b^t \rho^{mt}(q)$ e segue para cada $q \in Q_\rho(R)$ e $j \in \mathbb{Z}$

$$\rho^j(h) q(c_t b^t) = hc_t(qb^t) = hc_t b^t \rho^{mt}(q).$$

Desde que $h \in Z$, então,

$$\rho^j(h) q(c_t b^t) = c_t b^t \rho^{mt}(q) h = \rho^j(c_t b^t) \rho^{mt}(qh).$$

Assim, h satisfaz a condição 2.3, ou seja, $h \in \Gamma_{Q_\rho(R)}$.

Suponhamos que $b^s f_P = hl$, onde $h, l \in C_\rho(R)[bx^m]$. Deste modo, $f_P = (b^{-s} h) l$, onde, pelo que acabamos de deduzir, $h, l \in \Gamma_{Q_\rho(R)}$. Pela irredutibilidade de $f_P \in \Gamma^0_{Q_\rho(R)}$ em $\Gamma_{Q_\rho(R)}$ segue que $\delta(f_P) = \delta(l)$. Logo, $h \in C_\rho(R)$ e com isto, $b^s f_P$ é irredutível em $C_\rho(R)[z]$ e distinto de z. Por sua vez,

$$P = Q_\rho(R) < x;\rho > f_P \cap R < x,\rho >= Q_\rho(R) < x;\rho > b^s f_P \cap R < x,\rho >.$$

$(ii) \Rightarrow (i)$ Suponhamos que $P = Q_\rho(R) < x;\rho > g_0 \cap R < x;\rho >$ para algum polinômio mônico próprio $g_0 \in C_\rho(R)[z]$ irredutível em $C_\rho(R)[z]$ e distinto de $z = bx^m$. Em $(i) \Rightarrow (ii)$ foi mostrado que todo elemento de $C_\rho(R)[z]$ satisfaz 2.3 e com isto, é fácil ver que $g_0 \in \Gamma^0_{Q_\rho(R)}$.

Seja L um ideal primo de $R < x;\rho >$ tal que $P \subseteq L$. Pelo Teorema 2.1.18 temos que $L = Q_\rho(R) < x;\rho > f_0 \cap R < x;\rho >$, onde f_0 é o polinômio canônico de L irredutível em $\Gamma_{Q_\rho(R)}$. Não é difícil de mostrar que $g_0 = hf_0$ para algum $h \in Q_\rho(R) < x;\rho >$. Suponhamos que $\delta(h) \geq 1$. Desde que g_0 é central, então $chf_0 = h\rho^{\delta(f_0)}(c)f_0$, para todo $c \in Q_\rho(R)$ e, $xhf_0 = hxf_0$ e segue que $ch = h\rho^{\delta(f_0)}(c)$ e $xh = hx$. É evidente que $hx^{\delta(f_0)} \in C_\rho(R) < z >$. Assim, $g_0 = hx^{\delta(f_0)}x^{-\delta(f_0)}f_0$, com $hx^{\delta(f_0)}, x^{-\delta(f_0)}f_0 \in C_\rho(R) < z >$. Como g_0 é irredutível em $C_\rho(R) < z >$, então $hx^{\delta(f_0)}$ é invertível ou $x^{-\delta(f_0)}f_0$ é invertível, o que contradiz o fato que $\delta(h) \geq 1$ e $\delta(f_0) \geq 1$. Logo, $\delta(h) = 0$ e, pelo Lema 1.1.4, h é invertível em $Q_\rho(R)$. Portanto,

$$\begin{aligned} P = Q_\rho(R) < x;\rho > g_0 \cap R < x;\rho > &= Q_\rho(R) < x;\rho > hf_0 \cap R < x;\rho > \\ &= Q_\rho(R) < x;\rho > f_0 \cap R < x;\rho >= L \end{aligned}$$

e com isto, P é um ideal primo. □

Corolário 2.1.20. *Existe a correspondência biunívoca entre:*

(i) O conjunto de todos os ideais primos R-disjuntos de $R < x;\rho >$.

(ii) O conjunto de todos os ideais primos $Q_\rho(R)$-disjuntos de $Q_\rho(R) < x;\rho >$.

(iii) O conjunto de todos os ideais maximais de Z.

Além disto, esta correspondência associa o ideal primo R-disjunto P de $R < x;\rho >$ ao ideal primo $Q_\rho(R)$-disjunto P^* de $Q_\rho(R) < x;\rho >$ e ao ideal maximal M de Z se $P^* \cap R < x;\rho >= P$ e $MQ_\rho(R) < x;\rho >= P^*$.

Demonstração. Suponhamos que não existe ideal R-disjunto não-nulo de $R < x; \rho >$. Conseqüentemente, não existe ideal $Q_\rho(R)$-disjunto não-nulo de $Q_\rho(R) < x; \rho >$, ρ^k não é um automorfismo interno para todo $k \geq 1$ e com isto, $C_\rho(R) = Z$.

Suponhamos agora que $R < x; \rho >$ possua ideais não-nulos R-disjuntos e sejam os conjuntos:

$$X = \{M : M \text{ é ideal maximal de } Z\},$$
$$Y = \{P : P \text{ é ideal primo } R\text{-disjunto de } R < x; \rho >\} \text{ e}$$
$$W = \{P^* : P^* \text{ é ideal primo } Q_\rho(R)\text{-disjunto de } Q_\rho(R) < x; \rho >\}.$$

Seja $M \in X$. Então existe um polinômio irredutível $f \in C_\rho(R)[z]$ tal que $M = fC_\rho(R)[z]$. Consideremos $K = Q_\rho(R) < x; \rho > f \cap R < x; \rho >$ que, pelo Corolário 2.1.19, é um ideal primo R-disjunto de $R < x; \rho >$. Assim $K \in Y$ e podemos definir a aplicação $\gamma_1 : X \to Y$ por

$$\gamma_1(M) = \gamma_1(fC_\rho(R)[z]) = Q_\rho(R) < x; \rho > f \cap R < x; \rho >= K.$$

Seja $N \in Y$. Então, pelo Corolário 2.1.19, $N = Q_\rho(R) < x; \rho > f_0 \cap R < x; \rho >$ para algum polinômio próprio $f_0 \in C_\rho(R)[z]$ distinto de z e irredutível em $C_\rho(R)[z]$. Considere M' o ideal gerado por f_0. Claramente $M' \in X$ e por sua vez, podemos definir $\gamma_2 : Y \to X$ por

$$\gamma_2(N) = \gamma_2(Q_\rho(R) < x; \rho > f_0 \cap R < x; \rho >) = C_\rho(R)[z]f_0 = M'.$$

É fácil ver que $\gamma_1 \circ \gamma_2 = id|_Y$ e $\gamma_2 \circ \gamma_1 = id|_X$.

Consideremos $P \in Y$. Então, pelo Teorema 2.1.18,

$$P = Q_\rho(R) < x; \rho > f_P \cap R < x; \rho >,$$

onde f_P é o polinômio canônico de P. Seja $J = Q_\rho(R) < x; \rho > f_P$. Claramente J é maximal com relação a propriedade de ser $Q_\rho(R)$-disjunto e segue do Lema 2.1.16 que J é primo. Logo $J \in W$. Definimos $\varphi_1 : Y \to W$ por

$$\varphi_1(P) = \varphi_1(Q_\rho(R) < x; \rho > f_P \cap R < x; \rho >) = Q_\rho(R) < x; \rho > f_P = J.$$

Seja $L \in W$. Então, L é um ideal primo $Q_\rho(R)$-disjunto de $Q_\rho(R) < x;\rho >$ e, pelo Teorema 2.1.18, L é fechado e cada $f \in L$ com $\delta(f) = Min(L)$ é irredutível em $\Gamma_{Q_\rho(R)}$. Pelo Lema 2.1.14, temos que $L = Q_\rho(R) < x;\rho > f_0$, para algum polinômio próprio $f_0 \in \Gamma^0_{Q_\rho(R)}$. Consideremos $P' = L \cap R < x;\rho >$ um ideal não-nulo R-disjunto de $R < x;\rho >$ que, pelo Teorema 2.1.18, é primo. Definimos $\varphi_2 : W \to Y$ por

$$\varphi_2(L) = L \cap R < x;\rho >= P'.$$

Claramente, $\varphi_1 \circ \varphi_2 = id|_W$ e $\varphi_2 \circ \varphi_1 = id|_Y$ e isto completa a prova. □

Como caso particular do Corolário 2.1.20, temos o seguinte resultado

Corolário 2.1.21. *Existe uma correspondência biunívoca entre os conjuntos:*

$$X = \{P\text{: } P \text{ é um ideal primo } R\text{-disjunto de } R < x;\rho >\} \text{ e}$$
$$Y = \{T\text{: } T \text{ é um ideal primo de } C_\rho(R)[z] \text{ e distinto de } zC_\rho(R)[z]\}$$

Demonstração. Claramente, todo elemento de Y é um ideal maximal em $C_\rho(R)[z]$.

Seja $T \in X$. Pelo Corolário 2.1.19, $T = Q_\rho(R) < x;\rho > g_0 \cap R < x;\rho >$ para algum polinômio mônico próprio $g_0 \in C_\rho(R)[z]$ irredutível em $C_\rho(R)[z]$ e distinto de z. Por sua vez, $zC_\rho(R)[z]$ não contém g_0, pois g_0 é um polinômio próprio. Consideremos $P = g_0C_\rho(R)[z]$ e definimos $\gamma_1 : X \to Y$ por

$$\gamma_1(T) = \gamma_1(Q_\rho(R) < x;\rho > g_0 \cap R < x;\rho >) = g_0C_\rho(R)[z] = P.$$

Seja $P' \in Y$ e com isto, P' é gerado por um polinômio irredutível $f_0 \in C_\rho(R)[z]$ e distinto de $zC_\rho(R)[z]$. Pelo Corolário 2.1.19, $T = Q_\rho(R) < x,\rho > f_0 \cap R < x,\rho >$ é um ideal primo R-disjunto de $R < x;\rho >$. Definimos $\gamma_2 : Y \to X$ por

$$\gamma_2(P') = \gamma_2(f_0C_\rho(R)[z]) = Q_\rho(R) < x;\rho > f_0 \cap R < x;\rho >= T.$$

É fácil ver que $\gamma_1 \circ \gamma_2 = id|_Y$ e $\gamma_2 \circ \gamma_1 = id|_X$. □

Corolário 2.1.22. *Existe uma correspondência biunívoca entre os conjuntos*

$$K = \{L\text{: } L \text{ é ideal de } Z\},$$
$$X = \{P\text{: } P \text{ é ideal fechado } R\text{-disjunto de } R < x; \rho >\} \text{ e}$$
$$Y = \{P^*\text{: } P^* \text{ é ideal fechado } Q_\rho(R)\text{-disjunto de } Q_\rho(R) < x; \rho >\}.$$

Demonstração. Se não existirem ideais não-nulos R-disjuntos de $R < x; \rho >$, a prova segue análoga a primeira parte da prova do Corolário 2.1.20.

Seja $M \in X$. Então $M = [M] = Q_\rho(R) < x; \rho > f_M \cap R < x; \rho >$, onde f_M é o polinômio canônico de M. Pela Observação 2.1.7, temos que $f_M \in \Gamma^0_{Q_\rho(R)}$ e, pelo Lema 2.1.14, $T = Q_\rho(R) < x; \rho > f_M \in Y$. Definimos $\gamma_1 : X \to Y$ por

$$\gamma_1(M) = \gamma_1(Q_\rho(R) < x; \rho > f_M \cap R < x; \rho >) = Q_\rho(R) < x; \rho > f_M = T.$$

Consideremos $L \in Y$. Então, pelo Lema 2.1.14, $L = Q_\rho(R) < x; \rho > f_L$, para algum polinômio próprio $f_L \in \Gamma^0_{Q_\rho(R)}$. Claramente, $M = L \cap R < x; \rho >$ é um ideal R-disjunto de $R < x; \rho >$. Seja f_M o polinômio canônico de M. Assim, para cada $f \in M$ tal que $\delta(f) = Min(M)$, temos que $f = lc(f) f_M$.

Suponhamos que $f \in L$. Então, existe $g \in Q_\rho(R) < x; \rho >$ tal que $f = g f_L$. Pelo Lema 2.1.10, $Min(M) = Min(L)$ e deste modo, $\delta(f) = \delta(f_L)$. Assim, $f = lc(f) f_L$ e com isto, $0 = lc(f)[f_M - f_L]$. Conseqüentemente, $0 = \tau(M)[f_M - f_L]$ e, pelo Lema 1.1.2, $f_M = f_L$. Logo M é fechado. Definimos $\gamma_2 : Y \to X$ por

$$\gamma_2(L) = \gamma_2(Q_\rho(R) < x; \rho > f_L) = Q_\rho(R) < x; \rho > f_M \cap R < x; \rho >= M.$$

Claramente, $\gamma_1 \circ \gamma_2 = id|_Y$ e $\gamma_2 \circ \gamma_1 = id|_X$.

Seja $M \in X$. Então, $M = [M] = Q_\rho(R) < x; \rho > f_M \cap R < x; \rho >$, onde f_M é o polinômio canônico de M. Consideremos $L = Z(f_M x^{-\delta(f_M)})$ e definimos $\alpha_1 : X \to K$ por

$$\alpha_1(M) = \alpha_1(Q_\rho(R) < x; \rho > f_M \cap R < x; \rho >) = Z(f_M x^{-\delta(f_M)}) = L.$$

Para cada $L \in K$ existe $f_0 \in L$ um polinômio próprio de grau mínimo em L tal que $L = Zf_0$. Suponhamos que $\delta(f_0) = s$ e $lc(f_0) = c$. Claramente, $f_0' = c^{-1}f_0$ é um polinômio mônico e próprio em $Q_\rho(R) < x, \rho >$. Consideremos

$$M = Q_\rho(R) < x; \rho > f_0' \cap R < x; \rho >$$

e seja $f \in M$ tal que $\delta(f) = Min(M)$ e $lc(f) = a$. Deste modo, $f = af_M$. Além disto, podemos escrever $f = gf_0'$, para algum $g \in Q_\rho(R) < x; \rho >$. Pelo Lema 2.1.10, temos que $\delta(f_0') = Min(M) = \delta(f)$ e com isto, $\delta(g) = 0$. Como f_0' é mônico, então $g = lc(a)$. Logo, $f = af_0'$ e segue que,

$$0 = af_M - af_0' = a(f_M - f_0').$$

Conseqüentemente, $\tau(M)(f_M - f_0') = 0$ e, pelo Lema 1.1.2, $f_M = f_0'$. Assim, $M = [M]$. Definimos $\alpha_2 : K \to X$ por

$$\alpha_2(L) = \alpha_2(Zf_0) = Q_\rho(R) < x; \rho > f_M \cap R < x; \rho >= M.$$

É fácil ver que $\alpha_1 \circ \alpha_2 = id|_K$ e $\alpha_2 \circ \alpha_1 = id|_X$. $\square$

2.2 Ideais Fortemente ρ-Primos em Skew Anel de Polinômios do Tipo Automorfismo

Baseados nos resultados da seção anterior, iremos estudar nesta seção os ideais fortemente ρ-primos R-disjuntos no skew anel de polinômios do tipo automorfismo $R[x; \rho]$, onde R é um anel fortemente ρ-primo.

Definição 2.2.1. *Sejam I um ideal de $R[x; \rho]$ e $f, g \in R[x; \rho]$. Dizemos que x é regular módulo I se $xf, gx \in I$, então $f, g \in I$.*

Lema 2.2.2. *Seja P um ideal primo de $R[x; \rho]$ que não contém x. Então x é regular módulo P.*

Demonstração. Seja $f \in R[x;\rho]$ tal que $xf \in P$. Assim $R[x;\rho]xf \subseteq P$. Como $xR[x;\rho] = R[x;\rho]x$, temos que $xR[x;\rho]f = R[x;\rho]xf \subseteq P$. Desde que P é um ideal primo de $R[x;\rho]$ que não contém x, então $f \in P$. Analogamente se mostra o outro caso. $\square$

Lema 2.2.3. *Existe uma correspondência biunívoca via contração entre o conjunto de todos os ideais R-disjuntos de $R < x;\rho >$ e o conjunto de todos os ideais R-disjuntos I de $R[x;\rho]$ tais que x é regular módulo I.*

Demonstração. Seja I um ideal R-disjunto de $R < x;\rho >$. Então, $I_0 = I \cap R[x;\rho]$ é um ideal R-disjunto de $R[x;\rho]$ com a propriedade que x é regular módulo I_0 pois, para cada $f, g \in R[x;\rho]$ tais que $xf, gx \in I_0$, temos que $f \in x^{-1}I \subseteq I$ e $g \in Ix^{-1} \subseteq I$, o que implica que $f, g \in I \cap R[x;\rho] = I_0$.

Consideremos J um ideal R-disjunto de $R[x;\rho]$ tal que x é regular módulo J e seja $(J) = \sum_{i\geq 0} Jx^{-i}$. Mostraremos que (J) é um ideal de $R < x;\rho >$. Com efeito, claramente $0 \in (J)$. Sejam $f, g \in (J)$ e $rx^s \in R < x;\rho >$ tais que $f = \sum_{k=0}^{n} j_{i_k}x^{-i_k}$ e $g = \sum_{k=0}^{n} j'_{i_k}x^{-i_k}$, onde $j_{i_k}, j'_{i_k} \in J$. Então

$$f + g = \textstyle\sum_{k=0}^{n}(j_{i_k} + j'_{i_k})x^{-i_k} \in (J),$$
$$f(rx^s) = (\textstyle\sum_{k=0}^{n} j_{i_k}x^{-i_k})rx^s = \sum_{k=0}^{n} j_{i_k}\rho^{-i_k}(r)x^{-i_k+s} \in (J)$$
$$\text{e } (rx^s)f \in (J).$$

Sejam $f \in (J) \cap R[x;\rho]$ tal que $f = \sum_{k=0}^{n} j_{i_k}x^{-i_k}$, com $j_{i_k} \in J$ para todo $k \in \{0, 1, \cdots, n\}$ e $m = max\{i_1, \cdots, i_k\}$. Então, $fx^m = \sum_{k=0}^{n} j_{i_k}x^{-i_k+m} \in J$. Como x é regular módulo J, então $f \in J$. Deste modo, $(J) \cap R[x;\rho] \subseteq J$. A outra inclusão é imediata e com isto, $(J) \cap R[x;\rho] = J$.

Como $(J) \cap R \subseteq J \cap R = 0$, temos que (J) é um ideal R-disjunto de $R < x;\rho >$.

Sejam X o conjunto de todos os ideais R-disjuntos de $R < x;\rho >$ e Γ o conjunto de todos os ideais R-disjuntos I de $R[x;\rho]$ tais que x é regular módulo I. Definimos $f_1 : X \to \Gamma$ e $f_2 : \Gamma \to X$ por $f_1(I) = I \cap R[x;\rho]$ e $f_2(J) = (J)$, respectivamente.

Para cada $I \in X$, temos que

$$f_2 \circ f_1(I) = f_2(I \cap R[x;\rho]) = (I \cap R[x;\rho]).$$

Mostraremos que $(I \cap R[x;\rho]) = I$. De fato, seja $f = \sum_{k=0}^{n} t_{i_k} x^{-i_k}$, onde $t_{i_k} \in I \cap R[x;\rho]$ para todo $k \in \{0, 1, \cdots, n\}$. Como $t_{i_k} \in I$ para todo $k \in \{0, 1, \cdots, n\}$, então $f \in I$ e com isto, $(I \cap R[x;\rho]) \subseteq I$.

Por outro lado, seja $f \in I$. Então existe $t \in \mathbb{N}$ tal que $fx^t \in I \cap R[x;\rho]$. Assim, $f = (fx^t)x^{-t} \in (I \cap R[x;\rho])$. Logo, $I \subseteq (I \cap R[x;\rho])$ e segue que $(I \cap R[x;\rho]) = I$.

Deste modo, $f_2 \circ f_1 = Id|_X$. Claramente, $f_1 \circ f_2 = id|_\Gamma$. $\square$

Observação 2.2.4. *Sejam I um ρ-ideal e J um ideal de R. Então $J[x;\rho]I[x;\rho] = JI[x;\rho]$. Com efeito, para cada $ix^l \in J[x;\rho]$ e $ax^k \in I[x;\rho]$, temos que,*

$$i\rho^l(a)x^{l+k} = (ix^l)(ax^k) \in J[x;\rho]I[x;\rho].$$

Como $\rho(I) \subseteq I$, então $i\rho^l(a)x^{l+k} \in JI[x;\rho]$. Logo, $J[x;\rho]I[x;\rho] \subseteq JI[x;\rho]$.

Por outro lado, seja $iax^l \in JI[x;\rho]$. Então $iax^l = ix^0ax^l \in J[x;\rho]I[x;\rho]$ e deste modo, $JI[x;\rho] \subseteq J[x;\rho]I[x;\rho]$.

Lema 2.2.5. *Seja P um ideal primo de $R[x;\rho]$. Então $x \in P$ e $P = (P \cap R) + R[x;\rho]x$ ou x é regular módulo P e $P \cap R$ é um ideal fortemente ρ-primo de R.*

Demonstração. Seja P um ideal primo de $R[x;\rho]$ e suponhamos que $x \in P$. Assim, $R[x;\rho]x \subseteq P$ e segue que, $(P \cap R) + R[x;\rho]x \subseteq P$.

Por outro lado, seja $f \in P$ tal que $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Como $x \in P$, então $a_0 = f - (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x) \in P$. Por sua vez, $a_0 \in P \cap R$ e temos que $f = a_0 + a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \in (P \cap R) + R[x;\rho]x$. Deste modo, $P \subseteq (P \cap R) + R[x;\rho]x$ e com isto, $(P \cap R) + R[x;\rho]x = P$.

Suponhamos que P não contenha x. Pelo Lema 2.2.2, x é regular módulo P. Sejam I um ρ-ideal e J um ideal de R tais que $JI \subseteq P \cap R$. Pela Observação 2.2.4, $J[x;\rho]I[x;\rho] = JI[x;\rho]$ e, é fácil ver que, $J[x;\rho]I[x;\rho] \subseteq (P \cap R)[x;\rho] \subseteq P$. Logo,

$J \subseteq J[x;\rho] \subseteq P$ ou $I \subseteq I[x;\rho] \subseteq P$ e portanto, $P \cap R$ é um ideal fortemente ρ-primo de R. $\square$

Um ideal J de $R[x;\rho]$ é um *ρ-ideal* (*ideal ρ-invariante*) se $\rho(J) \subseteq J$ ($\rho(J) = J$). Além disto, um ideal ρ-invariante P de $R[x;\rho]$ é dito *fortemente ρ-primo* se para quaisquer ρ-ideal K de $R[x;\rho]$ e um ideal L de $R[x;\rho]$ tais que $KL \subseteq P$ tem-se que $K \subseteq P$ ou $L \subseteq P$.

A prova do seguinte lema é análoga à prova do Lema 2.2.5 e por isso iremos omitir.

Lema 2.2.6. *Seja P um ideal fortemente ρ-primo de $R[x;\rho]$. Então $x \in P$ e $P = P \cap R + R[x;\rho]x$ ou x é regular módulo P e $P \cap R$ é um ideal fortemente ρ-primo de R.*

Como os ideais fortemente ρ-primos de $R[x;\rho]$ que contém x são determinados pelos ideais fortemente ρ-primos de R, estaremos interessados nos ideais fortemente ρ-primos P que não contenham x. Fatorando $P \cap R$ podemos assumir que P é R-disjunto e R é fortemente ρ-primo.

A prova do próximo lema é análoga à prova do Lema 2.1.15.

Lema 2.2.7. *Sejam I um ideal não-nulo de $R[x;\rho]$ e $f \in I$ um polinômio não-nulo de grau mínimo n em I tal que $lc(f) = a$. Suponhamos que $m \geq n$ e que $g \in I \cap R_m$. Se $a_j \in R$ e i_j são inteiros não-negativos para todo $j \in \{1, 2, \cdots, m-n\}$, então existe $h \in R_{m-n}$ tal que*

$$ha_0\rho^{i_0}(f) = g \prod_{j=0}^{m-n} \rho^{-n}(a_{m-n-j}\rho^{i_{m-n-j}}(a)) \tag{2.8}$$

para todo $a_0 \in R$ e $i_0 \geq 0$.

Lema 2.2.8. *Seja P um ideal R-disjunto de $R[x;\rho]$ que não contém x. Se P é fortemente ρ-primo então P é maximal com relação à propriedade de ser R-disjunto no conjunto dos ideais ρ-invariantes R-disjuntos de $R[x;\rho]$.*

Demonstração. Para mostrar que $P \cap R_n = I \cap R_n$, procede-se como no Lema 2.1.16.

Sejam $f \in I$ e $g \in P$ tais que $\delta(f) = n+1$ e $\delta(g) = n$. Definimos $l = axr\rho^i(g) - f\rho^{-n}(r\rho^i(b))$, para todo $i \geq 0$ e $r \in R$. Claramente $l \in I \cap R_n = P \cap R_n$ e com isto $fR\rho^{i-n}(b) \subseteq P$.

Procedendo como no Lema 2.1.16, obtemos que $fR[x;\rho]\rho^{i-n}(b) \subseteq P$, para todo $i \geq 0$. Em particular, para $i = n$, temos que $fR[x;\rho]b \subseteq P$ e com isto, $f \in P$. Assim, $I \cap R_{n+1} = P \cap R_{n+1}$.

Suponhamos, por hipótese de indução, que $I \cap R_\kappa = P \cap R_\kappa$, para todo $\kappa < t$. Sejam $f \in I$ e $g \in P$ tais que $\delta(f) = t$ e $\delta(g) = n$. Consideremos $l = ax^{t-n}r\rho^i(g) - f\rho^{-n}(r\rho^i(b))$, para todo $i \geq 0$ e $r \in R$.

Claramente $l \in I \cap R_{t-1}$ e, pela hipótese de indução, $l \in P \cap R_{t-1}$. Usando métodos similares ao desenvolvido anteriormente, obtemos $I \cap R_t = P \cap R_t$, para todo $t \geq 0$. Logo, $f \in P \cap R_t$, para todo $t \geq 0$ e portanto, $I \subseteq P$. □

Lema 2.2.9. *Seja P um ideal R-disjunto de $R[x;\rho]$ que não contém x. Então P é fortemente ρ-primo se, e somente se, R é fortemente ρ-primo e P é maximal com relação a propriedade de ser R-disjunto no conjunto dos ideais ρ-invariantes R-disjuntos de $R[x;\rho]$.*

Demonstração. Sejam P um ideal fortemente ρ-primo R-disjunto de $R[x;\rho]$ que não contém x, I um ρ-ideal e J um ideal de R tais que $JI = 0$. Assim, pela Observação 2.2.4,

$$0 = JI[x;\rho] = J[x;\rho]I[x;\rho] \subseteq P$$

e, conseqüentemente $J \subseteq J[x;\rho] \subseteq P$ ou $I \subseteq I[x;\rho] \subseteq P$. Logo, $J \subseteq P \cap R = 0$ ou $I \subseteq P \cap R = 0$ e portanto R é um anel fortemente ρ-primo.

A maximalidade de P no conjunto dos ideais ρ-invariantes R-disjuntos de $R[x;\rho]$ é decorrência imediata do Lema 2.2.8.

Reciprocamente, sejam R um anel fortemente ρ-primo e P um ideal de $R[x;\rho]$ maximal com relação a propriedade de ser R-disjunto no conjunto dos ideais ρ-invariantes R-disjuntos de $R[x;\rho]$.

Sejam U um ideal de $R[x;\rho]$ e V um ρ-ideal de $R[x;\rho]$ tais que $UV \subseteq P$. Suponhamos que $U \nsubseteq P$ e $V \nsubseteq P$. Claramente $P+V$ é um ρ-ideal de $R[x;\rho]$. Desde que R é um anel fortemente ρ-primo, então $[(P+V)\cap R][(P+U)\cap R] \neq 0$, o que contradiz o fato que $[(P+V)\cap R][(P+U)\cap R] \subseteq P\cap R = (0)$. Logo, $U \subseteq P$ ou $V \subseteq P$ e portanto, P é um ideal fortemente ρ-primo de $R[x;\rho]$. $\square$

Os resultados apresentados a seguir são conseqüência dos estudos realizados até este momento.

Corolário 2.2.10. *Seja R um anel fortemente ρ-primo. Então existe uma correspondência biunívoca via contração entre os conjuntos*

$$X = \{P^*\colon\ P^* \text{ é ideal primo } R\text{-disjunto de } R<x;\rho>\} \text{ e}$$
$$Y = \{P\colon\ P \text{ é ideal fortemente } \rho\text{-primo } R\text{-disjunto de } R[x;\rho] \text{ que não contém } x\}.$$

Demonstração. Seja $P^* \in X$. Então, $P = P^* \cap R[x;\rho]$ é um ideal R-disjunto de $R[x;\rho]$. Suponhamos que $P = (0)$ e sejam $f, g \in R[x;\rho]$ tais que $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ e $fR[x;\rho]g = 0$. Em particular, para todo $rx^j \in R[x;\rho]$, temos que $f(rx^j)g = 0$ e com isto, $lc(f(rx^j)g) = a_n\rho^n(r)\rho^{n+j}(b_m) = 0$. Assim, $a_nR\rho^{n+j}(b_m) = 0$, para todo $j \geq 0$.

Por sua vez, $I = \sum_{j\geq 0} R\rho^{n+j}(b_m)R$ é um ρ-ideal de R e, pela igualdade anterior, $a_nI = 0$. Deste modo, $Ra_nRI = 0$. Como R é fortemente ρ-primo, temos que $Ra_nR = 0$ ou $I = 0$ e com isto, $a_n = 0$ ou $b_m = 0$.

Se $b_m = 0$, então repetindo o mesmo raciocínio anterior obtemos que $b_{m-1} = 0$. Aplicando este método um número suficiente de vezes, concluímos que $g = 0$. Se $b_m \neq 0$ então $a_n = 0$ e, de modo análogo, mostramos que $f = 0$. Logo, $P = (0)$ é um ideal primo de $R[x;\rho]$.

Suponhamos que $P \neq (0)$ e seja L um ideal fortemente ρ-primo R-disjunto de $R[x;\rho]$ tal que $P \subseteq L$. Se $x \in L$ então, pelo Lema 2.2.5, $L = R[x;\rho]x$. Assim, para cada $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in P$, obtemos $a_0 = f - (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x) \in L$ e, sendo L um ideal R-disjunto, temos que $a_0 = 0$. Desta maneira, $f_1 = a_n x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 \in P$. Repetindo o mesmo raciocínio acima um número suficiente de vezes, obtemos que $f = 0$. Logo, $P = (0)$ e isso contradiz o fato de que $P \neq (0)$. Deste modo, L não contém x e, usando um raciocínio análogo ao Lema 2.2.5, x é regular módulo L e $L \cap R$ é um ideal fortemente ρ-primo de R. Pelo Lema 2.2.3, x é regular módulo P e $(P) = (P^* \cap R[x;\rho]) = P^*$.

Seja $f \in P^*$. Então existe $n \in \mathbb{N}$ tal que $fx^n \in P^* \cap R[x;\rho] = P \subseteq L$. Claramente $f = (fx^n)x^{-n} \in (L)$ e com isto, $P^* \subseteq (L)$. Pelo Lema 2.1.16, P^* é maximal no conjunto dos ideais R-disjuntos de $R < x;\rho >$ e assim, $P^* = (L)$. Deste modo, $(P) = (L)$ e conseqüentemente, $P = L$. Definimos $\gamma_1 : X \rightarrow Y$ por $\gamma_1(P^*) = P$.

Pelo Lema 2.2.9, cada $P \in Y$ é maximal no conjunto dos ideais ρ-invariantes R-disjuntos de $R[x;\rho]$. Consideremos $P^* = (P)$ e seja L um ideal R-disjunto de $R < x;\rho >$ tal que $P^* \subseteq L$. Então, $P \subseteq L \cap R[x;\rho]$ e, pela maximalidade de P, temos que $P = L \cap R[x;\rho]$. Assim, $P^* = L$ e segue do Lema 2.1.16, que P^* é um ideal primo de $R < x;\rho >$. Logo, $P^* \in X$ e com isto, podemos definir $\gamma_2 : Y \rightarrow X$ por $\gamma_2(P) = P^*$.

Claramente $\gamma_1 \circ \gamma_2 = Id|_Y$ e $\gamma_2 \circ \gamma_1 = Id|_X$. A prova está completa. $\square$

Corolário 2.2.11. *Sejam R um anel fortemente ρ-primo e P um ideal não-nulo R-disjunto de $R[x;\rho]$. Então, P é fortemente ρ-primo se, e somente se, uma das seguintes condições for satisfeita:*

i) R é fortemente ρ-primo e $P = xR[x;\rho]$.

ii) $P = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$, onde f_0 é um polinômio mônico irredutível em $C_\rho(R)[z]$ distinto de z.

Demonstração. Seja P um ideal fortemente ρ-primo não-nulo R-disjunto de $R[x;\rho]$. Pelo Lema 2.2.6, temos que $x \in P$ e $P = R[x;\rho]x$ ou x é regular módulo P e $P \cap R$ é um ideal fortemente ρ-primo de R.

Se $P = R[x;\rho]x$ então, $R[x;\rho]/P = R[x;\rho]/R[x;\rho]x \simeq R$. Deste modo, R é fortemente ρ-primo e com isto, a condição (i) está satisfeita.

Suponhamos agora que x é regular módulo P e $P \cap R$ é um ideal fortemente ρ-primo de R. Pelo Corolário 2.2.10, existe um ideal primo R-disjunto T de $R < x;\rho >$ tal que $P = T \cap R[x;\rho]$ e, pelo Corolário 2.1.19, $T = Q_\rho(R) < x;\rho > f_0 \cap R < x;\rho >$, onde f_0 é um polinômio irredutível em $C_\rho(R)[z]$ e distinto de z. Por sua vez, pelo Corolário 2.2.10, obtemos $T \cap R[x;\rho] = Q_\rho(R) < x;\rho > f_0 \cap R[x;\rho] = P$.

Para cada $h \in P$, existe $g = \sum_{i=-n}^{k} a_i x^i \in Q_\rho(R) < x;\rho >$ tal que $h = gf_0 = (\sum_{i=-n}^{k} a_i x^i) f_0$. O termo de menor grau deste produto é $a_{-n}c_0x^{-n}$, onde $c_0 \in C_\rho(R)$ é o termo independente de f_0. Como $h \in R[x;\rho]$ então, $a_{-n}c_0 = 0$ o que implica que $a_{-n} = 0$. Analogamente se mostra que $a_{n-1}, \cdots, a_{-1} = 0$. Assim, $g \in Q_\rho(R)[x;\rho]$ e com isto, $h \in Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$. Logo, $P = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$, onde f_0 é um polinômio mônico irredutível em $C_\rho(R)[z]$ distinto de z e segue que, a condição (ii) está satisfeita.

Reciprocamente, suponhamos que R é fortemente ρ-primo e $P = xR[x;\rho]$. Deste modo,

$$R \simeq R/R[x;\rho]x = R[x;\rho]/P$$

e, com isto, P é um ideal fortemente ρ-primo.

Suponhamos que $P = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$, onde f_0 é um polinômio mônico irredutível em $C_\rho(R)[z]$ distinto de z e seja $T = Q_\rho(R) < x;\rho > f_0 \cap R < x;\rho >$. Então, T é um ideal não-nulo R-disjunto de $R < x;\rho >$ que, pelo Corolário 2.1.19, é primo. Finalmente, pelo Corolário 2.2.10, existe um ideal fortemente ρ-primo R-disjunto K de $R[x;\rho]$ que não contém x tal que

$$K = T \cap R[x;\rho] = Q_\rho(R) < x;\rho > f_0 \cap R < x;\rho > \cap R[x;\rho] =$$
$$Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho] = P.$$

Logo, P é um ideal fortemente ρ-primo. $\square$

Corolário 2.2.12. *Existe uma correspondência biunívoca entre os conjuntos*

$$X = \{M\colon M \text{ é um ideal maximal de } C_\rho(R)[z] \text{ que não contém } z\}$$
$$Y = \{P\colon P \text{ é um ideal fortemente } \rho\text{-primo } R\text{-disjunto de } R[x;\rho] \text{ que não contém } x\}$$
$$K = \{P^*\colon P^* \text{ é um ideal fortemente } \rho\text{-primo } Q_\rho(R)\text{-disjunto de } Q_\rho(R)[x;\rho] \text{ que não contém } x\}.$$

Demonstração. Seja $M \in X$. Então $M = fC_\rho(R)[z]$, para algum polinômio irredutível $f \in C_\rho(R)[z]$ distinto de z e consideremos $P = Q_\rho(R)[x;\rho]f \cap R[x;\rho]$. Pelo Corolário 2.2.11, $P \in Y$ e assim, podemos definir $\gamma_1 : X \to Y$ por

$$\gamma_1(M) = \gamma_1(fC_\rho(R)[z]) = Q_\rho(R)[x;\rho]f \cap R[x;\rho] = P.$$

Seja $P \in Y$. Pelo Corolário 2.2.11, $P = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$, onde f_0 é um polinômio mônico, irredutível em $C_\rho(R)[z]$ e distinto de z. Consideremos $M = f_0C_\rho(R)[z] \in X$ e definimos $\gamma_2 : Y \to X$ por

$$\gamma_2(P) = \gamma_2(Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]) = f_0C_\rho(R)[z] = M.$$

Claramente, $\gamma_1 \circ \gamma_2 = Id|_Y$ e $\gamma_2 \circ \gamma_1 = Id|_X$.

Seja $P \in Y$. Pelo Corolário 2.2.11, $P = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$, onde f_0 é um polinômio mônico, irredutível em $C_\rho(R)[z]$ e distinto de z. Pelo Corolário 2.1.20, $K = Q_\rho(R) < x;\rho > f_0$ é um ideal primo $Q_\rho(R)$-disjunto de $Q_\rho(R) < x;\rho >$ e, usando o Corolário 2.2.10, $J = K \cap Q_\rho[x;\rho]$ é um ideal fortemente ρ-primo de $Q_\rho(R)[x;\rho]$. Definimos $\alpha_1 : Y \to K$ por

$$\alpha_1(P) = \alpha_1(Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]) = Q_\rho(R)[x;\rho]f_0 = J.$$

Seja $J \in K$. Então, pelo Corolário 2.2.11, $P = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$ é um ideal fortemente ρ-primo de $R[x;\rho]$ que não contém x, onde f_0 é um polinômio mônico, irredutível em $C_\rho(R)[z]$ e distinto de z. Definimos $\alpha_2 : K \to Y$ por

$$\alpha_2(J) = \alpha_2(Q_\rho(R)[x;\rho]f_0) = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho] = P.$$

Claramente, $\alpha_1 \circ \alpha_2 = Id|_Z$ e $\alpha_2 \circ \alpha_1 = Id|_Y$. A prova está completa. $\square$

2.3 Ideais Primos em Skew Anel de Polinômios do Tipo Automorfismo

Nesta seção R é um anel primo, ρ é um automorfismo de R e $Q_\rho(R)$ é o anel de ρ-quocientes à esquerda de Martindale de R. Note que $Q_\rho(R)$ é um anel primo. Baseados nos resultados da seção anterior obtemos uma descrição completa dos ideais primos em $R[x;\rho]$. As provas dos resultados que seguem são completamente análogas às provas dos Lemas 2.2.5 e 2.2.9 e, Corolários 2.2.10, 2.2.11 e 2.2.12, respectivamente e por isto iremos omitir.

Lema 2.3.1. *Seja P um ideal primo de $R[x;\rho]$. Então $x \in P$ e $P = P \cap R + R[x;\rho]x$ ou x é regular módulo P e $P \cap R$ é um ideal fortemente ρ-primo de R.*

Lema 2.3.2. *Seja P um ideal R-disjunto de $R[x;\rho]$ que não contém x. As seguintes afirmações são válidas:*

i) Se P é um ideal primo, então P é maximal com relação a propriedade de ser R-disjunto no conjunto dos ideais ρ-invariantes R-disjuntos de $R[x;\rho]$.

ii) Se P é maximal no conjunto dos ideais R-disjuntos de $R[x;\rho]$, então P é primo.

Corolário 2.3.3. *Existe uma correspondência biunívoca via contração entre*

$$X = \{P^*\text{: } P^* \text{ é ideal primo } R\text{-disjunto de } R < x; \rho >\} \text{ e}$$
$$Y = \{P\text{: } P \text{ é ideal primo } R\text{-disjunto de } R[x;\rho] \text{ que não contém } x\}.$$

Corolário 2.3.4. *Seja P um ideal não-nulo R-disjunto de $R[x;\rho]$. Então, P é primo se, e somente se, uma das seguintes condições for satisfeita:*

i) $P = xR[x;\rho]$.

ii) $P = Q_\rho(R)[x;\rho]f_0 \cap R[x;\rho]$, *onde f_0 é um polinômio mônico irredutível em $C_\rho(R)[z]$ distinto de z.*

Corolário 2.3.5. *Existe uma correspondência biunívoca entre os seguintes conjuntos*

$$X = \{M\text{: } M \text{ é um ideal maximal de } C_\rho(R)[z] \text{ que não contém } z\}$$
$$Y = \{P\text{: } P \text{ é um ideal primo } R\text{-disjunto de } R[x;\rho] \text{ que não contém } x\}$$
$$K = \{P^*\text{: } P^* \text{ é um ideal primo } Q_\rho(R)\text{-disjunto de } Q_\rho(R)[x;\rho] \text{ que não contém } x\}.$$

Observação

Durante a preparação da dissertação, não pudemos encontrar uma prova ou contra-exemplo, mesmo após uma vasta procura na literatura, para o seguinte lema ([3], Lemma 3.2):

Seja P um ideal R-disjunto de $R[x;\rho]$ que não contém x. Então P é primo se, e somente se, R é fortemente ρ-primo e P é maximal com relação a propriedade de ser R-disjunto.

Os resultados mais próximos foram os Lemas 2.2.9 e 2.3.2, onde neste último, assumimos que R é um anel primo.

Claramente, se o Lema 2.2.9 fosse provado para ideais primos e não só para fortemente ρ-primos, o que seria a prova do Lema acima enunciado, obteríamos uma descrição completa dos ideais primos R-disjuntos de $R[x;\rho]$.

Capítulo 3

Ideais Primos em Skew Anel de Polinômios do Tipo Derivação

O objetivo deste capítulo é estudar os ideais primos R-disjuntos no skew anel de polinômios do tipo derivação $R[x;d]$, onde R é um anel d-primo. Todos os resultados que serão apresentados neste capítulo são do artigo [8].

Lema 3.1.1. *Seja L um d-ideal de R. Então, o conjunto de todos os polinômios com coeficientes em L, denotado por $L[x;d]$, é um ideal de $R[x;d]$.*

Demonstração. Claramente, $0 \in L[x;d]$ e a soma de elementos de $L[x;d]$ está em $L[x;d]$. Sejam $ax^j \in L[x;d]$ e $bx^k \in R[x;d]$. Então,

$$(ax^j)(bx^k) = a\sum_{i=0}^{j} \begin{pmatrix} j \\ i \end{pmatrix} d^i(b)x^{j-i}x^k \in L[x;d]$$

e

$$(bx^k)(ax^j) = b\sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} d^i(a)x^{k-i}x^j \in L[x;d]$$

desde que L é um d-ideal de R. □

Seja I um ideal de $R[x;d]$ e note que, para cada $f \in I$, $d(f) \in I$. Assim, $I \cap R$ é um d-ideal de R. Denotaremos por $\tau(I)$ o d-ideal de R consistindo de todos os coeficientes líderes dos polinômios próprios de grau mínimo $n \geq 0$ em I, juntamente com o zero.

Definimos $Min(I) = Min\{\delta(f);\ 0 \neq f \in I\}$. Um ideal I de $R[x;d]$ é dito *R-disjunto* se $I \cap R = 0$.

Lema 3.1.2. *Seja P um ideal primo de $R[x;d]$. Então, $P \cap R$ é um d-ideal primo de R.*

Demonstração. Sejam I e J d-ideais de R tais que $IJ \subseteq P \cap R$. Usando um raciocínio análogo ao da Observação 2.2.4, respeitando a regra de multiplicação em $R[x;d]$, obtemos que $I[x;d]J[x;d] = IJ[x;d]$ e com isto, $I[x;d]J[x;d] \subseteq P$.

Como P é um ideal primo de $R[x;d]$, então $I \subseteq I[x;d] \subseteq P$ ou $J \subseteq J[x;d] \subseteq P$. Logo, $I \subseteq P \cap R$ ou $J \subseteq P \cap R$ e portanto, $P \cap R$ é um d-ideal primo de R. $\square$

Seja P um ideal primo de $R[x;d]$. Então, fatorando $P \cap R$ e $(P \cap R)[x;d]$ de R e $R[x;d]$ respectivamente, podemos assumir que R é um anel d-primo e P é R-disjunto.

Vamos agora analisar a estrutura dos ideais R-disjuntos de $R[x;d]$.

Lema 3.1.3. *As seguintes afirmações são equivalentes*

i) Existe um ideal R-disjunto não-nulo de $R[x;d]$.

ii) O centro de $Q_d(R)[x;d]$ é não-trivial, ou seja, $Z = C_d(R)[z]$, onde z está descrito na Proposição 1.3.2.

Além disso, para todo ideal não-nulo R-disjunto I de $R[x;d]$, existe um único polinômio mônico $f_I \in Z$ tal que, para todo $f \in I$ com $\delta(f) = Min(I)$, $f = lc(f)f_I$.

Demonstração. $(i) \Rightarrow (ii)$ Seja I um ideal não-nulo R-disjunto de $R[x;d]$ tal que $Min(I) = n$ e consideremos $a \in \tau(I)$. Então, existe $f \in I$ tal que $lc(f) = a$ e $\delta(f) = n$.

Suponhamos que existe $g \in I$ tal que $lc(g) = a$ e $\delta(g) = n$. Então, $f - g \in I$ e note que $\delta(f - g) < n$. Com isto $f = g$ e deste modo, f é único.

Seja $f = ax^n + a_{n-1}x^{n-1} + \cdots + a_0$ e definimos $\beta_i : \tau(I) \to R$ por $\beta_i(a) = a_i$. Claramente β_i é um homomorfismo de R-módulos à esquerda bem definido para todo $i \in \{0, 1, \cdots, n\}$, onde $a_n = a$. Pelo Lema 1.1.6, existem $q_n = 1, q_{n-1}, \cdots, q_0 \in Q_d(R)$ tais que $\beta_i(a) = aq_i$, para todo $a \in \tau(I)$. Definimos

$$f_I = x^n + q_{n-1}x^{n-1} + \cdots + q_0 \in Q_d(R)[x; d]$$

e temos que, para todo $h \in I$ com $\delta(h) = n$, $lc(h)f_I = h$.

Suponhamos que existe $g \in Q_d(R)[x; d]$ com a propriedade que, para qualquer $f \in I$ com $\delta(f) = Min(I)$, $f = lc(f)g$. É evidente que $lc(f)[f_I - g] = 0$ e com isto, $\tau(I)[f_I - g] = 0$. Pelo Lema 1.1.6, $f_I = g$ e segue que f_I é único.

Seja $a \in \tau(I)$. Então, $d(a) \in \tau(I)$ e temos que, $af_I, d(a)f_I \in I$. Assim, $ad(f_I) = d(af_I) - d(a)f_I \in I$. Desde que $\delta(d(af_I) - d(a)f_I) < n$, então $ad(f_I) = 0$ e segue que $\tau(I)d(f_I) = 0$. Pelo Lema 1.1.6, $d(f_I) = 0$ e conseqüentemente, $xf_I = f_I x$.

Seja $b \in R$. Então $abf_I - af_I b \in I$ é tal que $\delta(abf_I - af_I b) < n$ e com isto, $\tau(I)[bf_I - f_I b] = 0$. Segue do Lema 1.1.6 que, $bf_I = f_I b$.

Seja $q \in Q_d(R)$. Pelo Lema 1.1.6, existe um d-ideal não-nulo J de R tal que $Jq \subseteq R$. Claramente, para todo $j \in J$

$$(jq)f_I = f_I(jq) = (f_I j)q = (jf_I)q.$$

Assim, $j[qf_I - f_I q] = 0$ e desta forma, $J[qf_I - f_I q] = 0$. Pelo Lema 1.1.6, $f_I q = qf_I$ e segue que $f_I \in Z$.

$(ii) \Rightarrow (i)$ Suponhamos que Z seja não-trivial. Desta maneira, existe um polinômio não-nulo $f \in Q_d(R)[x; d]$ com $\delta(f) \geq 1$ tal que $gf = fg$, para todo $g \in Q_d(R)[x; d]$. Claramente $Q_d(R)[x; d]f$ é um ideal de $Q_d(R)[x; d]$.

Seja $t \in Q_d(R)[x; d]f \cap Q_d(R)$. Então, existe $h \in Q_d(R)[x; d]$ tal que $t = hf$. Como $lc(f) \in C_d(R)$ e, pelo Lema 1.3.2, $C_d(R)$ é um corpo, então podemos assumir que f é mônico. Desde que $\delta(h) + \delta(f) = 0$, então $\delta(h) = \delta(f) = 0$, o que contradiz o fato de Z ser não-trivial. Logo, $t = 0$ e com isto, $Q_d(R)[x; d]f$ é $Q_d(R)$-disjunto.

Conseqüentemente, $Q_d(R)[x; d]f \cap R[x; d]$ é um ideal R-disjunto não-nulo de $R[x; d]$. $\square$

O polinômio f_I construído no lema anterior será denotado o *polinômio canônico* do ideal não-nulo R-disjunto I de $R[x; d]$.

Corolário 3.1.4. (i) *Seja f_I o polinômio canônico do ideal R-disjunto I de $R[x; d]$. Então $I \subseteq f_I Q_d(R)[x; d] \cap R[x; d]$.*

(ii) *Seja f_J o polinômio canônico do ideal $Q_d(R)$-disjunto J de $Q_d(R)[x; d]$. Então $f_J = f_{J \cap R[x;d]} \in Z$.*

Demonstração. (i) Seja $f \in I$. Pelo algoritmo da divisão, existem $h, r \in Q_d(R)[x; d]$ tais que $f = hf_I + r$, onde $r = 0$ ou $\delta(r) < \delta(f_I)$. Pelo Lema 1.1.6, existe um d-ideal não-nulo L de R tal que $Lh \subseteq R[x; d]$ e $Lr \subseteq R[x; d]$. Para todo $j \in L$ e $c \in \tau(I)$ temos que,

$$cjr = cj(f - hf_I) = cjf - cjf_I h = cjf - cf_I jh \in I$$

com $\delta(cjr) \leq \delta(r) < \delta(f_I) = Min(I)$ e desta maneira, $\tau(I)Lr = 0$. Por sua vez, $\tau(I)L$ é um d-ideal não-nulo de R e, pelo Lema 1.1.6, temos que $r = 0$. Logo, $f \in Q_d(R)[x; d]f_I \cap R[x; d]$ e portanto, $I \subseteq f_I Q_d(R)[x; d] \cap R[x; d]$.

(ii) É evidente que $I = J \cap R[x; d]$ é um ideal R-disjunto de $R[x; d]$ e suponhamos que existe um polinômio não-nulo $f \in J$ tal que $\delta(f) = Min(J) < Min(I)$. Pelo Lema 1.1.6, existe um d-ideal não-nulo L de R tal que $Lf \subseteq R[x; d]$ e com isto, $Lf \subseteq I$. Note que, para cada $l \in L$, $\delta(lf) \leq \delta(f) < Min(I)$. Logo, $Lf = 0$ e, pelo Lema 1.1.6, $f = 0$, o que contradiz a escolha de f. Com isto, $Min(J) = Min(I)$.

Sejam $g \in J$ tal que $\delta(g) = Min(J)$ e f_I o polinômio canônico de I. Pelo algoritmo da divisão, existem $h, r \in Q_d(R)[x; d]$ tais que $g = hf_I + r$, onde $r = 0$ ou $\delta(r) < \delta(f_I)$.

Como $\delta(g) = Min(I) = \delta(f_I)$ e $\delta(r) < \delta(f_I)$, então $\delta(h) = 0$. Sendo f_I um polinômio mônico, temos que $h = lc(g)$ e segue que $g = lc(g)f_I + r$. Por um método análogo ao desenvolvido em (i), obtemos $r = 0$ e com isto, $g = lc(g)f_I$. Pelo Lema 3.1.3, $g = lc(g)f_J$ e segue que $0 = lc(g)[f_I - f_J]$. Logo, $\tau(J)[f_I - f_J] = 0$ e portanto, pelos Lemas 1.1.6 e 3.1.3, obtemos $f_J = f_I = f_{J \cap R[x;d]} \in Z$. □

Antes de prosseguir na aplicação dos resultados anteriores ao estudo dos ideais primos, precisaremos do seguinte lema, cuja prova á análoga a do Lema 2.1.15.

Lema 3.1.5. *Sejam I um ideal não-nulo de $R[x;d]$ e f um polinômio não-nulo de grau mínimo n em I tal que $lc(f) = a$. Suponhamos que $m \geq n$ e $g \in I \cap R_m$. Se $a_j \in R$ e i_j são inteiros não-negativos para todo $j \in \{1, 2 \cdots, m-n\}$, então existe $h \in R_{m-n}$ tal que*

$$ha_0 d^{i_0}(f) = g \prod_{j=0}^{m-n} (a_{m-n-j} d^{i_{m-n-j}}(a)) \tag{3.1}$$

para todo $a_0 \in R$ e $i_0 \geq 0$.

Lema 3.1.6. *Seja P um ideal não-nulo R-disjunto de $R[x;d]$. Então, as seguintes condições são equivalentes:*

i) P é um ideal primo de $R[x;d]$.

ii) P é maximal entre todos os ideais R-disjuntos de $R[x;d]$.

Demonstração. $(i) \Rightarrow (ii)$ Seja I um ideal R-disjunto de $R[x;d]$ tal que $P \subseteq I$. Consideremos $f \in I$ um polinômio não-nulo de grau mínimo n em I tal que $lc(f) = a$ e $g \in P$ um polinômio não-nulo de grau mínimo m em P tal que $lc(g) = b$. Como $g \in P \cap R_m \subseteq I \cap R_m$ e suponhamos $1 \leq n < m$ então, pelo Lema 3.1.5, existe $h \in R_{m-n}$ tal que

$$ha_0 d^{i_0}(f) = g \prod_{j=0}^{m-n} (a_{m-n-j} d^{i_{m-n-j}}(a))$$

para todo $a_0 \in R$ e $i_0 \geq 0$ e segue que,

$$ha_0d^{i_0}(f) = g(a_{m-n}d^{i_{m-n}}(a)) \cdots (a_1d^{i_1}(a))(a_0d^{i_0}(a)).$$

Como $a_jd^{i_j}(a) \in \tau(I)$, para todo $j \in \{0, 1, \cdots, m-n\}$, então $ha_0d^{i_0}(f) = g\prod_{j=0}^{m-n}(a_{m-n-j}d^{i_{m-n-j}}(a)) \in g\tau(I) \subseteq gR \subseteq P$, para todo $a_0 \in R$ e $i_0 \geq 0$. Em particular, temos que $hrf \in P$, para todo $r \in R$ e, conseqüentemente, $hrfx = hrxf - hrd(f) \in P$. Desta maneira, $hrxf \in P$. Suponhamos, por hipótese de indução, que $hrx^kd^{i_0}(f) \in P$, para todo $k < i$ e $i_0 \geq 0$. Como

$$hrfx^i = hrx^if - hr\sum_{t=0}^{i-1}\begin{pmatrix} i \\ t+1 \end{pmatrix} d^{t+1}(f)x^{i-t-1}$$

e, por hipótese de indução, $hr\sum_{t=0}^{i-1}\begin{pmatrix} i \\ t+1 \end{pmatrix} d^{t+1}(f)x^{i-t-1} \in P$ então, $hrx^if \in P$. Deste modo $hR[x;d]f \subseteq P$. Desde que P é primo então, $f \in P$ ou $h \in P$. Como $m - n > 0$, então $f = 0$ ou $h = 0$, o que contradiz o fato que f e h não são nulos. Logo, $m = n$ e com isto, $I \cap R_n \subseteq P \cap R_n$.

Usando um processo análogo a prova do Lema 2.2.8, podemos concluir que $I \cap R_t = P \cap R_t$, para todo $t \geq 0$. Logo, $I \subseteq P$.

$(ii) \Rightarrow (i)$ Seja P um ideal não-nulo de $R[x;d]$ maximal com relação a propriedade de ser R-disjunto. Consideremos J e K ideais de $R[x;d]$ tais que $JK \subseteq P$, $J \nsubseteq P$ e $K \nsubseteq P$. Logo $P \subsetneqq (J+P)$ e $P \subsetneqq (K+P)$ e com isto, $(J+P) \cap R \neq 0$ e $(K+P) \cap R \neq 0$.

Desde que $[(J+P) \cap R][(K+P) \cap R] \subseteq P \cap R$, então $P \cap R \neq 0$, o que contradiz o fato que P é um ideal R-disjunto de $R[x;d]$. Portanto, P é primo. $\square$

Teorema 3.1.7. *Seja P um ideal não-nulo R-disjunto de $R[x;d]$. Então, as seguintes condições são equivalentes:*

i) P é um ideal primo de $R[x;d]$.

ii) $P = f_P Q_d(R)[x;d] \cap R[x;d]$ *e* f_P *é um polinômio irredutível em* $C_d(R)[z]$.

iii) *Existe um ideal primo* $Q_d(R)$*-disjunto* P^* *de* $Q_d(R)[x;d]$ *de tal forma que* $P = P^* \cap R[x;d]$.

Demonstração. $(i) \Rightarrow (ii)$ Seja $f_P \in Q_d(R)[x;d]$ o polinômio canônico de P. Pelo Corolário 3.1.4, $P \subseteq f_P Q_d(R)[x;d] \cap R[x;d]$. Desde que $f_P Q_d(R)[x;d] \cap R[x;d]$ é um ideal R-disjunto de $R[x;d]$ então, pelo Lema 3.1.6, temos $P = f_P Q_d(R)[x;d] \cap R[x;d]$.

Suponhamos que existem $h, l \in C_d(R)[z]$ tais que $\delta(h) > 0$, $\delta(l) > 0$ e $f_P = hl$. É evidente que $f_P Q_d(R)[x;d] \subseteq hQ_d(R)[x;d]$ e com isto, $P \subseteq hQ_d(R)[x;d] \cap R[x;d]$. Pelos Lemas 3.1.3 e 3.1.6, $P = hQ_d(R)[x;d] \cap R[x;d]$ e de maneira análoga, obtemos $P = lQ_d(R)[x;d] \cap R[x;d]$.

Pelo Lema 1.1.6, existe um d-ideal não-nulo I de R tal que $Il \subseteq R[x;d]$ e $Ih \subseteq R[x;d]$. Claramente, para todo $a \in I$, $al \in P$ e $ah \in P$. Como $\delta(h) < \delta(f_P)$ e $\delta(l) < \delta(f_P)$, então $al = ah = 0$ e, segue do Lema 1.1.6 que, $h = l = 0$, o que contradiz o fato que $\delta(h) > 0$ e $\delta(l) > 0$. Logo, f_P é irredutível em $C_d(R)[z]$.

$(ii) \Rightarrow (iii)$ Seja L um ideal primo $Q_d(R)$-disjunto de $Q_d(R)[x;d]$ tal que $L \supseteq f_P Q_d(R)[x;d]$ e consideremos f_L o polinômio canônico de L. De maneira análoga ao feito em $(i) \Rightarrow (ii)$, $L = f_L Q_d(R)'[x;d] \cap Q_d(R)[x;d]$, onde $Q_d(R)'$ é o anel de d-quocientes à esquerda de Martindale de $Q_d(R)$. Pelo Corolário 3.1.4, temos que $f_L Q_d(R)[x;d] \subseteq L$.

Seja $t \in L$. Então, existe $h \in Q_d(R)'[x;d]$ tal que $t = f_L h \in Q_d(R)[x;d]$. Suponhamos que

$$f_L = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \text{ e}$$
$$h = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_0.$$

Note que o coeficiente do termo de grau $n+s$ de t é $c_s \in Q_d(R)$ e o coeficiente do termo de grau $n+s-1$ é $c_{s-1} + \binom{n}{1} d(c_s) + a_{n-1}c_s$. Desde que $\binom{n}{1} d(c_s) + a_{n-1}c_s \in$

$Q_d(R)$ então $c_{s-1} \in Q_d(R)$. Procedendo com este raciocínio um número suficiente de vezes obtemos que $h \in Q_d(R)[x;d]$ e conseqüentemente, $t \in f_L Q_d(R)[x;d]$. Assim, $L = f_L Q_d(R)[x;d]$.

Como $f_P Q_d(R)[x;d] \subseteq L = f_L Q_d(R)[x;d]$, então existe $g \in Q_d(R)[x;d]$ tal que $f_P = f_L g$. Por sua vez, $0 = d(f_P) = f_L d(g)$ e, sendo f_L mônico, segue que $d(g) = 0$.

Para cada $q \in Q_d(R)$,

$$f_L(qg) = q(f_L g) = q f_P = f_P q = (f_L g)q = f_L(gq)$$

e com isto, $(qg - gq)f_L = 0$. Desde que f_L é mônico, então $qg = gq$ e desta forma, $g \in C_d(R)[z]$. Usando a hipótese que f_P é irredutível em $C_d(R)[z]$, obtemos que $f_P = f_L$. Logo, $f_L Q_d(R)[x;d] = f_P Q_d(R)[x;d] = L$ é um ideal primo e portanto, basta considerar $P^* = f_P Q_d(R)[x;d]$.

$(iii) \Rightarrow (i)$ Sejam L um ideal primo R-disjunto de $R[x;d]$ tal que $P \subseteq L$ e f_L o polinômio canônico de L. Procedendo de maneira análoga ao feito em $(i) \Rightarrow (ii)$, obtemos $L = f_L Q_d(R)[x;d] \cap R[x;d]$.

Consideremos $g \in P^*$. Pelo Lema 1.1.6, existe um d-ideal não-nulo H de R tal que $Hg \subseteq R[x;d]$ e segue que $Hg \subseteq L$.

Pelo algoritmo da divisão, existem $h, r \in Q_d(R)[x;d]$ tais que $g = f_L h + r$, onde $r = 0$ ou $\delta(r) < \delta(f_L)$. Usando um raciocínio análogo ao desenvolvido no Corolário 3.1.4, temos que $r = 0$ e com isto, $g \in f_L Q_d(R)[x;d]$. Logo, $P^* \subseteq f_L Q_d(R)[x;d]$.

Pela maximalidade de P^* no conjunto dos ideais $Q_d(R)$-disjuntos de $Q_d(R)[x;d]$ segue que $P^* = f_L Q_d(R)[x;d]$ e com isto, $P = L$. Logo, P é primo. $\square$

Corolário 3.1.8. *Existe uma correspondência biunívoca entre os conjuntos*

$$X = \{M : M \text{ é ideal maximal de } Z\},$$
$$Y = \{P : P \text{ é ideal primo } R\text{-disjunto de } R[x;d]\} \text{ e}$$
$$W = \{P^* : P^* \text{ é um ideal primo } Q_d(R)\text{-disjunto de } Q_d(R)[x;d]\}.$$

Demonstração. Se não existirem ideais primos não-nulos R-disjuntos de $R[x;d]$, a prova segue análoga a primeira parte da prova do Corolário 2.1.20.

Consideremos $M \in X$. Assim, M é gerado por um polinômio $f \in Z$ irredutível em Z. Pelo Teorema 3.1.7, $T = fQ_d(R)[x;d] \cap R[x;d] \in Y$ e com isto, definimos $\gamma_1 : X \to Y$ por

$$\gamma_1(M) = \gamma_1(Zf) = fQ_d(R)[x;d] \cap R[x;d] = T.$$

Seja $P \in Y$. Pelo Teorema 3.1.7 temos que $P = f_P Q_d(R)[x;d] \cap R[x;d]$, onde f_P é um polinômio irredutível em Z. Consideremos $M = Zf_P$ o ideal gerado por f_P. Logo, $M \in X$ e, definimos $\gamma_2 : Y \to X$ por

$$\gamma_2(P) = \gamma_2(f_P Q_d(R)[x;d] \cap R[x;d]) = Zf_P = M.$$

Claramente, $\gamma_1 \circ \gamma_2 = id|_Y$, $\gamma_2 \circ \gamma_1 = id|_X$.

Seja $J \in W$. Pelo Teorema 3.1.7, $P = J \cap R[x;d] \in Y$ e com isto, definimos $\alpha_1 : W \to Y$ por

$$\alpha_1(J) = J \cap R[x;d] = P.$$

Seja $L \in Y$. Pelo Teorema 3.1.7, $L = f_L Q_d(R)[x;d] \cap R[x;d]$, onde f_L é um polinômio irredutível em Z e $J = f_L Q_d(R)[x;d] \in W$. Definimos $\alpha_2 : Y \to W$ por

$$\alpha_2(L) = \alpha_2(f_L Q_d(R)[x;d] \cap R[x;d]) = f_L Q_d(R)[x;d] = J.$$

Claramente, $\alpha_1 \circ \alpha_2 = id|_Y$ e $\alpha_2 \circ \alpha_1 = id|_W$. A prova está completa. □

No que segue, iremos obter uma caracterização intrínseca para ideais primos de $R[x;d]$. Seja I um ideal não-nulo R-disjunto de $R[x;d]$. Definimos o fecho $[I]$ de I por $[I] = f_I Q_d(R)[x;d] \cap R[x;d]$, onde f_I é o polinômio canônico de I. Pelo Corolário 3.1.4, $I \subseteq [I]$. O ideal I é dito fechado se $I = [I]$. Mostraremos no Lema 3.1.12 que $[[I]] = [I]$.

Seja $f \in I$ tal que $lc(f) = a$ e $\delta(f) = n = Min(I)$. Consideremos $g = frd^i(a) - ard^i(f)$, para todo $i \geq 0$ e $r \in R$. Claramente, $g \in I$ e $\delta(g) < n$. Assim, $g = 0$ e conseqüentemente, para todo $i \geq 0$ e $r \in R$,

$$frd^i(a) = ard^i(f). \tag{3.2}$$

Seja Γ o conjunto de todos os polinômios de $R[x; d]$ que satisfazem a condição 3.2. Para cada $g \in \Gamma$, com $lc(g) = b$, consideremos

$$[g] = \{h \in R[x; d]\colon \text{ existe um } d\text{-ideal não-nulo } H \text{ de } R \text{ tal que } bHd^i(h) \subseteq gR[x; d], \\ \text{para todo } i \geq 0\}.$$

Lema 3.1.9. *Seja $f \in \Gamma$. Então, $[f]$ é um ideal R-disjunto de $R[x; d]$ que contém f como polinômio próprio de grau mínimo.*

Demonstração. Não é difícil ver que $[f]$ é um ideal de $R[x; d]$.

Como $f \in \Gamma$, então f satisfaz a condição 3.2, isto é, $ard^i(f) = frd^i(a)$, onde $a = lc(f)$, para todo $r \in R$ e $i \geq 0$. Assim, $aRd^i(f) \subseteq fR \subseteq fR[x; d]$ e com isto, $f \in [f]$.

Suponhamos que existe um polinômio próprio não-nulo $l \in [f]$ tal que $\delta(l) < \delta(f)$. Então, existe um d-ideal não-nulo H de R tal que $aHd^i(l) \subseteq fR[x; d]$, para todo $i \geq 0$. Em particular, $aHl \subseteq fR[x; d]$. Para cada $k \in H$, podemos escolher $g_k = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0 \in R[x; d]$, $c_i \in R$, de grau minimal tal que $akl = fg_k$.

Note que, $lc(fg_k) = ac_m = akb$, onde $b = lc(l)$. Se $ac_m \neq 0$ então $\delta(l) \geq \delta(akl) = \delta(fg_k) = m + n \geq n = \delta(f)$, o que contradiz o fato que $\delta(l) < \delta(f)$. Assim, $ac_m = 0$.

Pela condição 3.2, temos que $frd^i(a) = ard^i(f)$, para todo $r \in R$ e $i \geq 0$. Em particular, para $c_m r \in R$, $fc_m rd^i(a) = ac_m rd^i(f) = 0$, ou seja,

$$fc_m Rd^i(a) = 0 \tag{3.3}$$

para todo $i \geq 0$.

Consideremos $A = \sum_{i \geq 0} Rd^i(a)R$ um d-ideal não-nulo de R. Pela igualdade 3.3, segue que $fc_mA = 0$ e com isto, $fc_mA[x; d] = 0$. Por [10], $R[x; d]$ é um anel primo e como $A \neq 0$, temos que $fc_m = 0$.

Logo, $fg_k = f(g - c_mx^m)$, o que contradiz a escolha de g_k e, portanto, f é um polinômio de grau mínimo em $[f]$ e com isto, $[f] \cap R = 0$. □

Lema 3.1.10. *Sejam I um ideal R-disjunto de $R[x; d]$ e f_I o polinômio canônico de I. Então, $Min(f_IQ_d(R)[x; d]) = Min(I)$.*

Demonstração. Suponhamos que existe um polinômio não-nulo $h = f_Ig \in f_IQ_d(R)[x; d]$ tal que $\delta(h) < Min(I)$, para algum polinômio $g \in Q_d(R)[x; d]$. Pelo Lema 1.1.6, existe um d-ideal não-nulo L de R tal que $Lh \subseteq R[x; d]$ e $Lg \subseteq R[x; d]$. Seja $J = L \cap \tau(I) \in \mathcal{I}_d$. Assim, para cada $a, b \in J$, temos que $abh = abf_Ig = af_Ibg \in I$ é tal que $\delta(abh) \leq (h) < Min(I)$. Logo, $J^2h = 0$ e, pelo Lema 1.1.6, $h = 0$. Portanto, $Min(f_IQ_d(R)[x; d]) = Min(I)$. □

Lema 3.1.11. *Sejam I um ideal não-nulo R-disjunto de $R[x; d]$ e $f \in I$ com $\delta(f) = Min(I)$ e $lc(f) = a$. Então, $f \in \Gamma$ e $[I] = [f]$.*

Demonstração. Seja $g = ard^i(f) - frd^i(a) \in I$, para todo $i \geq 0$ e $r \in R$. Claramente $g = 0$ e, pela condição 3.2, $f \in \Gamma$. Pelo Lema 3.1.3, $f = af_I$.

Consideremos $h \in [I] = Q_d(R)[x; d]f_I \cap R[x; d]$, onde f_I é o polinômio canônico de I. Então, existe $g \in Q_d(R)[x; d]$ tal que $h = gf_I$. Pelo Lema 1.1.6, existe um d-ideal não-nulo J de R tal que $Jg \subseteq R[x; d]$ e temos que, para cada $j \in J$,

$$ajd^i(h) = ajd^i(gf_I) = ajf_Id^i(g) = fjd^i(g). \tag{3.4}$$

Por sua vez, $jd(g) = d(jg) - d(j)g \in R[x; d]$.

Suponhamos, por hipótese de indução, que $Jd^k(g) \subseteq R[x; d]$, para todo $k < i$ e note que,

$$d^i(jg) = \sum_{n=0}^{i} \begin{pmatrix} i \\ n \end{pmatrix} d^{i-n}(j)d^n(g) = jd^i(g) + \sum_{n=0}^{i-1} \begin{pmatrix} i \\ n \end{pmatrix} d^{i-n}(j)d^n(g).$$

Por hipótese de indução, $\sum_{n=0}^{i-1} \begin{pmatrix} i \\ n \end{pmatrix} d^{i-n}(j)d^n(g) \in R[x;d]$. Como $d^i(jg) \in R[x;d]$, então $jd^i(g) \in R[x;d]$. Deste modo, $Jd^i(g) \subseteq R[x;d]$ e segue da igualdade 3.4 que $aJd^i(h) \subseteq fR[x;d]$. Logo, $h \in [f]$ e com isto, $[I] \subseteq [f]$.

Por outro lado, seja $g \in [f]$. Então existe um d-ideal não-nulo L de R tal que $aLd^i(g) \subseteq fR[x;d]$, para todo $i \geq 0$. Pelo algoritmo da divisão, existem $h, r \in Q_d(R)[x;d]$ tais que $g = hf_I + r$, onde $r = 0$ ou $\delta(r) < \delta(f_I)$. Pelo Lema 1.1.6, existe um d-ideal não-nulo K de R tal que $Kh \subseteq R[x;d]$ e $Kr \subseteq R[x;d]$.

Para cada $l \in L \cap K$, temos que $ald^i(g) = alf_I d^i(h) + ald^i(r) \in fR[x;d]$, para todo $i \geq 0$. Assim, $ald^i(g) \in fR[x;d] \subseteq Q_d(R)[x;d]f_I$ e segue que, $ald^i(r) \in Q_d(R)[x;d]f_I$.

Pelo Lema 3.1.10, $Min(I) = Min(f_I Q_d(R)[x;d])$. Deste modo, $\delta(ald^i(r)) \leq \delta(r) < Min(f_I Q_d(R)[x;d])$ e com isto, $ald^i(r) = 0$. Seja $r = a_s x^s + a_{s-1}x^{s-1} + \cdots + a_0$. Então,

$$0 = ald^i(r) = al[d^i(a_s)x^s + d^i(a_{s-1})x^{s-1} + \cdots + d^i(a_0)].$$

Conseqüentemente, $aL \cap Kd^i(a_j) = 0$ para todo $i \geq 0$ e $0 \leq j \leq s$. Como $ald^i(a_0) = 0$, então

$$ald^{i+1}(a_0) + ad(l)d^i(a_0) + d(a)ld^i(a_0) = 0.$$

Usando o fato que $d(l) \in L \cap K$, obtemos $ald^{i+1}(a_0) = ad(l)d^i(a_0) = 0$ e segue que, $d(a)ld^i(a_0) = 0$, para todo $i \geq 0$ e $l \in L \cap K$.

Por indução, é fácil ver que, para todo $i, j \geq 0$ e $l \in L \cap K$

$$d^j(a)ld^i(a_0) = 0. \tag{3.5}$$

Consideremos $A = (\sum_{j \geq 0} Rd^j(a)R)(L \cap K)$ um d-ideal não-nulo de R. Como

$R(L \cap K) = L \cap K$ então, segue da igualdade 3.5 que $Aa_0 = 0$ e, pelo Lema 1.1.6, $a_0 = 0$. Repetindo este raciocínio aos demais coeficientes de r podemos concluir que $r = 0$.

Logo, $g = f_I h \in f_I Q_d(R)[x; d] \cap R[x; d]$ e portanto, $[f] \subseteq [I]$. $\square$

Lema 3.1.12. *Seja I um ideal não-nulo R-disjunto de $R[x; d]$. Então $[I]$ é o maior ideal de $R[x; d]$ que contém I e satisfaz $Min([I]) = Min(I)$. Em particular, $[[I]] = [I]$.*

Demonstração. Sejam I um ideal não-nulo R-disjunto de $R[x; d]$ e f um polinômio de grau mínimo n em I. Pelos Lemas 3.1.11 e 3.1.9, $f \in \Gamma$ e $[I] = [f]$ é um ideal R-disjunto de $R[x; d]$ que contém f como polinômio de grau mínimo. Assim,

$$Min([I]) = Min([f]) = \delta(f) = n = Min(I)$$

e, pelo Corolário 3.1.4, $I \subseteq [I]$.

Seja H um ideal de $R[x; d]$ que contém I tal que $Min(H) = Min(I)$. Como f é um polinômio em H de grau minimal, então $[H] = [f]$ e com isto, $H \subseteq [H] = [f] = [I]$. Assim, $[I]$ é o maior ideal de $R[x; d]$ que contém I e satisfaz $Min([I]) = Min(I)$.

Considere agora $f_{[I]}$ o polinômio canônico do ideal R-disjunto $[I]$ de $R[x; d]$. Pelo Corolário 3.1.4, $[I] \subseteq Q_d(R)[x; d] f_{[I]} \cap R[x; d] = [[I]]$. Logo, $Min([[I]]) = Min(I)$ e $I \subseteq [I] \subseteq [[I]]$ e com isto, $[I] = [[I]]$. $\square$

Lema 3.1.13. *Sejam $f, g \in \Gamma$. Então, $[f] \subseteq [g]$ se, e somente se, $f \in [g]$.*

Demonstração. Suponhamos que $[f] \subseteq [g]$. Pelo Lema 3.1.9, $f \in [f]$ e com isto, $f \in [g]$.

Reciprocamente, suponhamos que $f \in [g]$ e seja g' o polinômio canônico de $[g]$. Assim, existe um d-ideal não-nulo H de R tal que $bHd^i(f) \subseteq gR[x; d]$, para todo $i \geq 0$, com $b = lc(g)$. Como $g \in [g]$ é um polinômio de grau minimal em $[g]$ então, pelo Lema 3.1.3, $g = bg'$.

Pelo algoritmo da divisão, existem $q, r \in Q_d(R)[x;d]$ tais que $f = g'q + r$, onde $r = 0$ ou $\delta(r) < \delta(g')$. Pelo Lema 1.1.6, existe um d-ideal não-nulo J de R tal que $Jq \subseteq R[x;d]$ e $Jr \subseteq R[x;d]$. Seja $K = H \cap J$. Então, para cada $k \in K$,

$$bkd^i(r) = bkd^i(f - g'q) = bkd^i(f) - bkd^i(g'q) \in bKd^i(f) + bg'Kd^i(q).$$

Pela prova do Lema 3.1.11, $Jd^i(q) \subseteq R[x;d]$ e com isto,

$$bkd^i(r) \in bHd^i(f) + bg'R[x;d] \subseteq gR[x;d].$$

Assim, $bkd^i(r) \in [g]$, para todo $i \geq 0$ e $k \in K$. Como $\delta(bkd^i(r)) \leq \delta(r) < \delta(g')$ então,

$$bkd^i(r) = 0 \tag{3.6}$$

para todo $k \in K$ e $i \geq 0$. Em particular, $bkr = 0$ e com isto,

$$0 = d(bkr) = d(b)kr + bd(k)r + bkd(r).$$

Como $d(k) \in K$, então $bkd(r) = bd(k)r = 0$ e segue que $d(b)kr = 0$. Desta forma,

$$0 = d(d(b)kr) = d^2(b)kr + d(b)d(k)r + d(b)kd(r).$$

Pela igualdade 3.6, $bkd(r) = 0$ e com isto,

$$0 = d(bkd(r)) = d(b)kd(r) + bd(k)d(r) + bkd^2(r).$$

Como $bkd^2(r) = bd(k)d(r) = 0$, então $d(b)kd(r) = 0$ e desta maneira, $d^2(b)kr = 0$. Usando o fato que $bkd^2(r) = 0$, obtemos que $d(b)kd^2(r) = 0$. Assim,

$$0 = d(d(b)kd^2(r)) = d^2(b)kd^2(r) + d(b)d(k)d^2(r) + d(b)kd^3(r) =$$
$$d^2(b)kd^2(r) + d(b)kd^3(r).$$

Desde que $bkd^3(r) = 0$, então $d(b)kd^3(r) = 0$ e com isto, $d^2(b)kd^2(r) = 0$.

Procedendo com o raciocínio acima obtemos $d^i(b)kd^j(r) = 0$ para todo $0 \leq i, j \leq t$, $k \in K$ e $t \geq 0$. Em particular, $d^i(b)kr = 0$, para todo $i \geq 0$ e $k \in K$.

Consideremos $A = \sum_{i\geq 0} Kd^i(b)K$ um d-ideal não-nulo de R. Pelo resultado obtido anteriormente $Ar = 0$. Seja $r = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Então,

$$0 = Ar = A(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0)$$

e segue que $Aa_i = 0$, para todo $i \in \{0, 1, \cdots, n\}$. Pelo Lema 1.1.6, $a_i = 0$, para todo $i \in \{0, 1, \cdots, n\}$ e, com isto, $r = 0$. Deste modo, $f = g'q$.

Além disto, se f' é o polinômio canônico de $[f]$, então $f = af'$, onde $a = lc(f)$. Usando o fato que $f \in Q_d(R)[x; d]g'$, não é difícil de verificar que $f' = g'q'$, para algum $q' \in Q_d(R)[x; d]$.

Seja $h \in [f]$ tal que $lc(h) = l$ e $\delta(h) = Min([f])$. Então,

$$h = lf' = l(g'q') = lq'g'.$$

Como $lq' \in Q_d(R)[x; d]$ então, pelo Lema 1.1.6, existe um d-ideal não-nulo M de R tal que $Mlq' \subseteq R[x; d]$. Assim, para cada $m \in M$,

$$bmh = bm(lq'g') = bg'mlq' = gmlq' \in gR[x; d].$$

Por sua vez, M é um d-ideal de R e então, $bd(m)h \in gR[x; d]$.

Note que, $d(m)h + md(h) = d(mh) = g'd(mlq')$ e com isto, $bd(mh) = gd(mlq') \in gR[x; d]$. Deste modo, $bmd(h) = bd(mh) - bd(m)h \in gR[x; d]$.

Suponhamos, por hipótese de indução, que $bmd^t(h) \in gR[x; d]$, para todo $t < i$ e $m \in M$. É evidente que $Md^t(lq') \subseteq R[x; d]$ e assim,

$$bd(md^t(h)) = bd(mg'd^t(lq')) = bg'd(md^t(lq')) = gd(md^t(lq')) \in gR[x; d].$$

Logo, $bmd^{t+1}(h) = bd(md^t(h)) - bd(m)d^t(h) \in gR[x; d]$ e com isto, $bmd^i(h) \in gR[x; d]$ para todo $m \in M$ e $i \geq 0$. Conseqüentemente, $h \in [g]$. $\square$

Lema 3.1.14. *Sejam $f, g \in \Gamma$. Então, $[f] = [g]$ se, e somente se, $f \in [g]$ e $\delta(f) = \delta(g)$.*

Demonstração. Pelo Lema 3.1.9, $[f]$ é um ideal R-disjunto de $R[x;d]$ que contém f como polinômio de grau mínimo. Logo, $[g]$ contém f como polinômio de grau mínimo e segue que $\delta(f) = \delta(g)$.

Reciprocamente, suponhamos que $f \in [g]$ e $\delta(f) = \delta(g)$. Pelo Lema 3.1.11, $[[g]] = [g]$. Por hipótese, f é um polinômio de grau mínimo em $[g]$ e, novamente pelo Lema 3.1.11, $[[g]] = [f]$. Logo, $[f] = [g]$. $\square$

Seja I um ideal não-nulo R-disjunto de $R[x;d]$ e consideremos $f \in I$ tal que $\delta(f) = Min(I)$ e $lc(f) = a$. Pelo Lema 3.1.11, a caracterização intrínseca de $[I]$ é dada por

$$[I] = [f] = \{h \in R[x;d]\colon \text{existe um } d\text{-ideal não-nulo } H \text{ de } R \text{ tal que } aHd^i(h) \subseteq fR[x;d], \text{ para todo } i \geq 0\}.$$

Definição 3.1.15. *Um polinômio $f \in \Gamma$ é irredutível em Γ se existem $c \in R, g \in \Gamma$ e $h \in R[x;d]$ tais que $0 \neq cf = gh$ ou $0 \neq cf = hg$ então $\delta(f) = \delta(g)$.*

Corolário 3.1.16. *Seja P um ideal não-nulo R-disjunto de $R[x;d]$. Então, P é primo se, e somente se, P é fechado e cada $f \in P$ tal que $\delta(f) = Min(P)$ é irredutível em Γ.*

Demonstração. Seja P um ideal primo não-nulo R-disjunto de $R[x;d]$ e consideremos $f \in P$ tal que $\delta(f) = Min(P)$. Pelos Lemas 3.1.11 e 3.1.9 temos que $f \in \Gamma$ e $[f] = [P]$ é um ideal R-disjunto de $R[x;d]$ que contém f como polinômio de grau mínimo. Pelo Corolário 3.1.4 e Lema 3.1.6, obtemos $P = [P]$.

Suponhamos que existem $c \in R$, $g \in \Gamma$ e $h \in R[x;d]$ tais que $0 \neq fc = gh$. Mostraremos que $[fc] = [f]$. Com efeito, pelo Lema 3.1.11, $[[f]] = [f]$. Note que $fc \in [f]$ e $\delta(fc) \leq \delta(f)$.

Se $\delta(fc) < \delta(f)$ então, $fc = 0$ o que contradiz a escolha de c. Assim, $\delta(fc) = \delta(f)$ e, pelo Lema 3.1.11, $[[f]] = [fc]$, com $fc \in \Gamma$.

Pelo Lema 3.1.9, $[g]$ é um ideal R-disjunto de $R[x;d]$ que contém g como polinômio de grau mínimo. Deste modo, $fc = gh \in [g]$. Pelo Lema 3.1.13 temos que $[fc] \subseteq [g]$.

Assim, $P = [P] = [f] = [fc] \subseteq [g]$ e, por sua vez, da maximalidade de P no conjunto dos ideais R-disjuntos de $R[x;d]$, obtemos que $P = [g]$. Logo, $\delta(f) = \delta(g)$ e portanto, f é irredutível em Γ.

Reciprocamente, sejam L um ideal primo R-disjunto de $R[x;d]$ tal que $L \supseteq P$ e $f \in P$. Desde que $f \in f_L Q_d(R)[x;d] \cap R[x;d]$, então $f = q' f_L$. Pelo Lema 1.1.6, existe um d-ideal não-nulo M de R tal que $Mq' \subseteq R[x;d]$. Se $\tau(L)Mf = 0$, então $f = 0$, pois $\tau(L)M \in \mathcal{I}_d$ e R é um anel d-primo. Assim, existem $c \in \tau(L)$ e $m \in M$ tais que $cmf \neq 0$. Pelo Lema 3.1.11, $[cf_L] = L$. Deste modo, $0 \neq cmf = cmq' f_L = cf_L mq'$. Como f é irredutível em Γ, então $\delta(f) = \delta(cf_L)$. Pelo Lema 3.1.14, $[f] = [cf_L]$. Logo, $P = L$ e portanto, P é primo. $\square$

Referências Bibliográficas

[1] AMITSUR, S. A., *Derivations in Simple Rings*, Proc. London Math. Soc., 7 (1957), 87-112.

[2] BELL, Allen D., *When are all Prime Ideals in an Ore Extension Goldie?*, Communications in Algebra, 13 (8) (1985), 1743-1762.

[3] CISNEROS, E.; FERRERO, M.; CONZÁLEZ, M. I., *Prime Ideals of Skew Polynomial Rings and Skew Laurent Polynomial Ring*, Math Journal of Okayama University 32 (1990), 61-72.

[4] FERRERO, M., *Radicals of Skew Polynomial Rings and Skew Laurent Polynomial Rings*, Math Journal of Okayama University 29 (1987), 119-126.

[5] FERRERO, M., *Prime and Principal Closed Ideals in Polynomial Rings*, Journal of Algebra 134 (1990), 45-59.

[6] FERRERO, M., *The Strongly Prime Radical of an Ore Extension*, Communications in Algebra, 17 (2) (1989), 351-376.

[7] FERRERO, M.; KISHIMOTO K., *On Differential Rings and Skew Polynomials*, Communications in Algebra, 13 (2) (1985), 285-304.

[8] FERRERO, M.; MATCZUK, J., *Prime Ideals in Skew Polynomial Rings of Derivation Type*, Communications in Algebra, 18 (3) (1990), 689-710.

[9] LAM, T. Y., *A first course in noncommutative rings*, Springer-Verlag, 1991.

[10] LAM, T. Y.; LEROY, A.; MATCZUK, J., *Primeness, Semiprimeness and Prime Radical of Ore Extensions*, Communications in Algebra, 25 (8) (1997), 2459-2506.

[11] LEROY, A.; MATCZUK, J., *Derivations et Automorphismes Algebraiques d'anneaux Premiers*, Communications in Algebra. 13 (6), (1985), 1245-1266.

[12] MATCZUK, J., *Extended Centroids of Skew Polynomial Rings*, Math Journal of Okayama University 30 (1988), 13-20.

[13] MONTGOMERY, S., *Fixed rings of finite automorphism groups of associative rings*, Lecture Notes in Math. Springer-Verlag, 1980.

[14] PEARSON, K. R.; STEPHENSON, W.; WATTERS, J. F., *Skew Polynomials and Jacobson Rings*, Proc. London Math. Soc. (3) 42 (1981), 559-576.