Universidade Federal do Rio Grande do Sul

Ideais Primos e Fechados em Extensões de Anéis

por
Alvino Alves Sant'Ana

dezembro de 1992.

dedico este trabalho à Marilaine e ao Victor.

Dissertação submetida ao Curso de Pós-Graduação em Matemática da Universidade Federal do Rio Grande do Sul, sob orientação do Prof.Dr. Miguel Angel Alberto Ferrero, como requisito parcial para obtenção do grau de Mestre.

RESUMO

Nesta dissertação, estudamos ideais primos e ideais fechados em $S = R[E]$, onde S é uma extenção livre centralizante do anel primo R. Demonstramos um teorema, devido a M. FERRERO, que estabelece uma correpondência biunívoca entre os ideais fechados $R-disjuntos$ de $T[E]$ e $R[E]$, e os ideais de $C[E]$, onde T é um anel de quocientes à direita de R, e C é o centróide extendido de R. Além disso, esta correspondência preserva a propriedade de um ideal ser primo. Como aplicação deste resultado, entre outros, obtemos uma decomposição primária de um ideal fechado $R - disjunto$ do anel de polinômios a várias indeterminadas sobre R.

ABSTRACT

In this thesis, we study prime ideals and closed ideals in $S = R[E]$, where S is a centralizing free extension of the prime ring R. We prove a theorem, due to M. FERRERO, that establishes a 1-1 correspondence betweem the $R - disjoint$ closed ideals of $T[E]$ and $R[E]$, and the ideals of $C[E]$, where T is a ring of right quotients of R, and C is the extended centroid of R. Furthermore, this correspondence preserves the property for an ideal to be prime. As an application, among others, one gets a primary decomposition for the $R - disjoint$ closed ideals of the polynomial rings in several variables over R.

Índice

Introdução

Esta dissertação trata de ideais primos em extensões livres centralizantes de um anel R, segundo [6], de M.Ferrero. Aqui, estudamos uma classe de ideais mais geral, a dos ideais fechados e, como caso particular, se obtém resultados sobre ideais primos. Dado $S = R[E]$ uma extensão livre centralizante do anel primo com unidade R (S é um R-módulo livre e E é uma base centralizante de S sobre R, tal que $1 \in E$), consideramos $Q[E]$ e $C[E]$, onde Q é o anel completo de quocientes à direita de R, e C é o centróide extendido de R. Então, obtemos uma correspondência biunívoca entre os ideais fechados de $Q[E]$ e de $R[E]$ e os ideais de $C[E]$. A correspondência preserva a propriedade de um ideal ser primo.

Como conseqüência desta correspondência, entre outros, obtemos um resultado original, que é a decomposição primária dos ideais fechados do anel de polinômios a várias indeterminadas. Esta decomposição generaliza a representação de um ideal principal fechado do anel de polinômios a uma indeterminada como intersecção finita de ideais principais fechados associados à potências de ideais primos $R-disjuntos$, obtida em [5] (teorema 3.1).

Os ideais fechados também têm sido usados para estudar ideais primos em extensões de Öre ([3], [9] e [13]).

Este tema, na literatura, está apresentado de modo diferente. Os resultados sobre ideais fechados e primos em extensões livres centralizantes são obtidos posteriormente aos resultados em anéis de polinômios, como uma generalização. Aqui, desenvolvemos diretamente os resultados em extensões livres centralizantes e obtemos, como aplicação, os resultados em anéis de polinômios, destacando específicas particularidades deste caso.

No capítulo 1, apresentamos alguns tópicos que são pré-requisitos para a leitura do que segue. Dividimos este capítulo em três secções. Na primeira, revisamos alguns conceitos e mostramos algumas caracterizações de ideais e anéis primos. Noutra secção, construímos o anel completo de quocientes à direita de R. Encerramos este capítulo, tratando de extensões livres centralizantes de R. Aqui mostramos que, por passagem ao quociente, neste trabalho, sempre podemos supor R um anel primo. Ao final, damos alguns exemplos de extensões livres centralizantes de R.

No capítulo 2, estudamos os ideais primos $R-disjuntos$ e fechados de $S = R[E]$, onde S é uma extensão livre centralizante do anel primo com unidade R. Caracterizamos o fecho $[I] = \{b \in S \mid \exists 0 \neq H \lhd S \ : \ bH \subseteq I\}$ de um ideal $R-disjunto$ I de S, como o único ideal fechado de S que contém I e tem a mesma minimalidade de I (corolário 2.1.5). Dado um ideal primo $R-disjunto$ P de S, P é fechado ($P = [P]$). Em seguida, particularizamos os resultados ao anel de polinômios a uma indeterminada $R[X]$. Sejam I um ideal $R-disjunto$ de $R[X]$ e f um polinômio qualquer de mínimo grau no ideal I. Então, temos que $[I] = [f] = \{g \in R[X] \mid \exists 0 \neq H \lhd R \ : \ gHa \subseteq R[X]f\}$, onde $a = lc(f)$ (corolário 2.2.9). Assim, caracterizamos o fecho $[I]$ do ideal I através de um polinômio de mínimo grau em I. Aqui, o conceito de minimalidade é com respeito ao grau dos polinômios e não com respeito ao suporte dos elementos, considerado para o caso mais geral $S = R[E]$. Também caracterizamos os ideais $R-disjuntos$ de $R[X]$ que são primos (teorema 2.2.11).

No capítulo 3, é obtida a correspondência biunívoca entre os ideais fechados de $Q[E]$ e de $R[E]$ e os ideais de $C[E]$, citada acima. Além disso, dado um anel de quocientes à direita T de R (T é um subanel de Q que contém R), temos que a mesma correspondência está estabelecida para os ideais fechados de $T[E]$. Ela associa o ideal fechado I de $R[E]$ com o ideal fechado I^* de $T[E]$ e o ideal K de $C[E]$, se $I^* \cap R[E] = I$ e $I^* = Q[E]K \cap T[E]$ (teorema 3.1.5). Esta correspondência preserva a propriedade de um ideal ser primo (teorema 3.1.7).

A seguir, damos dois caminhos para representar um ideal primo $R-disjunto$ P de $R[X]$. O primeiro é uma conseqüência da correspondência acima, via polinômios irredutíveis de $C[X]$ (corolário 3.2.3). O segundo caminho, é intrínseco no anel $R[X]$, considerando polinômios completamente irredutíveis em $R[X]$ (teorema 3.2.10).

No capítulo 4, estudamos, numa primeira secção, a decomposição dos ideais principais fechados do anel de polinômios a uma indeterminada sobre R, segundo [5]. Os resultados obtidos na última secção são originais. O principal, é uma generalização do que estudamos na secção anterior, que é a decomposição primária de um ideal fechado do anel de polinômios a várias indeterminadas sobre R (teorema 4.2.12). Para isto, obtemos alguns resultados que generalizam conceitos e propriedades dos anéis comutativos Noetherianos.

Finalmente, a notação $A \subset B$, significa que o conjunto A está contido estritamente no conjunto B.

Capítulo 1

Preliminares

1.1 Anéis Primos e Ideais Primos

Seja R um anel qualquer. A seguir, lembramos algumas definições que utilizaremos nesta dissertação, particularmente sobre ideais primos de R. Daremos, também, algumas caracterizações do conceito de ideal primo.

Definição 1.1.1 *Seja P um ideal de R. P é chamado ideal primo de R se satisfaz a seguinte propriedade: se A e B são ideais de R tais que $AB \subseteq P$, então $A \subseteq P$ ou $B \subseteq P$.*

O teorema 1.1.2 estabelece propriedades equivalentes à definição 1.1.1. Sua demonstração pode ser encontrada em [15] (teorema 4.3).

Teorema 1.1.2 *Sejam R um anel e P um ideal de R. As seguintes condições são equivalentes:*
(i) P é um ideal primo de R
(ii) sejam $a, b \in R$ tais que $aRb \subseteq P$, então $a \in P$ ou $b \in P$
(iii) se (a) e (b) são ideais principais de R tais que $(a)(b) \subseteq P$, então $a \in P$ ou $b \in P$
(iv) se U, V são ideais à direita de R tais que $UV \subseteq P$, então $U \subseteq P$ ou $V \subseteq P$
(v) se U, V são ideais à esquerda de R tais que $UV \subseteq P$, então $U \subseteq P$ ou $V \subseteq P$

Definição 1.1.3 *Um anel R é chamado anel primo se o ideal $0 = \{0\}$ é um ideal primo de R.*

Corolário 1.1.4 *As seguintes condições são equivalentes:*
(i) R é um anel primo, isto é, dados A e B dois ideais de R tais que $AB = 0$, então $A = 0$ ou $B = 0$
(ii) sejam $a, b \in R$ tais que $aRb = 0$, então $a = 0$ ou $b = 0$
(iii) seja H um ideal não nulo de R. Se $aHb = 0$ então $a = 0$ ou $b = 0$

Demonstração : (ii)$\Rightarrow$ (iii) Como $aHb = 0$, $aHRb = 0$. Se $b \neq 0$, temos, por hipótese, que $aH = 0$ (se $h \in H$, $ahRb = 0$ e $ah = 0$, por (ii)). Logo, $aRH = 0$. Como $H \neq 0$, existe $0 \neq h \in H$ e obtemos $aRh = 0$ (com $h \neq 0$). Conseqüentemente, $a = 0$. As outras implicações são evidentes.

Em 1.1.2 e 1.1.4 consideramos produtos de ideais contidos em um ideal P, ou produto de R por elementos à direita e à esquerda contido em P ($aRb \subseteq P$). Vejamos o

Lema 1.1.5 *Sejam P um ideal primo de R, I um ideal de R e $b \in R$. Se $bI \subseteq P$ e $I \not\subseteq P$ então $b \in P$.*

Demonstração : Desde que $I \not\subseteq P$, existe $c \in I \setminus P$. Mas $bRc \subseteq P$, pois $Rc \subseteq I$. Como $c \notin P$, temos que $b \in P$, por 1.1.2(ii).

Para simplificar este trabalho, por passagem ao quociente, consideraremos R um anel primo (capítulo 2). Assim, vejamos o lema a seguir, que caracteriza o conceito de anel primo, para anéis quocientes.

Lema 1.1.6 *Seja P um ideal de R. Então o anel $\frac{R}{P}$ é primo se e somente se P é um ideal primo de R.*

Demonstração : Seja $\overline{R} = \frac{R}{P}$ e mostremos que $\overline{0}$ é um ideal primo de $\overline{R}$. Sejam $\overline{I}$ e $\overline{J}$ ideais de $\overline{R}$ tais que $\overline{I}\,\overline{J} \subseteq \overline{0}$. Então $\overline{IJ} \subseteq \overline{0}$ e, conseqüentemente, $IJ \subseteq P$, onde I e J são ideais de R tais que $\frac{I}{P} = \overline{I}$ e $\frac{J}{P} = \overline{J}$. Por hipótese, $I \subseteq P$ ou $J \subseteq P$, logo $\overline{I} = \overline{0}$ ou $\overline{J} = \overline{0}$. Assim, $\overline{0}$ é um ideal primo de $\overline{R}$. Reciprocamente, sejam I e J ideais de R tais que $IJ \subseteq P$, portanto $\overline{IJ} \subseteq \overline{0}$. Segue que, $\overline{I} = \overline{0}$ ou $\overline{J} = \overline{0}$ e obtemos $I \subseteq P$ ou $J \subseteq P$. Logo, P é um ideal primo de R. A prova está completa.

Lema 1.1.7 *Seja P um ideal de R. P é um ideal primo de R se e somente se para quaisquer ideais I e J de R tais que $P \subseteq I$, $P \subseteq J$ e $IJ \subseteq P$ então $I = P$ ou $J = P$.*

Demonstração : Se P é um ideal primo de R, desde que $IJ \subseteq P$, temos $I \subseteq P$ ou $J \subseteq P$ e segue, por hipótese, que $I = P$ ou $J = P$. Reciprocamente, sejam $a, b \in R$ tais que $(a)(b) \subseteq P$ e mostremos que $a \in P$ ou $b \in P$. Sejam $I = (P, a)$ e $J = (P, b)$, onde (K, α) é o ideal gerado por K e α, para qualquer $\alpha \in R$ e K ideal de R. Então $P \subseteq I$ e $P \subseteq J$. Por hipótese, concluímos que $I = P$ ou $J = P$. Conseqüentemente, $a \in P$ (pois $a \in I$) ou $b \in P$. Logo, P é um ideal primo de R, o que completa a prova.

O lema a seguir relaciona os conceitos de anel primo e ideal primo entre os anéis R e $R[X]$.

Lema 1.1.8 *As seguintes afirmações são verdadeiras:*
(i) R é um anel primo se e somente se $R[X]$ é um anel primo.
(ii) Seja I um ideal de R. I é primo se e somente se $I[X]$ é um ideal primo de $R[X]$.

Demonstração : (i) Suponhamos que R é um anel primo e sejam I e J dois ideais não nulos de $R[X]$ tais que $IJ = 0$. Para $f \in I$, $lc(f)$ denota o coeficiente dominante de f, e definimos $\tau(I) = \{a \in R \mid \exists 0 \neq f \in I : lc(f) = a\}$. Analogamente, definimos $\tau(J)$. É fácil ver que $\tau(I)$ e $\tau(J)$ são dois ideais não nulos de R. Como $IJ = 0$, $\tau(I)\tau(J) = 0$, o que contradiz o fato de R ser um anel primo. Reciprocamente, sejam I e J ideais de R satisfazendo $IJ = 0$. Portanto, $0 = IJ[X] = I[X]J[X]$ (ver lema 1.3.2). Assim, temos que $I[X] = 0$ ou $J[X] = 0$, e conseqüentemente $I = 0$ ou $J = 0$. Logo, R é um anel primo.

(ii) Conseqüência imediata de (i) por passagem ao quociente.

1.2 Anel Completo de Quocientes

Nesta secção construímos o anel completo de quocientes à direita Q de um anel primo R (ver cap. IX de [21] e secção 4.3 de [12]). No caso particular de R ser um domínio de integridade (comutativo) Q coincide com o corpo de frações de R. Ao final desta secção definimos o anel de Martindale de R.

Seja R um anel com unidade. Um ideal (bilátero) U de R, será denotado por $U \lhd R$. Começamos definindo ideal denso à direita de R.

Definição 1.2.1 *Seja D um ideal à direita de R. D é dito um ideal denso à direita se para quaisquer $0 \neq r_1 \in R$ e $r_2 \in R$ existe $r \in R$ tal que $r_1 r \neq 0$ e $r_2 r \in D$.*

Observemos que, se D é um ideal denso à direita de R, então D é um ideal não nulo. De fato, tomando $0 \neq r_1 = r_2 \in R$ na definição acima, obtemos que existe $r \in R$ tal que $0 \neq r_1 r \in D$.

Denotaremos por $\mathcal{D}$ o conjunto de todos os ideais densos à direita de R e, por (D, f), o homomorfismo de R-módulos à direita $f : D \rightarrow R$, onde $D \in \mathcal{D}$. Seja $\mathcal{T} = \{(D, f) \mid D \in \mathcal{D}\}$. Vejamos, a seguir, como determinar se um ideal $U \lhd R$, é denso à direita. Da definição anterior, obtemos o

Lema 1.2.2 *Um ideal U de R é denso à direita se e somente se para qualquer $r \in R$ com $rU = 0$ temos que $r = 0$.*

Demonstração : Assumimos que dado $r \in R$ tal que $rU = 0$ então $r = 0$, onde $U \lhd R$. Seja $r_1 \in R$.Se $r \neq 0$, por hipótese existe $s \in U$ tal que $rs \neq 0$. Desde que $U \lhd R, r_1 s \in U$, e por definição $U \in \mathcal{D}$. Reciprocamente, se $U \in \mathcal{D}$ então o resultado segue, tomando $r_2 = 1$ na definição 1.2.1. O lema está demonstrado.

Assim, se R é um anel primo, todo ideal não nulo de R é denso à direita. De fato, seja $0 \neq U \lhd R$, tal que $rU = 0$, onde $r \in R$. Então $r = 0$ ($rU = rU1$ e R é primo) e pelo lema 1.2.2 temos que $U \in \mathcal{D}$.

Daremos agora três propriedades importantes que $\mathcal{D}$ satisfaz.

Lema 1.2.3 *Sejam $D, D' \in \mathcal{D}$. Então:*
(i) $(D \cap D') \in \mathcal{D}$
(ii) $DD' \in \mathcal{D}$

Demonstração : (i) Sejam $0 \neq r_1 \in R$ e $r_2 \in R$. Como $D \in \mathcal{D}$, podemos encontrar $r \in R$ tal que $r_1r \neq 0$ e $r_2r \in D$. Também $D' \in \mathcal{D}$, logo existe $r' \in R$ tal que $(r_1r)r' \neq 0$ e $(r_2r)r' \in D'$. Então $r_2rr' \in (D \cap D')$ e conseqüentemente $(D \cap D') \in \mathcal{D}$.

(ii) Temos que $DD' = (DR)D' = D(RD')$. Sejam $0 \neq r_1, r_2 \in R$. Como $D \in \mathcal{D}$, existe $r \in R$ tal que $r_1r \neq 0$ e $r_2r \in D$. Por outro lado, $0 \neq (RD') \lhd R$, portanto existe $t \in RD'$ satisfazendo $r_1rt \neq 0$ e $r_2rt \in RD'$ (ver 1.2.2, já que $RD' \in \mathcal{D}$). Se $t = \sum_i s_id_i$ onde $d_i \in D'$ e $s_i \in R$, temos que $r_1(r\sum_i s_id_i) \neq 0$ e $\sum_i(r_2r)(s_id_i) \in D(RD')$. Logo $DD' \in \mathcal{D}$, o que demonstra o lema.

Em particular, se R é primo, $D \in \mathcal{D}$ e $0 \neq H \lhd R$, então $DH \in \mathcal{D}$.

Antes de provar a terceira propriedade de $\mathcal{D}$, consideremos a seguinte

Definição 1.2.4 *Sejam $U, V \in \mathcal{D}$ e $(U,f),(V,g) \in \mathcal{T}$. Dizemos que (U,f) é equivalente a (V,g) se existe $W \in \mathcal{D}$ tal que $W \subseteq (U \cap V)$ satisfazendo $(W,f|_W) = (W,g|_W)$.*

É fácil ver que a relação acima é uma relação de equivalência sobre $\mathcal{T}$. Seja Q o conjunto de todas as classes de equivalência determinadas por esta relação. Dado $(U,f) \in \mathcal{T}$, denotamos por $[U,f]$ a classe de equivalência de (U,f). Vejamos agora a terceira propriedade que destacamos de $\mathcal{D}$, que nos permitirá definir operações em Q, a fim de construirmos um anel.

Lema 1.2.5 *Sejam $(U,f) \in \mathcal{T}$ e $V \in \mathcal{D}$. Então $f^{-1}(V) \in \mathcal{D}$.*

Demonstração : Sejam $0 \neq r_1, r_2 \in R$. Sabendo que $U \in \mathcal{D}$, existe $r \in R$ tal que $r_1r \neq 0$ e $r_2r \in U$. Consideremos agora $r_1r \neq 0$ e $f(r_2r) \in R$. Do fato de que $V \in \mathcal{D}$, temos que existe $s \in R$ tal que $r_1rs \neq 0$ e $f(r_2r)s \in V$. Mas $f(r_2rs) = f(r_2r)s \in V$, então $r_2rs \in f^{-1}(V)$. Segue que $f^{-1}(V) \in \mathcal{D}$.

Agora podemos definir em Q as operções de adição e multiplicação como segue:

Definição 1.2.6 *Dados $[U,f],[V,g] \in Q$, definimos as seguintes operações:*
(i) $[U,f]+[V,g] = [U \cap V, f+g]$
(ii) $[U,f][V,g] = [g^{-1}(U), f \circ g]$

Verifiquemos que estas operações estão bem definidas. Sejam $[U,f] = [U',f']$ e $[V,g] = [V',g']$ pertencentes à Q. Assim, existem $W, W' \in \mathcal{D}$ tais que $W \subseteq U \cap U'$ e $W' \subseteq V \cap V'$ satisfazendo $f|_W = f'|_W$ e $g|_{W'} = g'|_{W'}$. Conseqüentemente,

$f+g(a) = f'+g'(a)$,para todo $a \in W \cap W'$, ou seja, $(W \cap W', f+g) = (W \cap W', f'+g')$. Como $W \cap W' \subseteq U \cap V \cap U' \cap V'$, obtemos que $[U \cap V, f+g] = [U' \cap V', f'+g']$. Portanto a adição está bem definida.

Para verificar se a multiplicação está bem definida, tomamos $a \in g^{-1}(U) \cap (g')^{-1}(U') \cap W \cap W'$. Assim, $g(a) \in U, g'(a) \in U'$ e $g(a) = g'(a)$. Obtemos que $f(g'(a)) = f'(g'(a))$. Mas $a \in W'$, logo $f(g(a)) = f(g'(a))$.

Conseqüentemente, $f \circ g(a) = f(g(a)) = f(g'(a)) = f'(g'(a)) = f' \circ g'(a)$ e, agora, é fácil ver que $[U, f][V, g] = [U', f'][V', g']$.

Mostremos que Q, munido destas operações é um anel.

Proposição 1.2.7 *$(Q, +, \cdot)$ é um anel.*

Demonstração : Sejam $[U, f], [V, g], [W, h] \in Q$.

(i)associatividade da adição
$([U, f] + [V, g]) + [W, h] = [U \cap V, f+g] + [W, h] = [U \cap V \cap W, (f+g)+h] =$
$= [U \cap V \cap W, f + (g+h)] = [U, f] + [V \cap W, g+h] = [U, f] + ([V, g] + [W, h])$

(ii)comutatividade da adição
$[U, f] + [V, g] = [U \cap V, f+g] = [V \cap U, g+f] = [V, g] + [U, f]$

(iii)$[R, 0]$ é o elemento neutro da adição, onde 0 denota a aplicação $0 : R \longrightarrow R$ tal que $0(r) = 0$ para cada $r \in R$. Temos:
$[R, 0] + [U, f] = [R \cap U, 0 + f] = [U, f]$

(iv)$[U, -f]$ é o elemento simétrico de $[U, f]$ em relação à adição, pois
$[U, -f] + [U, f] = [U, -f+f] = [U, 0] = [R, 0]$

(v)A associatividade da multiplicação mostra-se com argumentos análogos aos usados em (i).

(vi)Para provar que a multiplicação é distributiva em relação à adição, tomamos $L = g^{-1}(U) \cap h^{-1}(U) \cap V \cap W$ e é fácil ver que
$[L, f \circ (g+h)] = [L, f \circ g + f \circ h]$ e segue a distributividade.

Definição 1.2.8 *O anel Q é chamado de anel completo (ou maximal) de quocientes à direita de R.*

Proposição 1.2.9 *Seja R um anel com unidade e Q o anel completo de quocientes à direita de R. Então $R \subseteq Q$.*

Demonstração : Consideremos o homomorfismo de anéis $\varphi : R \longrightarrow Q$ definido por $\varphi(a) = [R, a_l]$ para todo $a \in R$, onde $a_l : R_R \longrightarrow R_R$ é definido por $a_l(r) = ar$

para cada $r \in R$ (multiplicação à esquerda). Verifiquemos que φ é um monomorfismo. Sejam $a, b \in R$. Então temos que $(a+b)_l = a_l + b_l$, pois dado $r \in R$, $(a+b)_l(r) = (a+b)r = ar + br = a_l(r) + b_l(r) = (a_l + b_l)(r)$. Logo $\varphi(a+b) = (a+b)_l = a_l + b_l = \varphi(a) + \varphi(b)$. Analogamenete $(ab)_l = a_l \circ b_l$ e assim, $\varphi(ab) = \varphi(a)\varphi(b)$. Concluímos que φ é um homomorfismo de R em Q.

Suponhamos que $[R, a_l] = 0$ para algum $a \in R$. Segue que $ar = 0$ para todo $r \in R$ e então $a = 0$ pois $1 \in R$. Isto é, Ker(φ)=0 e então φ é injetivo. Logo $R \simeq \varphi(R) \subseteq Q$. A prova está completa.

Para simplificar a notação, consideremos sempre $R \subseteq Q$, identificando cada $a \in R$ com $[R, a_l] \in Q$.

Lema 1.2.10 *Seja $(U, f) \in \mathcal{T}$. Então para qualquer $u \in U$, temos que $f \circ u_l = (f(u))_l$. Em particular, $[U, f][R, u_l] = [R, (f(u))_l]$.*

Demonstração : Como $f : U_R \to R_R$, então para cada $u \in U$ e $x \in R$ temos que $f \circ u_l(x) = f(u_l(x)) = f(ux) = (f(u))x = (f(u))_l(x)$. Assim, $f \circ u_l = (f(u))_l$. Agora, $[U, f][R, u_l] = [u_l^{-1}(U), f \circ u_l] = [R, f \circ u_l] = [R, (f(u))_l]$.

Lema 1.2.11 *Seja $q \in Q$. Seja $(U, f) \in \mathcal{T}$ tal que $q = [U, f]$. Então $f(r) = qr$, para todo $r \in U$.*

Demonstração : Sejam $q = [U, f] \in Q$ e $r \in U$. Temos que $qr = qr_l = [U, f][R, r_l] = [R, (f(r))_l] = \varphi(f(r))$. Assim, obtemos que $qr = f(r)$, para todo $r \in U$.

A seguinte proposição nos mostra uma propriedade importante de Q, que será freqüentemente utilizada.

Proposição 1.2.12 *Seja $q \in Q$. Seja $(U, f) \in \mathcal{T}$ tal que $q = [U, f]$. Então $qU \subseteq R$.*

Demonstração : Por 1.2.11 temos que $qU \subseteq R$.

Corolário 1.2.13 *Para quaisquer $q_1, \ldots\ldots, q_n \in Q$, existe $U \in \mathcal{D}$ tal que $q_iU \subseteq R$, para cada $i \in \{1, \ldots, n\}$.*

Demonstração : Para cada $i \in \{1, \ldots, n\}$ consideramos $U_i \in \mathcal{D}$ tal que $q_iU_i \subseteq R$. Então $U = \cap_{i=1}^n U_i$ satisfaz o corolário.

Corolário 1.2.14 *Seja U um ideal denso à direita de R e seja $f : U \to R$ um homomorfismo de R-módulos à direita. Então existe $q \in Q$ tal que $f(r) = qr$ para qualquer $r \in U$.*

Demonstração : Tomemos $q = [U, f] \in Q$ e aplicamos 1.2.11.

Lema 1.2.15 *Seja $q \in Q$ e $U \in \mathcal{D}$. Se $qU = 0$ então $q = 0$.*

Demonstração : Seja $q = [V, f] \in Q$. Por hipótese $q(U \cap V) = 0$. logo, por 1.2.11, $f\,|_{U\cap V} = 0$. Logo $q = [V, f] = [U \cap V, f\,|_{U\cap V}] = [U \cap V, 0] = [R, 0] = 0$.

Consideramos agora T um subanel de Q que contém R e vejamos que, se R é primo, T é um anel primo. Os subanéis de Q que contém R são chamados de Anéis de Quocientes à Direita de R. Vejamos a

Proposição 1.2.16 *Seja R um anel primo. Então todo anel de quocientes à direita de R é primo. Em particular, Q é um anel primo.*

Demonstração : Seja T um anel de quocientes à direita de R. Suponhamos que existam $q \neq 0$ e $p \neq 0$ em T tais que $qTp = 0$. De 1.2.12, existem $U, V \in \mathcal{D}$ satisfazendo $qU \subseteq R$ e $pV \subseteq R$, pois $T \subseteq Q$. Do fato de q e p serem não nulos, existem $u \in U$ e $v \in V$ com $qu \neq 0$ e $pv \neq 0$. Como R é primo, temos $0 \neq (qu)R(pv) \subseteq (qRp)v = 0$, uma contradição. Logo não existem tais elementos q e p em T, e portanto T é um anel primo. A prova está completa.

O conjunto dos elementos $q \in Q$ tais que $qr = rq$ para cada $r \in R$ é denominado Centralizador de R em Q e denotado por $V_Q(R)$. O centro de Q é o conjunto $C = \{q \in Q \mid qp = pq \ \forall p \in Q\}$. Vejamos o

Lema 1.2.17 *Seja $q = [U, f] \in Q$. As seguintes condições são equivalentes:*
(i) $q \in C$
(ii) Existe um ideal I de R tal que $U \subseteq I$ e $I \in \mathcal{D}$, e um homomorfismo f^* de R-bimódulos $f^* : I \to R$ satisfazendo $f^*\,|_U = f$
(iii) $q \in V_Q(R)$
Além disso, se (ii) é verificado, então $f^*(a) = qa$, para todo $a \in I$.

Demonstração : (i)$\Rightarrow$(iii) Imediato.
(iii)$\Rightarrow$(ii) Seja $q = [U, f] \in V_Q(R)$. Consideremos o ideal $I = RU$. É claro que $I = RU \in \mathcal{D}$, desde que $U \in \mathcal{D}$. Definimos $f^* : RU \to Q$ por $f^*(\alpha) = q\alpha$. O

resultado segue, desde que $f^*(U) \subseteq R$. De fato, seja $\alpha = \sum_{i=1}^{n} r_i u_i \in RU$. Então, como $q \in V_Q(R)$, $f^*(\alpha) = q\sum_{i=1}^{n} r_i u_i = \sum_{i=1}^{n} r_i q u_i$. Agora, por 1.2.12, temos que $f^*(\alpha) \in R$. Logo $f^*(U) \subseteq R$.

(ii)$\Rightarrow$(i) Seja $p = [V, g] \in Q$ um elemento qualquer de Q. Queremos mostrar que $qp = pq$. De fato, $qp = [I, f^*][V, g] = [g^{-1}(I), f^* \circ g]$. Tomamos $x = uv \in F^2$, onde $F = g^{-1}(I)$, temos:

$$f^*(g(uv)) = f^*(g(u)v) = g(u)f^*(v) = g(uf^*(v)) = g(f^*(uv)).$$

Assim, $f^* \circ g\,|_{F^2} = g \circ f^*\,|_{F^2}$ e segue que $qp = pq$, já que $F^2 \in \mathcal{D}$ (por 1.2.5 e 1.2.3) e que $f^* \circ g$ e $g \circ f^*$ são homomorfismos de R-módulos à direita de R. Logo $q \in C$.

Para completar a prova, suponhamos que $I \lhd R$ satisfaz as condições (ii). Conseqüentemente, $q = [U, f] = [I, f^*]$. Seja $a \in I$. Temos, por 1.2.9 e 1.2.10,

$$qa = [I, f^*][R, a_l] = [a_l^{-1}(I), f^* \circ a_l] = [a_l^{-1}(I), (f^*(a))_l] = [R, (f^*(a))_l] = f^*(a) \;,$$

o que completa a prova.

De agora em diante consideremos sempre R um anel primo. Mostremos a seguir que C é um corpo. Sejam $0 \neq a \in C$ e $b \in Q$. Suponhamos que $ab = 0$. Então $0 = Qab = aQb$. Como Q é primo, $b = 0$. Logo nenhum elemento de C é um divisor de zero em Q. Em particular, C é um domínio de integridade.

Observamos que se $c \in C$ então por 1.2.17 existem $U \lhd R$ e f, um homomorfismo de R-bimódulos, tais que $c = [U, f]$.

Proposição 1.2.18 *Se R é primo, então C é um corpo.*

Demonstração : Basta verificar que todo $0 \neq c \in C$ tem inverso multiplicativo em C. Sejam $0 \neq c \in C$ e $U \lhd R$ tais que $cU \subseteq R$ (proposição 1.2.12). Assim, por 1.2.15, $0 \neq cU \lhd R$ e a função $g : cu \mapsto u$ de cU em R induz um elemento $d = [cU, g] \in Q$. Pelo lema 1.2.11, temos $d(ca) = g(ca) = a$ para todo $a \in U$. Logo $(dc - 1)U = 0$ e, por 1.2.15, $dc = 1$, o que completa a prova.

O corpo C é chamado de Centróide Extendido de R. O subanel S de Q gerado por R e C, isto é, $S = RC$ é dito Clausura Central de R.

A proposição a seguir nos mostra que todo anel de quocientes à direita de R, que contém a clausura central de R, tem como centro exatamente o centro de Q.

Proposição 1.2.19 *Seja T um anel de quocientes à direita de R que contém S. Então $Z(T) = C$, onde $Z(T)$ denota o centro de T.*

Demonstração : Seja $c \in Z(T)$. Portanto $ct = tc$ para todo $t \in T$. Então, como $R \subseteq T$, $cr = rc$ para todo $r \in R$. Logo $c \in V_R(Q)$ e, pelo lema 1.2.17, $c \in C$. Assim $Z(T) \subseteq C$. A outra inclusão é óbvia, desde que $1 \in R$ e portanto $Z(T) = C$.

Um exemplo de anel de quocientes à direita de R, é o anel de Martindale definido por:

$$Q_{MART} = \{q \in Q \mid \exists\, 0 \neq U \lhd R \text{ tal que } qU \subseteq R\}.$$

É claro que $Z(Q_{MART}) = C$, pois $S \subseteq Q_{MART}$.

A construção do anel Q_{MART} pode ser feita de maneira independente de Q, tomando a família $\mathcal{I} = \{U \mid 0 \neq U \lhd R\}$ em vez de $\mathcal{D}$ considerada aqui, e $\mathcal{T}' = \{f : U_R \to R_R \mid U \in \mathcal{I} \text{ e } f \text{ é um homomorfismo}\}$ em vez de $\mathcal{T}$.
(ver secção 2 de [14]).

1.3 Extensões Livres Centralizantes

Nesta secção começamos definindo o que é uma extensão livre centralizante de um anel R com unidade. O objetivo principal desta dissertação é estudar ideais primos em tais extensões.

Ainda nesta secção, veremos alguns exemplos de extensões livres centralizantes.

Seja R um anel com unidade. Uma extensão S de R é dita uma extensão livre centralizante de R se S é um R-módulo livre e existe uma base $E = \{e_i\}_{i\in\Omega}$ de elementos R-centralizantes tais que a unidade $1 \in E$. Ou seja, $S = \sum_{i\in\Omega} \oplus Re_i$ e $xe_i = e_ix$ para todo $x \in R$ e qualquer $i \in \Omega$, e existe $i_0 \in \Omega$ tal que $e_{i_0} = 1$. Denotaremos este fato por $S = R[E]$.

Assim, qualquer $a \in S$ pode ser escrito univocamente como soma finita $a = \sum_{i\in\Omega} a_ie_i$, onde $a_i \in R$ para todo $i \in \Omega$.

O e-ésimo coeficiente de a será denotado por $a(e)$. Por exemplo, para o elemento a acima, $a(e_i) = a_i$ para todo $i \in \Omega$.

Definimos o suporte de a como sendo o seguinte conjunto:
$sup(a) = \{e \in E \mid a(e) \neq 0\}$. É claro que $sup(a)$ é um subconjunto finito de E, para qualquer $a \in S$.

Lema 1.3.1 *Sejam $S = R[E]$ $(E = \{e_i\}_{i\in\Omega})$ uma extensão livre centralizante de R e H um ideal de R. Então HS é um ideal de S.*

Demonstração : É claro que $0 \in HS$ e que HS é fechado para diferença e produto. Dados $u = \sum_i r_ie_i \in S$ e $h \in H$, temos que $uh = \sum_i r_ihe_i \in H[E]$, desde que $H \lhd R$. Mas $H[E]R[E] \subseteq HR[E] = HS$, e $HS^2 \subseteq HS$. Conseqüentemente, HS é um ideal de S.

Lema 1.3.2 *Sejam R um anel com unidade e $S = R[E]$ $(E = \{e_i\}_{i\in\Omega})$ uma extensão livre centralizante de R. Dados dois ideais I e J de R, então:*
(i) $I[E]$ é um ideal de S
(ii) $I[E]J[E] = IJ[E]$

Demonstração : (i) Imediato.

(ii) Desde que $1 \in E$, temos que $IJ[E] \subseteq I[E]J[E]$. Para provar a outra inclusão, basta ver que, se $\alpha \in I[E]$ e $\beta \in J[E]$, então $\alpha\beta \in IJ[E]$. Sejam $\alpha \in I[E]$ e $\beta \in J[E]$, portanto existem $\alpha_i \in I, \beta_j \in J$ tais que $\alpha = \sum_{i\in\Omega} \alpha_ie_i$ e $\beta = \sum_{j\in\Omega} \beta_je_j$. Agora,

$$\alpha\beta = (\sum_{i\in\Omega} \alpha_ie_i)(\sum_{j\in\Omega} \beta_je_j) = (\sum_{i,j\in\Omega} \alpha_i\beta_je_ie_j\ ) =$$

$$= \sum_{i,j\in\Omega} \alpha_i\beta_j(\sum_{k\in\Omega} r_{ijk}e_k) = \sum_{i,j,k\in\Omega} \alpha_i\beta_j r_{ijk}e_k \in IJ[E],$$

onde $e_{ij} = \sum_{i,j,k\in\Omega} r_{ijk}e_k$ com $r_{ijk} \in R$.

Lema 1.3.3 *Sejam R e S como no enunciado do lema anterior. Se P é um ideal primo de S, então $P \cap R$ é um ideal primo de R.*

Demonstração : Claramente, $P \cap R$ é um ideal de R. Sejam I e J ideais de R tais que $IJ \subseteq P \cap R$. Então $IJ[E] \subseteq P$. Como P é ideal primo de S e $I[E].J[E] = IJ[E] \subseteq P$, temos que $I[E] \subseteq P$ ou $J[E] \subseteq P$. Conseqüentemente , $I \subseteq P \cap R$ ou $J \subseteq P \cap R$. Logo $P \cap R$ é um ideal primo de R.

Definição 1.3.4 *Um ideal I não nulo de S é dito $R-disjunto$ se $I \cap R = 0$.*

Seja, como acima, S uma extensão livre centralizante de R. Se P é um ideal primo de S, então temos que $\overline{R} = \frac{R}{P\cap R} \subseteq \overline{S} = \frac{S}{(P\cap R)[E]}$. De fato, seja $a \in R$ e suponhamos que $\overline{a} = \overline{0}$ em $\overline{S}$. Então $a \in P$ e conseqüentemente $a \in P \cap R$. Assim $\overline{a} = \overline{0}$ em $\overline{R}$. Logo o homomorfismo $\varphi : \overline{R} \to \overline{S}$, onde $\varphi(a + P) = a + (P \cap R)[E]$, é injetivo e portanto $\overline{R} \subseteq \overline{S}$.

Lema 1.3.5 *Sejam P ideal primo de S, $\overline{R} = \frac{R}{P\cap R}$, $\overline{S} = \frac{S}{(P\cap R)[E]} \simeq \overline{R}[E]$ e $\overline{P} = \frac{P}{(P\cap R)[E]}$. Então $\frac{S}{P} \simeq \frac{\overline{S}}{\overline{P}}$ e $\overline{P}$ é um ideal primo $\overline{R}$-disjunto de $\overline{S}$.*

Demonstração : Temos que $\frac{S}{P} \simeq \frac{\overline{S}}{\overline{P}}$ é conseqüência do Teorema Clássico dos Isomorfismos (ver corol. 2 pg. 46 de [2]). Como $\frac{S}{P} \simeq \frac{\overline{S}}{\overline{P}}$ e, por 1.1.6, $\frac{S}{P}$ é um anel primo, logo $\frac{\overline{S}}{\overline{P}}$ é primo. Usando novamente 1.1.6, temos que $\overline{P}$ é um ideal primo de $\overline{S}$. Vejamos que $\overline{P} \cap \overline{R} = 0$. Seja $a \in P$ e $\overline{a} = a + (P \cap R)[E]$ tal que $\overline{a} \in \overline{P} \cap \overline{R}$. Logo existe $b \in R$ satisfazendo $\overline{a} = \overline{b}$, onde $\overline{b} = b + (P \cap R)[E]$.

Suponhamos que $a = a_0 + \sum_{i=1}^{n} a_ie_i$. Como $\overline{a} = \overline{b}$, temos que $a - b \in (P \cap R)[E]$. Assim, $(a_0 - b) + \sum_{i=1}^{n} a_ie_i \in (P \cap R)[E]$, e conseqüentemente $a_i \in P \cap R$ para todo $i \in \{1, 2, ..., n\}$. Também $(a_0 - b) \in P \cap R$ e então $a_0 \in P \cap R$. Logo, $a = a_0 + \sum_{i=1}^{n} a_ie_i \in (P \cap R)[E]$, ou seja, $\overline{a} = \overline{0}$ e concluímos que $\overline{P} \cap \overline{R} = \overline{0}$. O lema está demonstrado.

Como consequência imediata destes lemas, temos que, dado um ideal primo P de $S = R[E]$, passando aos quocientes $\frac{R}{P\cap R}$ e $\frac{S}{(P\cap R)[E]}$, podemos supor que R é um anel primo com unidade e que P é um ideal primo $R-$ *disjunto* de S.

Para terminar esta secção, relacionamos alguns exemplos de extensões livres centralizantes de um anel R:

(i) Anéis de Polinômios

O anel de polinômios a uma indeterminada X sobre R, denotado por $R[X]$ é bastante conhecido. Temos que $E = \{X^i\}_{i\in \mathbf{N}}$, o conjunto das potências da indeterminada, é uma base centralizante de $R[X]$ sobre R. É fácil ver que $R[X]$ é uma extensão livre centralizante de R.

Consideremos agora $S = R[X_1, ..., X_n]$, o anel de polinômios a n indeterminadas sobre R. Também S é conhecido. Seja $E_1 = \{X_1^{i_1}X_2^{i_2}...X_n^{i_n} \mid i_k \in \mathbf{N}, \forall k \in \Lambda\}$ o conjunto dos produtos entre as potências das indeterminadas, onde $\Lambda = \{1, 2, ..., n\}$. Então E_1 é uma base centralizante de S sobre R e $1 \in E_1$. Temos que S é uma extensão livre centralizante de S sobre R.

Observemos também que o conjunto de indeterminadas F não precisa ser comutativo e tampouco finito. Isto é, o anel de polinômios $R[F]$, $F = \{X_\lambda\}_{\lambda\in\Omega}$ sobre um conjunto arbitrário de indeterminadas, que comutem ou não, também é uma extensão livre centralizante de R.

(ii) Anéis de Matrizes

Seja $n \in \mathbf{N}$ e $S = M_n(R)$ o anel de matrizes quadradas sobre R de dimensão n. Definimos as matrizes $E_{ij} \in S$ de modo que a j-ésima entrada da linha i de E_{ij} é 1, e as demais entradas de E_{ij} são nulas. Sejam $F = \{E_{ij}\}_{i,j\in\Lambda}$ onde $\Lambda = \{1, ..., n\}$, $F_0 = F \setminus \{E_{11}\}$, I a matriz identidade ($I = \sum_{i=1}^{n} E_{ii}$) e $E = F_0 \cup \{I\} = \{e_k\}_{k\in\Omega}$. Dado $r \in R$, identificamos r com rI e portanto $R \subseteq S$. Em particular, $1 = I \in E$. Também é evidente que $re_k = e_k r$, para todo $r \in R$ e qualquer $e_k \in E$.

É imediato verificar que cada matriz $M \in S$ é dada por $M = \sum_{i,j\in\Lambda} \oplus r_{ij}E_{ij}$ univocamente. A partir daí, é fácil ver que $M = \sum_{k\in\Omega} \oplus r_k e_k$, com $r_k \in R$, univocamente. Assim, $S = \sum_{k\in\Omega} \oplus Re_k$ e concluímos que S é uma extensão livre centralizante de R.

(iii) Anel de Matrizes Infinitas

Seja $M(R)$ o anel de todas as matrizes quadradas infinitas sobre R, onde cada matriz tem um número finito de entradas não nulas. Observemos que, dadas as matrizes A e B em $M(R)$, existem $m, n \in \mathbf{N}$ tais que $A \in M_m(R)$ e $B \in M_n(R)$. Seja $l = max\{m, n\}$. Então $A, B \in M_l(R)$ onde, se necessário, completamos uma das matrizes com zeros. Assim, $A + B$ e AB estão definidas e temos uma estrutura de anel para $M(R)$.

Notemos que $M(R)$ não tem unidade. Consideremos então $S = M(R) \oplus R$ e definimos a adição e a multiplicação em S do seguinte modo: Dados $A, B \in M(R)$ e $r, s \in R$, $(A, r) + (B, s) = (A + B, r + s)$ e $(A, r)(B, s) = (AB + sA + rB, rs)$

É fácil ver que S é um anel e que $(0, 1)$ é a unidade do anel S.

Considerando o exemplo anterior, obtemos que $M(R) = \sum_{i,j=1}^{\infty} \oplus RE_{ij}$. Assim, $S = \sum_{i,j=1}^{\infty} \oplus RE_{ij} \oplus RI$ é uma extensão livre centralizante de R.

(iv) Anéis de Grupo

Seja G um grupo. Consideremos o seguinte conjunto:

$RG = \{\sum_{g \in G} r_g g \mid r_g \in R$ e $r_g = 0$ exceto para um número finito de $r_g\}$.

Definimos em RG a adição e a multiplicação do seguinte modo:

$$\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$$

Para dois elementos $r_g g$ e $s_f f$ de RG definimos $(r_g)(s_f)$ por $(r_g s_f) gf$ e, mais geralmente,

$$(\sum_{g \in G} r_g g)(\sum_{f \in G} s_f f) = \sum_{h \in G} (\sum_{gf = h} r_g s_f) h$$

O conjunto RG, com estas operações, é um anel chamado de anel de grupo de G sobre R.

Temos que G é uma base centralizante de RG sobre R e, considerando o monomorfismo de R em RG dado por $r \mapsto re$, onde e é a unidade de G, obtemos que $R \subseteq RG$ e $1_{RG} = e \in G$. Assim, é fácil ver que RG é uma extensão livre centralizante de R (ver §1.2, ex. 1.7.18 de [19]).

(v) Produto Tensorial sobre Corpos

Sejam L um corpo e R e K duas L-álgebras. Então o produto tensorial $S = R \otimes_L K$ é uma extensão livre centralizante de R. De fato, sejam B e B' bases de R e K sobre L, respectivamente. Então temos que $C = \{b \otimes b' \mid b \in B \text{ e } b' \in B'\}$ é uma base de S sobre L. Além disso, temos que $R \subseteq S$, via o monomorfismo canônico $\varphi : R \to R \otimes_L K$ definido por $\varphi(r) = r \otimes 1$. Temos que $E = \{1 \otimes b' \mid b' \in B'\}$ é uma base centralizante de S sobre R e $1 = 1 \otimes 1 \in E$ (ver secção 1.7 de [19]).

Capítulo 2

Ideais Primos e Ideais Fechados

2.1 Ideais Fechados em Extensões Livres Centralizantes

Sejam R um anel primo e S uma extensão livre centralizante de R. Seja I um ideal $R-disjunto$ de S. Um elemento não nulo a de I é dito de suporte mínimo em I se para qualquer $b \in I$ com $sup(b) \subset sup(a)$ temos $b = 0$. Denotamos por $M(I)$ o conjunto de todos os elementos de suporte mínimo em I. A minimalidade de I é definida por $Min(I) = \{sup(a) \mid a \in M(I)\}$.

Definição 2.1.1 *Seja I um ideal $R-disjunto$ de S. Chamamos de fecho do ideal I em S ao conjunto* $[I]_R = [I] = \{b \in S \mid \exists 0 \neq H \lhd R : bH \subseteq I\}$.

Omitiremos o índice R em $[I]_R$, sempre que esteja claro no contexto.

Lema 2.1.2 *Seja I um ideal $R-disjunto$ de S. Então $[I]$ é um ideal $R-disjunto$ de S que satisfaz $I \subseteq [I]$ e $Min(I) = Min([I])$.*

Demonstração : É fácil ver que $[I]$ é um ideal de S contendo I, desde que R é primo.

Suponhamos que $\Gamma \in Min(I)$. Então existe $0 \neq a \in M(I)$ com $sup(a) = \Gamma$, e também $a \in [I]$. Agora seja $b \in [I]$ tal que $sup(b) \subset \Gamma$. Temos que existe $0 \neq H \lhd R$ satisfazendo $bH \subseteq I$. Como $sup(bx) \subseteq sup(b) \subset \Gamma$ para todo $x \in H$, temos que $bH = 0$ e assim $b = 0$, pois R é primo. Conseqüentemente, $a \in M([I])$ e portanto $\Gamma \in Min([I])$.

Reciprocamente, assumimos que $\Gamma \in Min([I])$. Então existe $a \in M([I])$ tal que $sup(a) = \Gamma$ e existe $0 \neq H \lhd R$ com $aH \subseteq I$. Outra vez temos que para qualquer $x \in H$, $sup(ax) \subseteq sup(a)$. Como $a \in M([I])$ e $ax \in I \subseteq [I]$ para cada $x \in H$, obtemos que ou $sup(ax) = sup(a)$ ou $sup(ax) = \emptyset$ (isto é ax=0). Mas $aH \neq 0$ já que R é primo, e assim existe $x \in H$ tal que $ax \neq 0$ e $sup(ax) = \Gamma$. Conseqüentemente $\Gamma \in Min(I)$ (para $b \in I$ com $sup(b) \subset \Gamma$ temos $b = 0$, desde que $b \in [I]$ e $\Gamma \in Min([I])$). Logo $Min(I) = Min([I])$. Agora também é claro que $[I]$ é $R - disjunto$.

Definição 2.1.3 *Um ideal $R - disjunto$ I de S é dito fechado se $[I] = I$.*

O teorema a seguir dá uma caracterização do fecho de um ideal $R - disjunto$ I de S, em função das minimalidades de I e de $[I]$.

Teorema 2.1.4 *Seja I um ideal $R - disjunto$ de S. Então $[I]$ é o maior ideal J de S que contém I e satisfaz $Min(J) = Min(I)$.*

Demonstração : Seja J um ideal $R - disjunto$ de S com $I \subseteq J$ e $Min(J) = Min(I)$. Suponhamos que $\Gamma = \{e_1, ..., e_n\} \in Min(J)$. Seja $a = \sum_{i=1}^{n} a_i e_i \in I$ com $sup(a) = \Gamma$. Se $b = \sum_{i=1}^{n} b_i e_i \in J$ então $(bxa_1 - b_1xa) \in J$ para todo $x \in R$. Ainda $sup(bxa_1 - b_1xa) \subset \Gamma$ e conseqüentemente $bxa_1 = b_1xa$. Mas $b_1xa \in I$ e portanto $bxa_1 \in I$. Segue que $bRa_1R \subseteq I$. Logo existe um ideal não nulo $H = Ra_1R$ de R, que depende somente de Γ , satisfazendo $bH \subseteq I$, para todo $b \in J$ com $sup(b) = \Gamma$. Isto mostra que $b \in [I]$.

Agora suponhamos que $\Gamma = \{e_1, ..., e_t\}$ é qualquer subconjunto finito de E. Usaremos indução para mostrar que existe $0 \neq H \lhd R$ tal que $bH \subseteq I$ para qualquer $b \in J$ com $sup(b) \subseteq \Gamma$. De fato, se $t = 1$ a afirmação segue pela primeira parte. Assim, podemos supor que $t > 1$ e existe $c \in M(I)$ com $sup(c) \subset \Gamma$. Seja $c = c_1e_1 + ... + c_ne_n$, onde $n < t$. Pela hipótese de indução, existe um ideal F não nulo de R tal que $dF \subseteq I$, para todo $d \in J$ com $sup(d) \subseteq \{e_2, ..., e_t\}$. Seja $b = b_1e_1 + ... + b_te_t \in J$. Se $b_1 \neq 0$, para cada $x \in R$ consideramos $d_x = bxc_1 - b_1xc \in J$. Desde que $sup(d_x) \subseteq \{e_2, ..., e_t\}$, nós temos por hipótese de indução, que $d_xF \subseteq I$, onde $0 \neq F \lhd R$. Também $b_1x \in F \subseteq I$ e conseqüentemente $bxc_1F \subseteq I$. O mesmo resultado é verdadeiro se $b_1 = 0$, desde que, neste caso, $sup(b) \subseteq \{e_2, ..., e_t\}$. Portanto $bRc_1F \subseteq I$. Logo $b \in [I]$ e então $J \subseteq [I]$. O teorema está demonstrado.

Corolário 2.1.5 *Seja I um ideal $R - disjunto$ de S. Então $[I]$ é o menor ideal fechado de S que contém I. Em particular, $[I]$ é o único ideal fechado de S que contém I e satisfaz $Min([I]) = Min(I)$.*

Demonstração : Por 2.1.2, temos que $Min(I) = Min([I]) = Min([[I]])$ e assim, pelo teorema 2.1.4 $[I] = [[I]]$, isto é, $[I]$ é fechado.

Para terminar a prova, mostremos que $[I]$ é o menor ideal fechado de S que contém I. Seja L um ideal fechado de S com $I \subseteq L \subseteq [I]$ e $b \in [I]$. Temos que existe $0 \neq H \lhd R$ tal que $bH \subseteq I \subseteq L$. Conseqüentemente $b \in [L] = L$ e assim $[I] \subseteq L$. Portanto $L = [I]$, como queríamos. A unicidade citada no enunciado é agora evidente.

Proposição 2.1.6 *Todo ideal primo $R-disjunto$ de S é fechado.*

Demonstração : Seja P um ideal primo $R-disjunto$ de S e $b \in [P]$. Então existe $0 \neq H \lhd R$ tal que $bH \subseteq P$ e portanto $bHS \subseteq P$. Como S é uma extensão livre centralizante de R, temos que $HS \lhd S$ e por 1.1.5 temos que $b \in P$. Logo $P = [P]$, ou seja P é fechado. A prova está completa.

Nós podemos definir $[I]$ por um caminho dual:

$$[I]^* = \{b \in S \mid \exists 0 \neq H \lhd R : Hb \subseteq I\}.$$

Podemos provar como antes que $[I]^*$ é o maior ideal J de S que contém I e satisfaz $Min(J) = Min(I)$. Então pelo teorema 2.1.4 segue que $[I]^* = [I]$.

Para demonstrar o teorema 2.1.4 e o corolário 2.1.5, nós usamos somente que J é um ideal à direita de S. Assim, se I é um ideal fechado e L é um ideal à direita de S com $I \subseteq L$ e $Min(L) = Min(I)$, então $L = I$. O mesmo resultado é verdadeiro para um ideal à esquerda, como se pode provar facilmente usando a definição dual do fecho $[I]$. Temos o seguinte

Corolário 2.1.7 *Sejam I e J ideais $R-disjuntos$ de S, e seja L um ideal à direita (esquerda) de S.*
(i) Se $I \subseteq J$ então $[I] \subseteq [J]$.
(ii) Se $I \subseteq J$ e $Min(I) = Min(J)$ então $[I] = [J]$.
(iii) Se I é fechado, $L \supseteq I$ e $Min(L) = Min(I)$ então $I = L$.

Demonstração : (i) Se $I \subseteq J$ então $I \subseteq [J]$ e como $[J]$ é um ideal fechado, obtemos que $[I] \subseteq [J]$, já que $[I]$ é o menor ideal fechado que contém I.

(ii) Temos que $I \subseteq J \subseteq [J]$ e $Min([J]) = Min(J) = Min(I)$. Logo $[I] = [J]$.

(iii) Está provado na observação anterior ao corolário.

A seguir mostraremos que o fecho $[I]$ de um ideal $R-disjunto$ I de S é também o fecho de $RM(I)$ (ou seja, $[SM(I)]_R = [I]_R$). Para isso, consideramos as seguintes notações: Dado I um ideal $R-disjunto$ de S denotamos

$$\overline{I} = \{b \in S \mid \exists 0 \neq H \lhd R : bH \subseteq SM(I)\} = [SM(I)]_R \quad \text{e}$$

$$\overline{\overline{I}} = \{b \in S \mid \exists 0 \neq H \lhd R : bH \subseteq RM(I)\} = [RM(I)]_R.$$

Corolário 2.1.8 *Seja I um ideal $R-disjunto$ de S. Então $[I] = \overline{I} = \overline{\overline{I}}$.*

Demonstração : É claro que $\overline{\overline{I}} \subseteq \overline{I} \subseteq [I]$, já que $RM(I) \subseteq SM(I) \subseteq I$. Seja $b \in [I]$ com $sup(b) \in M(I)$. Então existe $0 \neq H \lhd R$ tal que $bH \subseteq I$. Sejam $b = \sum_{i=1}^{n} b_i e_i$ e $h \in H$. Assim, $bh = \sum_{i=1}^{n} b_i e_i h = \sum_{i=1}^{n} b_i h e_i \in I$. Logo $bh = 0$ ou $sup(bh) \subseteq sup(b)$ e portanto $bh \in M(I)$. Logo vale que $bH \subseteq M(I) \cup \{0\} \subseteq RM(I)$ e conseqüentemente $b \in \overline{\overline{I}}$.

Pelo mesmo raciocínio usado na demonstração do teorema 2.1.4, nós podemos mostrar que para qualquer subconjunto finito Γ de E existe um ideal não nulo F de R satisfazendo $dF \subseteq \Gamma$, para todo $d \in [I]$ com $sup(d) \subseteq \Gamma$. Segue que $[I] \subseteq \overline{\overline{I}}$ e a prova está completa.

2.2 Ideais Fechados em R[X]

Nesta secção R continua sendo um anel com unidade. Aqui, mostraremos que o fecho de um ideal I de $R[X]$, fica determinado por um polinômio f de mínimo grau em I. Isto é bem mais simples que considerar todos os elementos de suporte mínimo de I.

Dado $g \in R[X]$, um polinômio não nulo no anel de polinômios $R[X]$, denotamos por ∂g o grau de g e por $lc(g)$ o coeficiente dominante de g. Para um ideal I não nulo de $R[X]$, ∂I denota o mínimo dos graus dos polinômios não nulos de I, isto é, $\partial I = min\{\partial g \mid 0 \neq g \in I\}$.

Consideramos agora os seguintes conjuntos:

$$\Gamma = \Gamma_R = \{f \in R[X] \mid arf = fra, \forall r \in R; a = lc(f)\}.$$

Para $f \in \Gamma_R$ tal que $lc(f) = a$

$$[f] = [f]_R = \{g \in R[X] \mid \exists 0 \neq H \lhd R, gHa \subseteq R[X]f\}.$$

Sempre que estiver claro no texto, omitiremos o índice R em Γ_R e $[f]_R$. Vejamos o seguinte lema:

Lema 2.2.1 *Seja $f \in \Gamma$ com $\partial f \geq 1$. Então $[f]$ é um ideal $R-disjunto$ de $R[X]$, o qual contém f como polinômio de mínimo grau.*

Demonstração : É fácil ver que $[f] \lhd R[X]$. Desde que $fra = arf \in R[X]f$, para todo $r \in R$ onde $a = lc(f)$, nós temos que $f \in [f]$. Suponhamos que exista $0 \neq g \in [f]$ satisfazendo $\partial g < \partial f$. Então existe $0 \neq H \lhd R$ tal que $gHa \subseteq R[X]f$. Para $h \in H$, existe $k = k_h = X^m b_m + ... + b_0 \in R[X]$ com $gha = kf$. Temos que $b_m a = 0$. De fato, se $b_m a \neq 0$ então $\partial(kf) = m + \partial f > \partial g \geq \partial(gha)$. Além disso, para todo $r \in R, ghara = kfra = karf$.

Assumimos por indução que $b_i a = 0$ para qualquer $i = m, ..., m-s+1$. Da igualdade $ghara = karf$ para todo $r \in R$, obtemos que $b_{m-s}ara = 0$, pois se $b_{m-s}ara \neq 0$ temos que $\partial(karf) = (m-s) + \partial f > \partial g \geq \partial(ghara)$. Segue que $b_{m-s}a = 0$, pois R é primo e $a = lc(f) \neq 0$.

Assim $ghara = 0$ $\forall h \in H, r \in R$ e conseqüentemente $g = 0$, desde que $R[X]$ é primo (1.1.8(i)). A prova está completa.

O lema a seguir relaciona $[f]$ e $[f']$ para dois polinômios f e f' em Γ.

Lema 2.2.2 *Sejam* $f, f' \in \Gamma$. *As seguintes condições são equivalentes:*
(i) $[f] \subseteq [f']$
(ii) $f \in [f']$

Demonstração : Claramente (i)$\Rightarrow$(ii).

(ii)$\Rightarrow$(i) Sejam $a = lc(f)$ e $a' = lc(f')$. Se $g \in [f]$ então existe $0 \neq H \lhd R$ tal que $gHa \subseteq R[X]f$. Além disso, $f \in [f']$ e portanto existe $0 \neq H' \lhd R$ tal que $fH'a' \subseteq R[X]f'$. Temos que $gHaH'a' \subseteq R[X]fH'a' \subseteq R[X]f'$. Logo $g \in [f']$, desde que $0 \neq HaH'$.

Do lema acima obtemos facilmente o

Corolário 2.2.3 *Sejam* $f, f' \in \Gamma$. *São equivalentes:*
(i) $[f] = [f']$
(ii) $f \in [f']$ *e* $f' \in [f]$
(iii) $fra' = arf'$ *e* $a'rf = f'ra$, *para qualquer* $r \in R$,
onde $a = lc(f)$ *e* $a' = lc(f')$

Demonstração : (i)$\Leftrightarrow$(ii) Imediato.

(iii)$\Rightarrow$(ii) Por hipótese, para qualquer $r \in R$ temos que $fra' = arf'$. Então $fRa' \subseteq R[X]f'$ e portanto $f \in [f']$. Analogamente, temos que $f' \in [f]$.

(i)$\Rightarrow$(iii) Temos, pelo lema 2.2.1, que $\partial f = \partial f'$. Assim dado $r \in R$, $h_r = fra' - arf' \in [f]$ e ou $h_r = 0$ ou $\partial(h_r) < \partial f$. Novamente pelo lema 2.2.1, temos que $h_r = 0$ para qualquer $r \in R$. Logo $fra' = arf'$ para todo $r \in R$. Analogamente temos que $a'rf = f'ra$, onde $r \in R$.

Como na secção anterior, $M(I)$ denota o conjunto de todos os elementos de suporte mínimo em I, para I um ideal de $R[X]$.

Lema 2.2.4 *Seja* I *um ideal de* $R[X]$ *e* $f \in I$. *Se* $\partial f = \partial I$ *então* $f \in M(I) \cap \Gamma$.

Demonstração : Para $r \in R$, consideramos $h_r = fra - arf$, onde $a = lc(f)$. É claro que $\partial h_r < \partial f$ ou $h_r = 0$. Por hipótese, $h_r = 0$ já que $h_r \in I$. Assim, $fra = arf$ para todo $r \in R$ e conseqüentemente $f \in \Gamma$.

Suponhamos que $f \notin M(I)$. Então existe $0 \neq g \in I$ tal que $sup(g) \subset sup(f)$. Sejam $g = \sum_{j=0}^{n} b_j X^j$ e $f = \sum_{i=0}^{n} a_i X^i$, $a = a_n$ e $b = b_n$. Da hipótese existe $0 \leq i \leq n$ tal que $b_i = 0 \neq a_i$. Para $r \in R$ definimos $h_r = arg - frb \in I$. Logo

$h_r = 0$. Olhemos o coeficiente de X^i em h_r. Segue que $0 = (arb_i - a_i rb) = -a_i rb$. Assim para todo $r \in R$ temos que $a_i rb = 0$ e $a_i \neq 0$. Conseqüentemente $b = 0$, pois R é primo. Assim, $g = 0$ pois $\partial f = \partial I$. Isto contradiz a hipótese de que $f \notin M(I)$. O lema está demonstrado.

Definição 2.2.5 *Um ideal I de $R[X]$ é dito um ideal principal fechado se existe $f \in \Gamma$ tal que $[f] = I$*

Teorema 2.2.6 *Sejam R um anel primo e I um ideal $R-disjunto$ de $R[X]$. Então existe um menor ideal principal fechado $[I]'$ de $R[X]$ o qual contém I. Além disso, $[I]' = [f]$ para qualquer f de mínimo grau em I.*

Demonstração : Seja $f \in I$ tal que $\partial f = \partial I = n$ e $a = lc(f)$. Por 2.2.4, $f \in \Gamma$. Se $g \in I$ e $\partial g = n$, temos que $gra - brf \in I$, para todo $r \in R$ onde $b = lc(g)$. Conseqüentemente, $gra = brf \in R[X]f$, para qualquer $r \in R$, e assim $g \in [f]$.

Suponhamos por indução que para $g \in I$ com $\partial g \leq m - 1$ nós temos $gHa \subseteq R[X]f$ para $H = RaR...aR$ (onde R aparece $(m-n)$ vezes). Conseqüentemente $g \in [f]$. Tomemos $k \in I$ tal que $\partial k = m$, digamos $k = X^m c_m + ... + c_0$ e $c = c_m$. Para $r \in H$, seja $k_r = kra - X^{m-n} crf \in I$, pois $k, f \in I$.

Desde que $\partial k_r \leq m - 1$, $k_r Ha \subseteq R[X]f$ e segue que $kRaHa \subseteq R[X]f$. Isto completa a prova de que $I \subseteq [f]$.

Agora suponhamos que $I \subseteq [f']$ para algum $f' \in \Gamma$. Desde que $f \in I$, por 2.2.2 temos que $[f] \subseteq [f']$. Então $[f]$ é o menor ideal principal fechado de $R[X]$ que contém I. O resto é claro.

Definição 2.2.7 *Seja I um ideal $R-disjunto$ de $R[X]$. O ideal $[I]'$ definido no teorema 2.2.6 será chamado de ideal principal fechado associado à I.*

Observamos que um ideal $R-disjunto$ I de $R[X]$ é principal fechado se e somente se $I = [I]'$. O nosso objetivo agora é mostrar que $[I]' = [I]$, onde $[I]$ é o fecho de I estudado na secção anterior. Ou seja, mostrar que $[f] = [I]$ para qualquer $f \in I$ tal que $\partial f = \partial I$ (corol.2.2.9). Para isso, vejamos o

Corolário 2.2.8 *Seja I um ideal $R-disjunto$ de $R[X]$. Então $[I]'$ é o maior ideal J de $R[X]$ o qual contém I e satisfaz $\partial J = \partial I$. Em particular $[I]'$ é o único ideal principal fechado de $R[X]$ o qual contém I e satisfaz $\partial[I]' = \partial I$.*

Demonstração : É claro que $\partial[I]' = \partial I$. Suponhamos que exista $J \lhd R[X]$ satisfazendo $\partial J = \partial I = n$ e $J \supseteq I$. Se $f \in I$ com $\partial f = n$ então $f \in J$ e assim $J \subseteq [f] = [I]'$ pelo teorema 2.2.6. O resto está claro.

Corolário 2.2.9 *Seja I um ideal $R-disjunto$ de $R[X]$, e $f \in I$ satisfazendo $\partial f = \partial I$. Então $[f] = [I]$.*

Demonstração : Seja $g \in [f]$.Então existe $0 \neq H \lhd R$ tal que $gHa \subseteq R[X]f \subseteq I$ pois $f \in I$, onde $a = lc(f)$. Conseqüentemente $gHaR \subseteq I$ e portanto $g \in [I]$. Logo $[f] \subseteq [I]$.

Reciprocamente, sendo que $I \subseteq [I]$ segue que $\partial[I] \leq \partial I$. Por outro lado se $g \in [I]$, temos que existe $0 \neq H \lhd R$ tal que $gH \subseteq I$. Assim, para $h \in H$ existe $k \in I$ tal que $gh = k$, com algum k não nulo. Para este k temos $\partial k = \partial(gh) \leq g$ e então segue que $\partial I \leq \partial[I]$.Logo $\partial[I] = \partial I$ e pelo corolário anterior $[f] = [I]$.

Observamos que em [5], a minimalidade de um ideal $R-disjunto$ I de $R[X]$ é definida por $Min(I) = min\{\partial f : 0 \neq f \in I\}$. Aqui, $Min\{\partial f : 0 \neq f \in I\}$ é denotado por ∂I e $Min(I)$ denota o conjunto dos suportes dos elementos de suporte mínimo pertencentes à I.

Pelo corolário anterior, vemos que para um ideal I no anel de polinômios $R[X]$ podemos definir o fecho $[I]$ a partir de ∂I (como em [5]).

Assim, dado um ideal $R-disjunto$ I de $R[X]$, dizer que I é um ideal principal fechado ($I = [f]$ para $f \in I$ com $\partial f = \partial I$) é equivalente a dizer que o ideal I é fechado ($I = [I]$).

Se $I \subseteq J$ são dois ideais $R-disjuntos$ de $R[X]$ então $Min(I) = Min(J)$ se e somente se $\partial I = \partial J$. De fato, se $Min(I) = Min(J)$ temos que $[I] = [J]$. Mas $[I] = [f]$ para $f \in I$ com $\partial f = \partial I$ e $[J] = [g]$ para $\partial g = \partial J$. Como $[I] = [J]$, temos que $\partial f = \partial g$ e conseqüentemente $\partial I = \partial J$. Reciprocamente, se $\partial I = \partial J$, obtemos que $[I] = [f] = [J]$, para $f \in I \subseteq J$ com $\partial f = \partial I = \partial J$.

Observamos ainda que dado $0 \neq r \in R$ então $r \in \Gamma$ e conseqüentemente $[r] = R[X]$. Assim, se I é um ideal de $R[X]$ tal que $I \cap R \neq 0$, definimos $[I] = R[X]$ e $[0] = 0$. Temos então o

Corolário 2.2.10 *Sejam I e J ideais de $R[X]$. Então*
(i) $[[I]] = [I]$
(ii) Se $I \subseteq J$ então $[I] \subseteq [J]$
(iii) $[[I] + [J]] = [I + J]$

Demonstração : (i) Se $I \cap R = 0$ o resultado segue por 2.2.8. Se $I \cap R \neq 0$, pela observação acima temos que $[I] = R[X] = [[I]]$.

(ii) Se $I \cap R = 0$, temos que $[I] = [f]$ para $f \in I$ tal que $\partial f = \partial I$. Como $f \in J$ temos que (pelo lema 2.2.2 se $J \cap R = 0$) que $[I] \subseteq [J]$. Se $J \cap R \neq 0$, é claro que $[I] \subseteq [J] = R[X]$.

(iii) Do fato de $I + J \subseteq [I] + [J]$ temos que $[I + J] \subseteq [[I] + [J]]$. Agora $[I], [J] \subseteq [I + J]$ e portanto $[I] + [J] \subseteq [I + J]$. Conseqüentemente $[[I] + [J]] \subseteq [[I + J]] = [I + J]$. O corolário está demonstrado.

O teorema a seguir caracteriza os ideais $R-$ *disjuntos* de $R[X]$ que são primos:

Teorema 2.2.11 *Seja P um ideal $R-$ disjunto de $R[X]$. Então P é primo se e somente se P é maximal com respeito a propriedade $P \cap R = 0$.*

Para demonstrar este teorema, precisamos do seguinte lema:

Lema 2.2.12 *Seja L um ideal $R-$ disjunto de $R[X]$. Sejam $f \in L$ tal que $\partial f = \partial L = n$ e $a = lc(f)$. Seja $g \in L$ de grau m, com $b = lc(g)$. Então para toda família $a_1, a_2, ..., a_{m-n} \in R$ existe $h \in R[X]$ com $\partial h \leq m - n$ tal que $fa_0h = (\prod_{i=0}^{m-n} aa_i)g$ para todo $a_0 \in R$.*

Demonstração : Demonstraremos por indução com respeito a $(m - n)$. Se $m = n$, tomamos $h = b$ e vale $fa_0b = aa_0g$, para todo $a_0 \in R$. Seja $m - n > 0$. Dados $a_1, a_2, ..., a_{m-n} \in R$ definimos $g' = aa_{m-n}g - fa_{m-n}bX^{m-n}$. Então $\partial g' < m$ pois o coeficiente de X^m em g' é $(aa_{m-n}b - aa_{m-n}b) = 0$. Logo $\partial g' - n < m - n$. Seja $m' = \partial g'$. Por indução temos que para qualquer família $c_1, c_2, ..., c_{m'-n} \in R$ existe $h' \in R[X]$ com $\partial h' \leq m' - n$ tal que $fc_0h' = (\prod_{1=0}^{m'-n} ac_i)g'$, para todo $c_0 \in R$.

Mas $(\prod_{i=0}^{m'-n} ac_i)g' = (\prod_{i=0}^{m'-n} ac_i)(aa_{m-n}g - fa_{m-n}bX^{m-n})$ e portanto temos que:

$$fc_0h' = (\prod_{i=0}^{m'-n} ac_i)aa_{m-n}g - \prod_{i=0}^{m'-n}(ac_i)fa_{m-n}bX^{m-n}$$

para qualquer $c_0 \in R$. Como $\partial f = \partial L$ temos que $f \in \Gamma$ e portanto temos:

$$\prod_{i=0}^{m'-n} ac_ifa_{m-n}bX^{m-n} = f\prod_{i=0}^{m'-n} ac_ia_{m-n}bX^{m-n}.$$

Logo

$$fc_0(h' + \prod_{i=0}^{m'-n} ac_i a_{m-n} bX^{m-n}) = (\prod_{i=0}^{m'-n} ac_i) a a_{m-n} g$$

para qualquer $c_0 \in R$.

O resultado segue, se tomamos $c_1 = a_1, c_2 = a_2, \ldots, c_{m'-n-1} = a_{m'-n-1}$ e $c_{m'-n} = a_{m'-n} a a_{m'-n+1} a \ldots a a_{m-n-1}$.

Os dois lemas a seguir demonstram o teorema 2.2.11

Lema 2.2.13 *Seja P um ideal de $R[X]$ que é maximal com respeito à propriedade $P \cap R = 0$. Então P é primo.*

Demonstração : Seja I e J ideais de $R[X]$ tais que $P \subseteq J$, $P \subseteq I$ e $IJ \subseteq P$. Como $P \cap R = 0$ e R é primo, segue que $I \cap R = 0$ ou $J \cap R = 0$. Logo, da hipótese segue que $I = P$ ou $J = P$. Por 1.1.7 temos que P é um ideal primo, o que demonstra o lema.

Lema 2.2.14 *Seja P um ideal primo $R-disjunto$ de $R[X]$ $(P \neq 0)$. Então P é maximal com respeito à propriedade $P \cap R = 0$.*

Demonstração : Seja L um ideal de $R[X]$ tal que $P \subseteq L$, $L \cap R = 0$. Se $\partial L = \partial P$ então $L \subseteq [P] = P$, e portanto $L = P$. Suponhamos que $\partial L < \partial P$. Seja $f \in P$ e $g \in L$ tais que $\partial f = \partial P = n$ e $\partial g = \partial L = m$ com $m < n$. Pelo lema 2.2.12 (escolhendo uma família $a_1, \ldots, a_{n-m}$) existe $h \in R[X]$ com $\partial h \leq n - m$ tal que $ga_0 h \in P$, para qualquer $a_0 \in R$. Conseqüentemente, $gR[X]h \subseteq P$ com $h \notin P$, pois $\partial h \leq n - m < n = \partial P$ $(m = 0 \Rightarrow L \cap R \neq 0)$. Logo $g \in P$ e portanto $n = \partial P \leq m$ o que é uma contradição. O lema está demonstrado.

O seguinte corolário é evidente:

Corolário 2.2.15
(i) Qualquer ideal primo $R-disjunto$ de $R[X]$ é principal fechado.
(ii) Um ideal principal fechado é primo se e somente se ele é maximal no conjunto de todos os ideais principais fechados de $R[X]$.

Capítulo 3

Extensão e Contração de Ideais Fechados

3.1 Extensão e Contração em $Q[E]$

Sejam R um anel primo, $S = R[E]$ uma extensão livre centralizante de R e I um ideal $R - disjunto$ de S. Para $\Gamma \in Min(I)$ e $e \in \Gamma$, denotamos por $\theta_{\Gamma,e}(I)$ ao ideal de R definido por $\theta_{\Gamma,e}(I) = \{x \in R \mid \exists b \in I : sup(b) = \Gamma \text{ e } b(e) = x\}$. Como denotamos na secção 1.2, Q é o anel completo de quocientes à direita de R e C é o centro de Q.

Como o centralizador de R em S é um subanel $V_S(R) = C_R[E]$ onde C_R é o centro de R, temos que $L = Q \otimes_{C_R} C_R[E]$ é um anel contendo Q e S. Além disso, L é uma extensão livre centralizante de Q com a mesma base E, identificando e com $1 \otimes e$, para cada $e \in E$. Denotaremos $L = Q[E]$. Conseqüentemente podemos considerar $S = R[E] \subseteq Q[E]$ e também $C[E] = C \otimes_{C_R} C_R[E] = V_{Q[E]}(Q) \subseteq Q[E]$. Finalmente, se T é um anel de quocientes à direita de R, então $T[E]$ é um subanel de $Q[E]$ (contendo $R[E]$).

Nesta secção mostraremos que existe uma correspondência biunívoca entre os ideais de $C[E]$ e os ideais fechados de $R[E]$ e de $T[E]$, onde T é um anel de quocientes à direita de R. Além disso, esta correspondência preserva a propriedade de um ideal ser primo (teoremas 3.1.5 e 3.1.7). Para isso, precisamos de alguns resultados prévios e começamos definindo o conjunto $M_C(I)$ para I um ideal $R - disjunto$ de S. Vejamos o seguinte lema:

Lema 3.1.1 *Sejam I um ideal $R-disjunto$ de S, $\Gamma \in Min(I)$ e $e \in \Gamma$. Então, existe um único elemento $m_{\Gamma,e} \in C[E]$ tal que para qualquer $a \in I$ com $sup(a) = \Gamma$ nós temos $a = m_{\Gamma,e}a(e) = a(e)m_{\Gamma,e}$. Além disso, $sup(m_{\Gamma,e}) = \Gamma$ e $m_{\Gamma,e}(e) = 1$.*

Demonstração : Sejam I um ideal $R-disjunto$ de S, $J = \theta_{\Gamma,e}(I)$ e $\Gamma = \{e_1, e_2, ..., e_n\}$ onde $e_1 = e$. Se $x \in J$, existe um único $a = \sum_{i=1}^{n} x_i e_i \in I$ com $x_1 = x$ e $x_i \in R$, $i = 1, 2, ..., n$. Conseqüentemente, a função $\alpha_i : J \to R$ definida por $\alpha_i(x) = x_i$ (está bem definida) é uma função de R-bimódulos. Assim, existe $c_i \in C$ com $c_i x = x_i$ para $i = 1, 2, ...n$ (ver lema 1.2.17) onde $c_1 = 1$. Seja $m_{\Gamma,e} = \sum_{i=1}^{n} c_i e_i$ então existe $m_{\Gamma,e} \in C[E]$ que satisfaz $sup(m_{\Gamma,e}) = \Gamma$ e $m_{\Gamma,e}(e) = c_1 = 1$. Também, dado $a \in I$ com $sup(a) = \Gamma$, $m_{\Gamma,e}a(e) = \sum_{i=1}^{n} c_i e_i x = \sum_{i=1}^{n} c_i x e_i = \sum_{i=1}^{n} x_i e_i = a$. Analogamente, $a(e)m_{\Gamma,e} = a$. A prova está completa.

Dado um ideal $R-disjunto$ de S, denotamos por $M_C(I)$ o conjunto de todos os elementos $m_{\Gamma,e}$ construídos no lema anterior, onde $\Gamma \in Min(I)$ e $e \in \Gamma$. Assim, $M_C(I) \subseteq C[E]$ e, para qualquer $m \in M_C(I)$, existe um $0 \neq J \lhd R$ com $Jm = mJ \subseteq I$. De fato, dado $m \in M_C(I)$, m é do tipo $m_{\Gamma,e}$, isto é, para qualquer $a \in I$ tal que $sup(a) = \Gamma$ temos que $a = m_{\Gamma,e}a(e) = a(e)m_{\Gamma,e}$. Assim, tomando $J = \theta_{\Gamma,e}(I)$ e dado $x \in J$, por definição de $\theta_{\Gamma,e}$, existe $b \in I$ tal que $sup(b) = \Gamma$ e $b(e) = x$. Logo, $m_{\Gamma,e}x = xm_{\Gamma,e} = b \in I$, portanto $mJ = Jm \subseteq I$.

O lema seguinte define um processo de divisão para o nosso contexto. Sejam T um anel de quocientes à direita de R e I um ideal $T-disjunto$ de $T[E]$. Um elemento $0 \neq b \in Q[E]$ é dito um *"resto módulo I"* se para qualquer $a \in I$ com $sup(a) \subset sup(b)$ nós temos $a = 0$.

Para um ideal $T-disjunto$ I de $T[E]$, denotamos $I_0 = I \cap R[E]$, então I_0 é claramente um ideal não nulo $R-disjunto$ de $R[E]$ e $Min(I_0) = Min(I)$. Denotaremos por $J \lhd_r T$, para dizer que J é um ideal à direita de T. Vejamos o

Lema 3.1.2 *Seja $b \in Q[E]$. Então, existe $q_i \in Q$, $m_i \in M_C(I_0)$ $i = 1, 2, ..., n$ e $r \in Q[E]$ tal que $b = \sum_{i=1}^{n} q_i m_i + r$, onde ou $r = 0$ ou r é um resto módulo I. Se $b \in T[E]$ (respectivamente $b \in J[E]$ para $J \lhd_r T$) então nós podemos tomar $q_i \in TC$ (respectivamente $q_i \in JC$) e $r \in TC[E]$ (respectivamente $r \in JC[E]$.*

Demonstração : Se b é um *resto módulo I* não há o que provar. Suponhamos que b não é um *resto módulo I*. Seja $\Gamma = sup(b)$ e $t =\mid \Gamma \mid$, onde $\mid \Gamma \mid$ representa a cardinalidade do conjunto Γ. Então, existe $\emptyset \neq \Gamma_1 \subseteq \Gamma$ tal que $\Gamma_1 \in Min(I) = Min(I_0)$. Tomamos $e_1 \in \Gamma_1$ e escrevemos $m_1 = m_{\Gamma_1,e_1} \in M_C(I_0)$. Logo, $c_1 = b - b(e_1)m_1$ satisfaz $c_1(e_1) = b(e_1) - b(e_1) = 0$, desde que $m_1(e_1) = 1$, assim

$|\,sup(c_1)\,| \leq t-1$. Se c_1 é um *resto módulo* I, paramos o processo. Caso contrário, nós repetimos o argumento começando com c_1. Continuando, nós encontramos $q_1 = b(c_1), q_2, ..., q_j$ em Q e $m_1, ..., m_j$ em $M_C(I_0)$ tal que $|\,sup(c_j)\,| \leq t-j$, onde $c_j = b - \sum_{i=1}^{j} q_i m_i$. Agora está claro que este processo é finito, quando algum c_k é ou zero ou um *resto módulo* I.

Observemos que, se $b \in T[E]$ então $b(c_1) \in T \subseteq TC$ e assim $c_1 \in TC[E]$. Por indução, obtemos que $q_i \in TC$, $i = 1, 2, ..., n$ e assim $r \in TC[E]$. Um argumento semelhante pode ser usado para o caso $b \in J[E]$. O lema está demonstrado.

Lema 3.1.3 *Com a mesma notação, temos:*
(i) $b \in QM_C(I_0) \Leftrightarrow \exists J \in \mathcal{D}$ *tal que* $bJ \subseteq I_0$
(ii) $Q[E]M_C(I_0) = QM_C(I_0) \lhd Q[E]$

Demonstração : (i) Suponhamos $b = \sum_{i=1}^{n} q_i m_i$, com $q_i \in Q$ e $m_i \in M_C(I_0)$ para qualquer $i \in \Lambda = \{1, 2, ..., n\}$. Existem $F \in \mathcal{D}$ e $0 \neq H \lhd R$ tais que $q_i F \subseteq R$ e $m_i H \subseteq I_0$ para todo $i \in \Lambda$. Conseqüentemente, $bFH \subseteq I_0$ com $FH \in \mathcal{D}$.

Reciprocamente, seja $b = \sum_{j=1}^{t} q'_j m'_j + r$, onde $q'_j \in Q$ e $m'_j \in M_C(I_0)$ para $j \in \{1, 2, ..., t\}$ e, ou $r = 0$ ou r é um *resto módulo* I.

Suponhamos que exista $J \in \mathcal{D}$ com $bJ \subseteq I_0$. Também $(\sum_{j=1}^{t} q'_j m'_j)J' \subseteq I_0$ para um certo $J' \in \mathcal{D}$, como acima. Então, $r(J \cap J') \subseteq I_0$, pois $r = b - \sum_{j=1}^{t} q'_j m'_j$. Assim, $r(J \cap J') = 0$ e, conseqüentemente, $r = 0$. Logo, $b \in QM_C(I_0)$.

(ii) Sejam $e \in E$, $m \in M_C(I_0)$ e $q \in Q$. Então, existe $0 \neq H \lhd R$ tal que $emH \subseteq eI_0 \subseteq I_0$ e $meH = mHe \subseteq I_0 e \subseteq I_0$. Por (i), temos que $em, me \in QM_C(I_0)$. Conseqüentemente, $qem, meq \in QM_C(I_0)$ e, por distributividade, obtemos $Q[E]M_C(I_0) \subseteq QM_C(I_0)$. A outra inclusão é óbvia. Logo, $Q[E]M_C(I_0) = QM_C(I_0)$. O resto é imediato.

Da demonstração deste lema obtemos o seguinte

Corolário 3.1.4 *Mantendo a notação anterior, temos:*
(i) $[I]_T = Q[E]M_C(I_0) \cap T[E]$
(ii) $[I]_T = \{b \in T[E] \mid \exists J \in \mathcal{D} : bJ \subseteq I_0\}$

Demonstração : Seja $b \in T[E]$. Existe $J \in \mathcal{D}$ tal que $bJ \subseteq I_0$ e então, pelo lema 3.1.3, $b \in QM_C(I_0) \cap T[E] = Q[E]M_C(I_0) \cap T[E]$. Por outro lado, se $b \in Q[E]M_C(I_0) \cap T[E]$ então $b = \sum_{i=1}^{n} q_i m_i$, onde $q_i \in TC$ e $m_i \in M_C(I_0)$ (lema 3.1.2), para cada $i \in \{1, 2, ..., n\}$. Como na prova de 3.1.3(i) , podemos obter $bH \subseteq I$ onde $0 \neq H \lhd T$. Conseqüentemente, $b \in [I]_T$.

Finalmente, se $b \in [I]_T$, obtemos (novamente como na prova de 3.1.3(i)) que $b \in QM_C(I_0)$. Então, existe $J \in \mathcal{D}$ com $bJ \subseteq I_0$. Isto completa a prova.

Com estes resultados, podemos obter a correspondência procurada entre os ideais de $C[E]$ e os ideais fechados de $R[E]$ e de $T[E]$, para T um anel de quocientes à direita de R.

Teorema 3.1.5 *Sejam R um anel primo e T um anel de quocientes à direita de R. Então existe uma correspondência biunívoca entre:*
(i) o conjunto dos ideais fechados de $R[E]$
(ii) o conjunto dos ideais fechados de $T[E]$
(iii) o conjunto dos ideais de $C[E]$
Além disso, esta correspondência associa o ideal fechado I de $R[E]$ com o ideal fechado I^* de $T[E]$ e o ideal K de $C[E]$ se $I^* \cap R[E] = I$ e $I^* = Q[E]K \cap T[E]$.

Demonstração : Se J é um ideal fechado de $T[E]$ e $J_0 = J \cap R[E]$, então $J = Q[E]M_C(J_0) \cap T[E]$ e $[J_0]_R = Q[E]M_C(J_0) \cap R[E] = J \cap R[E]$ pelo corolário 3.1.4. Assim J_0 é fechado. Se J' é outro ideal fechado com $J_0 = J' \cap R[E]$, o mesmo corolário nos fornece que $J' = J$.

Por outro lado, seja I um ideal fechado de $R[E]$. Então $L = Q[E]M_C(I) \cap T[E]$ é um ideal de $T[E]$ e $L_0 = L \cap R[E] = [I]_R = I$. Conseqüentemente $[L] = Q[E]M_C(L_0) \cap T[E] = Q[E]M_C(I) \cap T[E] = L$, então L é fechado e satisfaz $L \cap R[E] = I$. Isto estabelece a correspondência entre (i) e (ii).

Para completar a prova é suficiente mostrar a correspondência (ii) e (iii) para $T = Q$.

Se I é um ideal fechado de $Q[E]$, então $I = Q[E]M_C(I_0)$, onde $I_0 = I \cap R[E]$. Logo $I \cap C[E]$ é um ideal fechado de $Q[E]$ e, como $M_C(I_0) \subseteq I \cap C[E]$ ($M_C(I_0) \subseteq [I] \cap C[E] = I \cap C[E]$), temos que $I \supseteq Q[E](I \cap C[E]) \supseteq Q[E]M_C(I_0) = I$. Conseqüentemente, $I = Q[E](I \cap C[E])$.

Reciprocamente, seja $K \lhd C[E]$ e $J = Q[E]K$. ($J \lhd Q[E]$). Basta mostrar que $M_C(J_0) \subseteq K$ e teremos $[J] = Q[E]M_C(J_0) \subseteq Q[E]K = J$, portanto $[J] = J$, ou seja, J é um ideal fechado de $Q[E]$.

Suponhamos que $M_C(J_0) \nsubseteq K$. Seja $m \in M_C(J_0)$ tal que $m \notin K$. Temos que $Q[E] = Q \otimes_C C[E]$. Seja $\{v_i\}_{i\in\Omega}$ base de K sobre C. Também, $m \in C[E]$ e $\{v_i\}_{i\in\Omega} \cup \{m\}$ é C-independente. Conseqüentemente, $\{v_i\}_{i\in\Omega} \cup \{m\}$ é linearmente independente em $Q[E]$. Seja H tal que $mH \subseteq J = QK$. Portanto, para $h \in H$, existem $q_i \in Q$, com $i \in \Omega$, tal que $mh = \sum_{i\in\Omega} q_i v_i$. Conseqüentemente, temos

$0 = mh - \sum_{i\in\Omega} q_i v_i$ e portanto $h = 0$. Assim, $H = 0$. Logo, temos que $\{v_i\} \cup \{m\}$ é linearmente dependente, ou seja, $M_C(I_0) \subseteq K$. O teorema está demonstrado.

A correspondência determinada pelo teorema 3.1.5 preserva a propriedade de um ideal ser primo (teorema 3.1.7). Vejamos o

Lema 3.1.6 *As seguintes condições são equivalentes:*
(i) $R[E]$ *é primo*
(ii) $T[E]$ *é primo, onde* T *é um anel de quocientes à direita de* R
(iii) $C[E]$ *é primo*

Demonstração : Basta ver que (iii)⇒(i), já que (i)⇒(ii) e (ii)⇒(iii). Sejam A, B ideais de $R[E]$ com $AB = 0$ e assumimos que $C[E]$ é primo. Então, ou $A \cap R = 0$ ou $B \cap R = 0$. Nós podemos assumir que $A \cap R = 0$ e $A \neq 0$, assim, $0 \neq M_C(A) \subseteq C[E]$. Seja $0 \neq a \in M_C(A)$ e escolhemos um $0 \neq H \lhd R$ com $Ha \subseteq A$. Conseqüentemente, $HaB = 0$. Se $B \cap R \neq 0$, nós facilmente obtemos $a = 0$. Assim, também podemos assumir que $B \cap R = 0$ e suponhamos $B \neq 0$. Neste caso, existe $0 \neq b \in M_C(B)$ e um ideal F de R com $bF \subseteq B$. Conseqüentemente, $HaebF = 0$ e assim, segue que $aeb = 0$, para todo $e \in E$. Então, $aC[E]b = 0$, contradição. Logo, $B = 0$ e a prova está completa.

Nós agora obtemos um segundo resultado forte desta secção:

Teorema 3.1.7 *Seja* R *um anel primo e* T *um anel de quocientes à direita de* R. *Então, a mesma correspondência do teorema 3.1.5 é uma correspondência entre os seguintes conjuntos:*
(i) o conjunto de todos ideais primos P *de* $R[E]$ *com* $P \cap R = 0$
(ii) o conjunto de todos ideais primos P^* *de* $T[E]$ *com* $P^* \cap T = 0$
(iii) o conjunto de todos ideais primos de $C[E]$

Demonstração : Pelo lema anterior, podemos considerar somente ideais não nulos. Suponhamos que P é um ideal fechado de $R[E]$ e P^* é o ideal fechado de $T[E]$ com $P^* \cap R[E] = P$.

Se P é um ideal primo de $R[E]$ e $A \supseteq P^*$, $B \supseteq P^*$ são ideais de $T[E]$ tais que $AB \subseteq P^*$, então $(A \cap R[E])(B \cap R[E]) \subseteq P$. Conseqüentemente, ou $A \cap R[E] = P$ ou $B \cap R[E] = P$. Assumimos que $A \cap R[E] = P$. Como
$Min(P^*) = Min(P) = Min(A \cap R[E]) = Min(A)$ e P^* é fechado, temos que $A = P^*$ e, portanto, P^* é um ideal primo de $T[E]$.

Reciprocamente, assumimos que P^* é primo. Sejam A, B ideais de $R[E]$ com $A \supseteq P$, $B \supseteq P$ e $AB \subseteq P$. Sejam $a \in A$, $b \in [B]_R$ e $0 \neq H \lhd R$ tal que $bH \subseteq B$. Conseqüentemente $abH \subseteq P$ e assim $ab \in P$, pois P é fechado. Então, $A[B]_R \subseteq P$. Agora, se $A \not\subseteq P$ escolhemos $a \in A \setminus P$.

Sejam B^* o ideal fechado de $T[E]$ com $B^* \cap R[E] = [B]_R$ e $c \in B^*$. Existe $F \in \mathcal{D}$ satisfazendo $cF \subseteq B^* \cap R[E] = [B]_R$. Conseqüentemente, $acF \subseteq P \subseteq P^*$ e $ac \in P^*$ pelo corolário 3.1.4(i). Logo, $aB^* \subseteq P^*$, assim, $B^* \subseteq P^*$ então $B = P$. A correspondência entre (i) e (ii) está provada.

Para provar a correspondência entre (ii) e (iii) é suficiente provar para $T = Q$, como na demonstração do teorema 3.1.5. Seja K um ideal de $C[E]$ e $L = Q[E]K$. Como $L \cap C[E] = K$, é claro que K é primo se L é primo. Reciprocamente, assumimos que K é um ideal primo e sejam A, B ideais de $Q[E]$ com $AB \subseteq L$. Como L é fechado, vemos facilmente que, como acima, $A[B]_Q \subseteq L$. Se $M_C(A \cap R[E]) \subseteq K$, obtemos $[A]_Q = Q[E]M_C(A \cap R[E]) \subseteq L$, o que completa a prova. Assumimos então que existe $m \in M_C(A \cap R[E]) \setminus K$ e seja $0 \neq H \lhd Q$ tal que
$m([B]_Q \cap C[E])H = mH([B]_Q \cap C[E]) \subseteq L$. Conseqüentemente,
$m([B]_Q \cap C[E]) \subseteq L \cap C[E] = K$ e obtemos $[B]_Q \cap C[E] \subseteq K$. Assim,
$[B]_Q = Q[E]([B]_Q \cap C[E]) \subseteq L$. A prova está completa.

O corolário a seguir é a aplicação dos teoremas 3.1.5 e 3.1.7 para o caso particular $R[E] = R[X]$. Sua demonstração pode ser feita de forma independente desta secção (ver [5]).

Corolário 3.1.8 *Sejam R um anel primo e T um anel de quocientes à direita de R. Então existe uma correspondência biunívoca entre os seguintes:*
(i) o conjunto de todos os ideais principais fechados (respectivamente ideais primos R − disjuntos) de $R[X]$
(ii) o conjunto de todos os ideais principais fechados (respectivamente ideais primos T − disjuntos) de $T[X]$
(iii) o conjunto de todos os polinômios mônicos (respectivamente ideais maximais) de $C[X]$.
Além disso, esta correspondência associa $[f]_R$ com $[f']_T$ e $f_0 \in C[X]$ (respectivamente P com P^* e M) se $[f']_T \cap R[X] = [f]_R$ e $Q[X]f_0 \cap T[X] = [f']_T$ (respectivamente se $P^* \cap R[X] = P$ e $P^* = Q[X]M \cap T[X]$).

3.2 Caracterização de Ideais Primos em R[X]

Como antes, R é um anel primo com unidade e Q o anel completo de quocientes à direita de R. Nesta secção estudamos a representação dos ideais primos $R-disjuntos$ do anel de polinômios $R[X]$. Também caracterizamos os ideais fechados (corolário 3.2.2) e os ideais primos (corolário 3.2.3) de $T[X]$, onde T é um anel de quocientes à direita de R. Os resultados desta secção, obtidos a partir do estudo dos polinômios completamente irredutíveis, fazem parte de um manuscrito não publicado do Prof. M.Ferrero. Começamos pelo seguinte

Lema 3.2.1 *Sejam T um anel de quocientes à direita de R e $f \in \Gamma_T$. Então existe um único $f_0 \in C[X]$, mônico e tal que $[f]_T = Q[X]f_0 \cap T[X]$.*

Demonstração : Seja $I = [f]_T \cap R[X]$ e $n = \partial I$. Então $\partial[f]_T = n$. De fato, se $g \in I$, temos que $g \in [f]_T$ e, portanto, $\partial[f]_T \leq \partial I = n$. Reciprocamente, seja $g = x^k a_k + ... + a_0 \in [f]_T$. Existe $J \in \mathcal{D}$ tal que $a_i J \subseteq R$ para todo $i = 0, 1, 2, ..., k$. Seja $j \in J$ com $0 \neq h = gj \in R[X]$ e portanto $h \in I$. Mas $\partial h \leq \partial g$, ou seja, $\partial I \leq \partial[f]_T$. Logo $\partial[f]_T = \partial I = n$.

Se $b \in \tau(I) = \{o\} \cup \{a \mid \exists f \in I : \partial f = n \text{ e } lc(f) = a\}$ $\quad (\tau \lhd R)$ então existe um único $g = x^n b + x^{n-1} b_{n-1} + ... + b_0 \in I$ tal que $lc(g) = b$. Conseqüentemente, a função $\alpha_i : \tau(I) \to R$ dada por $\alpha_i(b) = b_i$ está bem definida e é um homomorfismo de R-módulos. Portanto existe $c_i \in C$ com $c_i b = b_i$ para todo $i = 0, 1, 2, ..., n-1$.

Seja $f_0 = X^n + X^{n-1}c_{n-1} + ... + c_0 \in C[X]$ e seja $f_1 \in I$ com $\partial(f_1) = n$ e $lc(f_1) = a$. Portanto, $f_1 = f_0 a = a f_0$. Como f_0 é mônico,
$\partial(f_0 Q[X] \cap T[X]) = n = \partial([f]_T)$. Se $g \in [f]_T = [f_1]_T$, existe $0 \neq H \lhd T$ satisfazendo $gha \subseteq T[X]f_1 \subseteq Q[X]f_0$. Sejam $p, r \in Q[x]$ tais que $g = pf_0 + r$ onde ou $\partial r < n$ ou $r = 0$. Para $h \in H$, $rha = gha - phaf_0 \in Q[X]f_0$ e, portanto, $rHa = 0$. Sabemos que existe $J \in \mathcal{D}$ tal que $rJ \subseteq R[X]$, e assim $rJH = 0$. Como T é primo, $rJ = 0$ e $R = 0$, pois $J \in \mathcal{D}$. Logo, $g \in Q[X]f_0 \cap T[X]$ e, pelo corolário 2.2.8, concluímos que $[f]_T = Q[X]f_0 \cap T[X]$.

Finalmente, se g_0 é um polinômio mônico em $C[X]$ tal que
$[f]_T = Q[X]g_0 \cap T[X]$, então $\partial(f_0 - g_0) < n$ e existe $0 \neq K \lhd R$ satisfazendo $(f_0 - g_0)K \subseteq [f]_T$. Conseqüentemente, $(f_0 - g_0)K = 0$, então temos $f_0 = g_0$, já que $T[X]$ é primo. O lema está demonstrado.

Usando este lema, obtemos o seguinte corolário:

Corolário 3.2.2 *Seja I um ideal $T-disjunto$ de $T[X]$. Então I é um ideal principal fechado de $T[X]$ se e somente se $I = Q[X]f_0 \cap T[X]$ para algum polinômio mônico $f_0 \in C[X]$.*

Demonstração : Suponhamos que I é um ideal principal fechado de $T[X]$. Então existe $f \in \Gamma_T$ tal que $I = [f]_T$. Por 3.2.1, existe $f_0 \in C[X]$ mônico que satisfaz $I = Q[X]f_0 \cap T[X]$. Reciprocamente, seja $I = Q[X]f_0 \cap T[X]$, onde $f_0 = X^n + X^{n-1}c_{n-1} + ... + c_0 \in C[X]$, então $\partial I = n$. De fato, se $g \in I$ existe $k \in Q[X]$ tal que $g = kf_0 = f_0k$. Como f_0 é mônico, temos que $\partial g = \partial k + \partial f_0 \geq \partial f_0 = n$. Assim, $\partial I \geq n$. Por outro lado, existe $J \in \mathcal{D}$ tal que $c_iJ \subseteq R$ para todo $i = 0, 1, 2, ..., n-1$. Conseqüentemente, para $0 \neq j \in J$, temos que $h = f_0j = jf_0 \in R[X]$, portanto $h \in I$. Mas $\partial h = \partial f_0 = n$, logo $\partial I = n$. Seja $f \in I$ tal que $\partial f = n$ e $lc(f) = a$. Como $\partial f_0 = n$, obtemos que $f = f_0a = af_0$. Assim, como na demonstração do lema 3.2.1, $[f]_T = I$ o que completa a prova.

Como conseqüência imediata de 3.2.1 e 2.2.15(ii), obtemos o seguinte

Corolário 3.2.3 *Sejam R um anel primo e T um anel de quocientes à direita de R. Um ideal $T-disjunto$ P de $T[X]$ é primo se e somente se $P = Q[X]f_0 \cap T[X]$ para algum polinômio mônico irredutível $f_0 \in C[X]$.*

Corolário 3.2.4 *Sejam K um fecho algébrico de C, $Q_1 = Q \otimes_C K$ e P um ideal primo de $R[X]$. Então:*
(i) existe $c \in K$ tal que $P = Q_1[X](X-c) \cap R[X]$
(ii) existe um número finito de ideais primos $Q_1-disjuntos$ de $Q_1[X]$, $P_1, ..., P_t$, tais que $P_i \cap R[X] = P$ para todo $i = 1, ..., t$.

Demonstração : (i) Sejam P^* um ideal primo $Q-disjunto$ de $Q[X]$ tal que $P^* \cap R[X] = P$ e $f_0 \in C[X]$ um polinômio irredutível tal que $P^* = Q[X]f_0$ (corolário 3.2.3). Seja c uma raiz de f_0 em K, logo $P_1 = Q_1[X](X-c)$ é um ideal primo $Q_1-disjunto$ de $Q_1[X]$ e $P_1 \cap Q[X] \supseteq P^*$. Assim, $P^* = P_1 \cap Q[X]$ e, conseqüentemente, temos $P = Q_1[X](X-c) \cap R[X]$.

(ii) Seja P' um ideal primo $Q_1-disjunto$ de $Q_1[X]$ tal que $P' \cap R[X] = P$. Então, $P' = Q_1[X](X-d)$ para algum $d \in K$ e $P' \cap Q[X] = P^*$, onde P^* é como em (i). Assim, $f_0 \in P'$ e, conseqüentemente, d é uma raiz de f_0. Agora é claro que o número máximo de ideais primos $Q_1-disjuntos$ de $Q_1[X]$ é o número de raízes de f_0 em K (que é ∂f_0). Aprova está completa.

Corolário 3.2.5 *Sejam R um anel qualquer e P_0 um ideal primo de R. Então, existe um corpo F e uma correspondência biunívoca entre o conjunto de todos os ideais primos P de $R[X]$ tais que $P \neq P_0[X]$ e $P \cap R = P_0$, e o conjunto de todos os polinômios mônicos irredutíveis de $F[X]$.*

Demonstração : Basta tomarmos F como o centróide extendido do anel primo $\frac{R}{P_0}$ e aplicarmos o corolário 3.2.3.

Consideramos agora T um anel de quocientes à direita de R contendo a clausura central RC de R e $f_0 \in C[X]$. Então, $Q[X]f_0 \cap T[X] = f_0T[X]$. Conseqüentemente, obtemos que, neste caso, os ideais que são principais fechados em $T[X]$ são do tipo $T[X]f$, onde f é um polinômio mônico de $T[X]$.

Se R é um domínio de fatorização única comutativo e $f \in R[X]$, então $f \in \Gamma_R$ (em anéis de polinômios comutativos, todo polinômio pertence à Γ) e $[f]_R = R[X]f_1$, para algum $f_1 \in R[X]$. De fato, sejam F o corpo de frações de R e $f_0 \in F[X]$ mônico tal que $[f]_R = F[X]f_0 \cap R[X]$. Se $g \in [f]_R$ então $g = kf_0$ para algum $k \in F[X]$. Seja $d \in R$ tal que $f_1 = df_0 \in R[X]$ e f_1 é primitivo. Então $d^{-1}k \in R[X]$, pois $d^{-1}kf_1 = f_0k = g$. Assim, $g = d^{-1}kf_1 \in R[X]f_1$ e conseqüentemente, $[f]_R \subseteq R[X]f_1 \subseteq [f]_R$.

Em 3.2.3 obtemos uma representação dos ideais primos $T-$*disjuntos* de $T[X]$. Mas, para isto, precisamos considerar Q, o anel completo de quocientes à direita de R. A seguir, obteremos uma representação dos ideais primos $R-$*disjuntos* de $R[X]$ (teorema 3.2.10), onde não será necessário considerar o anel Q. Para isto, definiremos o que é um polinômio completamente irredutível em $R[X]$.

Definição 3.2.6 *Sejam R um anel e $f \in \Gamma_R$. Dizemos que f é completamente irredutível em $R[X]$ se f satisfaz a seguinte propriedade: Se existem $h \in R[X]$, $b \in R$ e $g \in \Gamma_R$ tais que $fb = hg$ e $fb \neq 0$ então $\partial g = \partial f$.*

Lema 3.2.7 *Sejam R um anel primo e $f \in R[X]$. Se $f \in \Gamma$ então $[fb] = [f]$ para qualquer $b \in R$ tal que $fb \neq 0$.*

Demonstração : Sejam $f \in \Gamma$ e $b \in R$ tais que $fb \neq 0$. É fácil verificar que $fb \in \Gamma$ e que $[f] \subseteq [fb]$. Mas, $\partial[f] = \partial f = \partial fb = \partial[fb]$, portanto $[f] = [fb]$. O lema está demonstrado.

A propriedade que define um polinômio completamente irredutível em $R[X]$, onde R é um anel primo, pode ser reformulada de modo equivalente: Se existem

$h \in \Gamma$, $b \in R$ e $g \in R[X]$ tais que $fb = hg$ e $fb \neq 0$, então $\partial h = \partial f$. De fato, sejam $0 \neq fb = hg$, $h \in \Gamma$, $\partial h < \partial f$ e f completamente irredutível em $R[X]$. Mas, $0 \neq fb \in hR[X] \subseteq [h]$, logo $[f] = [fb] \subseteq [h]$. Assim, se $d = lc(f)$, existe $0 \neq H \lhd R$ satisfazendo $fHd \subseteq R[X]h$. Conseqüentemente, para algum $r \in H$ temos que $0 \neq frd = g'h$, onde $g' \in R[X]$, $h \in \Gamma$ e $\partial h < \partial f$, o que é uma contradição.
A recíproca é análoga.

Lema 3.2.8 *Sejam R um domínio comutativo e $f \in R[X]$. Então f é completamente irredutível em $R[X]$ se e somente se f é irredutível em $F[X]$, onde $F = cf(R)$ é o corpo de frações de R.*

Demonstração : Suponhamos que f é irredutível em $F[X]$, ou seja, existem $h, g \in F[X]$ tais que $f = hg$ com $\partial h < \partial f$ e $\partial g < \partial f$. Sabemos que existem $p, q \in R$ não nulos tais que $ph \in R[X]$ e $qg \in R[X]$. Conseqüentemente, $fpq = (ph)(qg)$. Logo fb é irredutível em $R[X]$, onde $b = pq$. Reciprocamente, suponhamos que fb seja redutível em $R[X]$, ou seja, existem $h, g \in R[X]$ tais que $fb = hg$ com $\partial h < \partial(fb) = \partial f$ e $\partial g < \partial(fb) = \partial f$. Assim, $f = (\frac{1}{b}h)g$, portanto, f é redutível em $F[X]$. A prova está completa.

Lema 3.2.9 *Sejam R um domínio de fatorização única comutativo e $f \in R[X]$. Então f é irredutível em $R[X]$ se e somente se f é completamente irredutível em $R[X]$.*

Demonstração : Se f é irredutível e primitivo em $R[X]$ então f é irredutível em $F[X]$, onde $F = cf(R)$. De 3.2.8, f é completamente irredutível em $R[X]$. Se f não é primitivo, escrevemos $f = df'$ com $d \in R$ e f' primitivo. Como f é irredutível em $R[X]$, temos que f' também é. Pela primeira parte, f' é completamente irredutível em $R[X]$. Agora, se existe $b \in R$ tal que $0 \neq fb$ é redutível em $R[X]$, então $f'db$ é redutível em $R[X]$, o que é uma contradição. Logo f é completamente irredutível em $R[X]$. A recíproca é evidente.

De um modo geral, a classe dos polinômios irredutíveis num anel $R[X]$ é maior que a classe dos polinômios completamente irredutíveis em $R[X]$. Vejamos o seguinte exemplo:

Seja D o domínio de integridade das séries de potências de $\mathbb{Q}[[Y]]$ com coeficiente de Y nulo, onde $\mathbb{Q}$ é o corpo dos números racionais. Então $F = cf(D) = \mathbb{Q}[[Y, Y^{-1}]]$. Agora, $(X^2 - Y^2) \in D[X]$ e $(X^2 - Y^2)$ não é completamente irredutível em $D[X]$, pois $Y^4(X^2 - Y^2) = Y^4X^2 - Y^6 = (Y^2X - Y^3)(Y^2X + Y^3)$. Mas se $(X^2 - Y^2)$ for redutível em $D[X]$, temos que existem $\alpha, \beta \in D$, tais que $(X^2 - Y^2) = (X-\alpha)(X-\beta)$ (pois $\partial(X^2 - Y^2) = 2$). Sejam $\alpha = q_0 + q_2Y^2 + \ldots$ e $\beta = p_0 + p_2Y^2 + \ldots$ onde $q_i, p_i \in \mathbb{Q}, \forall i \in \mathbb{N} \setminus \{1\}$. Assim, $(X^2 - Y^2) = (X-\alpha)(X-\beta) = X^2 - (\alpha+\beta)X + \alpha\beta$, portanto $-Y^2 = \alpha\beta = (q_0 + q_2Y^2 + \ldots)(p_0 + p_2Y^2 + \ldots)$. Conseqüentemente, $q_0p_0 = 0$ e $q_2p_0 + q_0p_2 = -1$. Também, $\alpha + \beta = 0$, e obtemos que $\alpha = -\beta$. Assim, temos que $q_0 = p_0 = 0$ e $Y^2 = \beta^2$, o que é um absurdo, pois $\beta^2 = (p_0 + p_2Y^2 + \ldots)^2 = (p_2Y^4 + \ldots)$. Logo $(X^2 - Y^2)$ é irredutível em $D[X]$.

Vejamos agora o teorema que dá uma caracterização para os ideais primos de $R[X]$.

Teorema 3.2.10 *Sejam R um anel primo e P um ideal $R-$disjunto de $R[X]$. P é um ideal primo se e somente se P é um ideal principal fechado de $R[X]$ e, para todo $f \in P$ tal que $\partial f = \partial P$, f é completamente irredutível em $R[X]$.*

Demonstração : Suponhamos que P é um ideal primo de $R[X]$, portanto P é um ideal fechado. Sejam $f \in P$ tal que $\partial f = \partial P$ e $b \in R$ satisfazendo $0 \neq fb = hg$, com $g \in \Gamma$ tal que $\partial g < \partial f$ e $h \in R[X]$. Segue que, $P = [f] = [fb] \subset [g]$, o que contradiz 2.2.15(ii). Logo f é completamente irredutível em $R[X]$.

Reciprocamente, sejam P um ideal principal fechado de $R[X]$ e $f \in P$ tal que $[f] = P$. Suponhamos que P não seja primo de $R[X]$. Então, pelo corolário 2.2.15(ii), existe $g \in \Gamma$ tal que $f \in [f] \subset [g]$, com $1 \leq \partial g < \partial f$. Logo, existem $0 \neq H \lhd R$ tal que $fHc \subseteq R[X]g$, onde $c = lc(g)$, e $r \in H$ com $0 \neq f(rc) = hg$, onde $g \in \Gamma$ e $\partial g < \partial f$. Ou seja, f não é completamente irredutível em $R[X]$, o que é uma contradição. Assim, P é um ideal primo de $R[X]$ e o teorema está demonstrado.

Capítulo 4

Decomposição Primária

4.1 Fatorização de um Ideal Fechado em R[X]

Seja R um anel primo com centróide extendido C e anel completo de quocientes à direita Q. O objetivo mais importante desta secção é demonstrar o seguinte

Teorema 4.1.1 *Seja I um ideal principal fechado de $R[X]$. Então, existe um conjunto finito de ideais primos $R-$disjuntos $P_1, ..., P_t$ de $R[X]$ e números naturais $e_1, ..., e_t$ tais que $I = \cap_{i=1}^{t}[P_i^{e_i}]$ onde $[P_i^{e_i}]$ é o ideal principal fechado associado com $P_i^{e_i}$. Além disso, esta representação é única a menos da ordem dos fatores.*

Nós começamos esta secção provando um caso particular do teorema 4.1.1 (lema 4.1.3). Vejamos primeiro o seguinte

Lema 4.1.2 *Sejam f e g dois polinômios de $C[X]$ tais que $MDC\{f,g\} = 1$. Então $Q[X]fg = Q[X]f \cap Q[X]g$.*

Demonstração : Desde que $f, g \in C[X]$ temos que $Q[X]fg \subseteq Q[X]f \cap Q[X]g$. Reciprocamente, sejam $f, g \in C[X]$ tais que $MDC\{f,g\} = 1$ e $p \in Q[X]f \cap Q[X]g$. Então, existem $q, q' \in Q[X]$ tais que $p = qf = q'g$, e $a, b \in C[X]$, satisfazendo $1 = af + bg$. Conseqüentemente, $p = afq'g + bgqf = (aq' + bq)fg \in Q[X]fg$.
A prova está completa.

Lema 4.1.3 *Seja I um ideal principal fechado de $Q[X]$. Então, existe um conjunto finito de ideais primos $Q-$disjuntos $P_1, ..., P_t$ de $Q[X]$, e números naturais $e_1, ..., e_t$ tais que $I = \cap_{i=1}^{t} P_i^{e_i}$. Esta representação é única a menos da ordem dos fatores.*

Demonstração : Pelo corolário 3.2.2, existe um polinômio mônico $f_0 \in C[X]$ tal que $I = Q[X]f_0$. Suponhamos que $f_0 = p_1^{e_1}...p_t^{e_t}$ é a decomposição de f_0 como um produto de fatores mônicos irredutíveis em $C[X]$. Então, pelo lema anterior, $I = Q[X]p_1^{e_1}...p_t^{e_t} = \cap_{i=1}^{t} Q[X]p_i^{e_i} = \cap_{i=1}^{t}(Q[X]p_i)^{e_i}$, onde $Q[X]p_i$ é um ideal primo de $Q[X]$, se p_i é irredutível.

Sejam P um ideal primo $Q-$*disjunto* de $Q[X]$ e e um número natural satisfazendo $I \subseteq P^e$. Consideremos $p \in C[X]$ um polinômio mônico irredutível tal que $P = Q[X]p$. Conseqüentemente, p^e divide f_0 em $C[X]$ e assim, existe $1 \le i \le t$ tal que $P = P_i$, com $1 \le e \le e_i$. A unicidade agora é facilmente obtida.

Lema 4.1.4 *Sejam P um ideal primo $R-$ disjunto de $R[X]$ e $p \in C[X]$ um polinômio mônico irredutível tal que $P = Q[X]p \cap R[X]$. Então, o ideal principal fechado associado com P^e é $[P^e] = Q[X]p^e \cap R[X]$ para qualquer número natural $e \ge 1$.*

Demonstração : Seja $f \in Q[X]p^e \cap R[X]$. Então, existe $g \in Q[X]$ tal que $f = gp^e$ e, conseqüentemente, $\partial f \ge \partial(p^e)$, já que p é mônico. Assim, $\partial(Q[X]p^e \cap R[X]) \ge \partial(p^e)$. Também, $\partial P^e \ge \partial(p^e)$ pois $P^e \subseteq Q[X]p^e \cap R[X]$. Agora, desde que R é primo, $\tau(P)$ não é nilpotente e então dado um inteiro $e \ge 1$, existem $a_1, ..., a_e \in \tau(P)$ tais que $a_1 \cdot ... \cdot a_e \ne 0$. Portanto, existe um polinômio em P^e de grau igual a $\partial(p^e)$. Logo, $\partial(P^e) = \partial(p^e) = \partial(Q[X]p^e \cap R[X])$. O resultado segue por 2.2.8 e por 3.2.2, usando novamente que $P^e \subseteq Q[X]p^e \cap R[X]$.

Demonstração do Teorema 4.1.1 : Seja $f_0 \in C[X]$, mônico tal que $I = Q[X]f_0 \cap R[X]$. Pelo lema 4.1.3 temos que $Q[X]f_0 = \cap_{i=1}^{t}(Q[X]p_i)^{e_i}$, onde $f_0 = p_1^{e_1}...p_t^{e_t}$ é a decomposição de f_0 em fatores irredutíveis em $C[X]$. Conseqüentemente, $P_i = Q[X]p_i \cap R[X]$ é um ideal primo de $R[X]$ e o ideal principal fechado associado com P^{e_i} é $[P_i^{e_i}] = Q[X]p_i^{e_i} \cap R[X] = (Q[X]p_i)^{e_i} \cap R[X]$, pelo lema 4.1.4. Assim, temos que $I = \cap_{i=1}^{t}(Q[X]p_i)^{e_i} \cap R[X] = \cap_{i=1}^{t}[P_i^{e_i}]$.

Suponhamos que $I = \cap_{j=1}^{s}[L_j^{e'_j}]$, onde L_j é primo para todo $1 \le j \le s$. Então, $[L_j^{e'_j}] = Q[X]q_j^{e'_j} \cap R[X]$, onde $q_j \in C[X]$ é um polinômio mônico irredutível para todo $1 \le j \le s$. Logo, $I = J \cap R[X]$ onde $J = \cap_{j=1}^{s} Q[X]q_j^{e'_j}$ é um ideal principal fechado de $Q[X]$. Conseqüentemente, pelo teorema 3.1.8, $J = \cap_{i=1}^{t} Q[X]p_i^{e_i}$. A unicidade decorre do lema 4.1.3. O teorema está demonstrado.

Como conseqüência direta do teorema 4.1.1, obtemos dois corolários:

Corolário 4.1.5 *Seja I um ideal $R-$ disjunto de $R[X]$, onde R é um anel primo. Então:*
(i) existe um número finito de ideais primos $R-$ disjuntos $P_1, ..., P_t$ de $R[X]$ e números naturais $e_1, ..., e_t$ unicamente determinados tais que $[I] = \cap_{i=1}^{t}[P_i^{e_i}]$.
(ii) I é um ideal principal fechado de $R[X]$ se e somente se I é intersecção finita de ideais, cada um dos quais é um ideal principal fechado associado à uma potência de um ideal primo.

Corolário 4.1.6 *Uma intersecção de ideais primos distintos $R-$ disjuntos de $R[X]$ é não nula se e somente se é uma intersecção finita.*

Se P é um ideal primo $Q-$ *disjunto* de $Q[X]$ então $P = Q[X]p$, para algum polinômio irredutível $p \in C[X]$. Então, $P^e = Q[X]p^e$ é também um ideal principal fechado de $Q[X]$. O exemplo a seguir (já estudado na secção 3.2) nos mostra que, em geral, uma potência de um ideal primo não precisa ser um ideal principal fechado:

Sejam $\mathbb{Q}$ o corpo dos números racionais e D o domínio de integridade de todas as séries de potências de $\mathbb{Q}[[Y]]$ com coeficiente de Y nulo. O corpo de frações de D é $F = \mathbb{Q}[[Y, Y^{-1}]]$. Seja $P^* = (X - Y)F[X]$. P^* é um ideal primo de $F[X]$, pois $\partial(X - Y) = 1$ (logo irredutível). Então $P = P^* \cap D[X]$ é um ideal primo de $D[X]$. Temos que, se $f \in P$ e $\partial f = 1$, então $f = (X - Y)\sum_{i=2}^{\infty} q_i Y^i$, onde $q_i \in \mathbb{Q}$. Conseqüentemente, se $g \in P^2$, $g = (X^2 - 2XY + Y^2)\sum_{j\geq 4} q_j' Y^j$, onde $q_j' \in \mathbb{Q}$. Seja, agora $h = (X^2 - 2XY + Y^2)Y^2 \in (X - Y)^2 F[X] \cap D[X]$. Segue que $h \notin P^2$ logo $P^2 \not\subseteq P^{*2} \cap D[X]$.

A seguir, provamos que a situação deste exemplo não ocorre se o ideal primo é maximal.

Proposição 4.1.7 *Seja M um ideal maximal $R-$ disjunto de $R[X]$. Então:*
(i) se T é um anel de quocientes à direita de R que contém a clausura central RC de R, então T é simples.
(ii) M^i é um ideal principal fechado de $R[X]$, para qualquer $i \geq 1$.

Demonstração : (i) Seja $M^* = T[X]f_0$, um ideal primo $T-$ *disjunto* de $T[X]$ tal que $M^* \cap R[X] = M$, onde $f_0 \in C[X]$ (corolário 3.1.8). Como M é maximal em $R[X]$, M^* é maximal em $T[X]$. Seja $0 \neq I \lhd T$. Então $M^* + I[X] = T[X]$, pois $I[X] \not\subseteq M^*$. Conseqüentemente, existem $g \in T[X]$ e $h \in I[X]$, com $b = lc(g)$ e $c = lc(h)$, tais que $1 = gf_0 + h$. Como $\partial f_0 \geq 1$, temos que $b = -c$, portanto $b \in I$. Usando que f_0 é mônico, é fácil mostrar por indução que todo coeficiente de g pertence à I, ou seja, $g \in I[X]$. Logo $1 \in I[X]$ e portanto $I = T$.

(ii) Sejam $f \in M^2$ tal que $\partial f = \partial M^2$, $a = lc(f)$ e $g \in [f]_R$. Então existe $0 \neq H \lhd R$ satisfazendo $gHa \subseteq R[X]f \subseteq M^2$. Portanto, $gHaR \subseteq M^2 \subseteq M$. Seja $F = HaR$, temos $gF \subseteq M$. Logo, $g \in M$ e $F[X] + M = R[X]$. Conseqüentemente, $1 = k_1 + k_2$, para certos $k_1 \in F[X]$ e $k_2 \in M$. Assim, $g = gk_1 + gk_2 \in M^2$ e $[f]_R \subseteq M^2$. Agora, $M^2 \subseteq [M^2]_R \subseteq [f]_R \subseteq M^2$, portanto M^2 é um ideal principal fechado de $R[X]$.

Suponhamos, por indução, que $M^{n-1} = [f]_R$ para algum polinômio $f \in M^{n-1}$. Seja $k \in M^n$ satisfazendo $\partial k = \partial M^n$. De modo análogo à primeira parte, temos que $M^n = [k]_R$. A prova está completa.

4.2 Decomposição Primária de Ideais Fechados

O objetivo desta secção é de demonstrar o teorema 4.2.12, que estabelece a decomposição primária de um ideal fechado de $R[E]$ sob certas condições e generaliza a fatorização de um ideal principal fechado do anel de polinômios $R[X]$, obtida na secção anterior (teorema 4.1.1). Os resultados apresentados aqui não aparecem na literatura, e foram obtidos pelo autor, seguindo sugestões do prof. M.Ferrero.

Dado q, um ideal fechado de $R[E]$, estudaremos quando q tem uma "decomposição primária" em $R[E]$. Para isto, é preciso que $C[E]$ seja Noetheriano. Consideremos então nesta secção $R[E] = R[X_1, ..., X_k]$, o anel de polinômios a k indeterminadas sobre R, onde R é um anel primo. Assim, como C é um corpo, $C[E] = C[X_1, ..., X_k]$ é um anel Noetheriano. A partir daqui, denotaremos $R[E]$ (respectivamente $Q[E]$ e $C[E]$) por $R[X]$ (respectivamente $Q[X]$ e $C[X]$).

Seja N o conjunto dos números naturais, excluindo-se o zero. Vejamos a

Proposição 4.2.1 *Sejam $K \lhd C[X]$, $a, b \in C[X]$ e $I \lhd C[X]$. São equivalentes:*
(i) $ab \in K, a \notin K \Rightarrow \exists n \in \mathrm{N}$ tal que $b^n \in K$
(ii) $aI \subseteq K, a \notin K \Rightarrow \exists n \in \mathrm{N}$ tal que $I^n \subseteq K$
(iii) $Ia \subseteq K, a \notin K \Rightarrow \exists n \in \mathrm{N}$ tal que $I^n \subseteq K$

Demonstração : (ii)$\Leftrightarrow$ (iii) Imediato, desde que $aI = Ia$.

(i)$\Rightarrow$ (ii) Seja I um ideal de $C[X]$. Como $C[X]$ é um anel Noetheriano, o ideal I é finitamente gerado. Portanto, existem $a_1, ..., a_t \in C[X]$ tais que $I = (a_1, ..., a_t)$. Suponhamos que $aI \subseteq K$, onde $a \in C[X]$ e $a \notin K$. Então $aa_i \in K$, para todo $i \in \Lambda = \{1, ..., t\}$. Por hipótese, para qualquer $i \in \Lambda$ existe $n_i \in \mathrm{N}$ tal que $a_i^{n_i} \in K$. Assim, temos que $m = max\{n_1, ..., n_t\}$ satisfaz $a_i^m \in K$, $\forall i \in \Lambda$. Logo, $I^{tm} \subseteq K$.

(ii) $\Rightarrow$ (i) Sejam $a, b \in C[X]$ tais que $ab \in K$ e $a \notin K$. Como $ab \in K$, temos que $a(C[X]b) \subseteq K$ e por hipótese, existe $m \in \mathrm{N}$ tal que $(C[X]b)^m \subseteq K$. Conseqüentemente, $b^m \in K$. A prova está completa.

De modo semelhante, podemos provar que a proposição acima vale em qualquer anel comutativo Noetheriano. Um ideal que satisfaz a condição (i) da proposição é chamado ideal primário de R. Assim, 4.2.1 motiva a seguinte generalização, para $R[X]$, do conceito de um ideal ser primário.

Definição 4.2.2 *Um ideal fechado q de $R[X]$ é dito um ideal primário de $R[X]$ se satisfaz a seguinte propriedade: dados $a \in R[X]$ e I, um ideal fechado de $R[X]$, tais que $aI \subseteq q$ e $a \notin q$, então existe $n \in \mathrm{N}$ satisfazendo $I^n \subseteq q$.*

Na definição 4.2.2, é suficiente considerarmos um ideal fechado. Se q é um ideal primário e J é um ideal $R-disjunto$ de $R[X]$ tais que $aJ \subseteq q$, onde $a \in R[X] \setminus q$, então existe $n \in \mathrm{N}$ satisfazendo $J^n \subseteq q$. De fato, dado $b \in [J]$, existe $0 \neq H \lhd R$ tal que $bH \subseteq J$. Conseqüentemente, $abH \subseteq q$ e, logo, $ab \in q$. Segue que, $a[J] \subseteq q$ e, como $a \notin q$, $[J]$ é um ideal fechado de $R[X]$ e, por definição de ideal primário, existe $n \in \mathrm{N}$ tal que $[J]^n \subseteq q$. Como $J \subseteq [J]$, obtemos que $J^n \subseteq q$.

O teorema a seguir, mostra que a correspondência determinada em 3.1.5 preserva a propriedade de um ideal ser primário.

Teorema 4.2.3 *Sejam q um ideal fechado de $R[X]$, q^* o ideal fechado de $Q[X]$ tal que $q = q^* \cap R[X]$, e K o ideal de $C[X]$ que satisfaz $q = Q[X]K \cap R[X]$. São equivalentes:*
(i) q é um ideal primário de $R[X]$
(ii) q^* é um ideal primário de $Q[X]$
(iii) K é um ideal primário de $C[X]$

Demonstração : (i) $\Rightarrow$ (iii) Sejam $a, b \in C[X]$ onde $ab \in K$ e $a \notin K$. Como $a \in C[X]$, existe $0 \neq H \lhd R$ tal que $aH \subseteq R[X]$. Assim, existe h satisfazendo $a_0 = ah \notin q$. De fato: se $aH \subseteq q$ então $aQHQ \subseteq q^*$, portanto $a \in [q^*] = q^*$, donde concluímos que $a \in q^* \cap C[X] = K$, o que é uma contradição. Por outro lado, existe $0 \neq J \lhd R$ com $bJ \subseteq R[X]$. Seja $L = R[X]bJR[X] \lhd R[X]$. Agora, $a_0L = hR[X]abJR[X] \subseteq q^* \cap R[X] = q$ e $a_0 \notin q$. Conseqüentemente, existe $n \in \mathrm{N}$ tal que $L^n \subseteq q$. Assim, como $bJ \subseteq L$, temos que $b^nJ^n \subseteq q \subseteq q^*$, pois $b \in C[X]$. Logo, $b^n \in q^* \cap C[X] = K$, portanto K é um ideal primário de $C[X]$.

(iii) $\Rightarrow$ (ii) Seja q^* um ideal fechado de $Q[X]$ tal que $K = q^* \cap C[X]$ é um ideal primário de $C[X]$. Sejam $a \in Q[X]$ e I um ideal fechado de $Q[X]$ tais que $aI \subseteq q^*$. Consideremos $J = \{b \in Q[X] \mid bI \subseteq q^*\}$ ideal de $Q[X]$. Dado $b \in [J]$, existe $0 \neq H \lhd Q$ tal que $Hb \subseteq J$. Para todo $c \in I$ temos que $Hbc \subseteq Jc \subseteq q^*$. Logo, $bc \in [q^*] = q$, ou seja, $[J]I \subseteq q^*$. Da definição de J, obtemos que $[J] \subseteq J$, portanto, J é um ideal fechado não nulo de $Q[X]$ ($a \in J$). Se $J \cap Q \neq 0$, temos que $J = Q$, pois J é fechado. Então, $I \subseteq q^*$ e q^* é primário.

Se $J \cap Q \neq 0$, $J \cap C[X]$ é um ideal não nulo de $C[X]$ e, além disso, $J \cap C[X] \nsubseteq q^* \cap C[X]$. De fato: suponhamos que $J \cap C[X] \subseteq q^* \cap C[X]$. Então, por 3.1.5, temos que $J \subseteq q^*$, o que é um absurdo, pois $a \in J \setminus q^*$. Seja $0 \neq a_0 \in J \cap C[X] \setminus q^* \cap C[X]$. Temos $a_0(I \cap C[X]) \subseteq K$. Assim, existe $n \in \mathrm{N}$ satisfazendo $(I \cap C[X])^n \subseteq K$. Mas $(I \cap C[X])^n = I^n \cap C[X]$ e, novamente por 3.1.5, obtemos que $I^n \subseteq q^*$. Logo q^* é primário em $Q[X]$.

(ii) $\Rightarrow$ (i) Suponhamos que q^* é um ideal primário de $Q[X]$. Sejam $a \in R[X]$ e I um ideal fechado de $R[X]$ tais que $aI \subseteq q$ e $a \notin q$. Seja I^* o ideal fechado de $Q[X]$ tal que $I = I^* \cap R[X]$. Dado $b \in I^*$, existe $0 \neq H \lhd R$ tal que $bH \subseteq R[X]$. Assim, $abH \subseteq I^* \cap R[X] = I$ e, por 3.1.3, $ab \in q^*$. Logo $aI^* \subseteq q^*$. Mas, $a \notin q^*$ e da hipótese, temos que existe $n \in \mathbb{N}$ satisfazendo $I^{*n} \subseteq q^*$. Agora, $I \subseteq I^*$, portanto $I^n \subseteq I^{*n} \cap R[X] \subseteq q^* \cap R[X] = q$. Logo, q é um ideal primário de $R[X]$ e o teorema está demonstrado.

O lema a seguir, mostra que a correspondência estabelecida em 3.1.5 preserva intersecção de ideais (corolário 4.2.5).

Lema 4.2.4 *Sejam q_1, q_2 ideais fechados de $R[X]$, q_1^*, q_2^* ideais fechados de $Q[X]$ e K_1, K_2 ideais de $C[X]$ satisfazendo $q_1 = q_1^* \cap R[X]$, $q_2 = q_2^* \cap R[X]$, $q_1^* = Q[X]K_1$ e $q_2^* = Q[X]K_2$. Então:*
(i) $q_1 \cap q_2$ é um ideal fechado $R[X]$.
(ii) $q_1^* \cap q_2^*$ é um ideal fechado $Q[X]$.
(iii) $q_1 \cap q_2 = (q_1^* \cap q_2^*) \cap R[X]$.
(iv) $K_1 \cap K_2 = (q_1^* \cap q_2^*) \cap C[X]$.
(v) $q_1 \cap q_2 = Q[X](K_1 \cap K_2) \cap R[X]$.

Demonstração : (i) e (ii). Seja T um anel de quocientes à direita de R, mostremos que, dados dois ideais fechados de q_1 e q_2 de $T[X]$, $q_1 \cap q_2$ é um ideal fechado de $T[X]$. De fato, seja $b \in [q_1 \cap q_2]_T$. Portanto existe $0 \neq H \lhd T$ tal que $bH \subseteq q_1 \cap q_2$. Conseqüentemente, $b \in [q_1]_T \cap [q_2]_T = q_1 \cap q_2$, ou seja, $[q_1 \cap q_2]_T = q_1 \cap q_2$. Logo, $q_1 \cap q_2$ é um ideal fechado de $T[X]$.

(iii) Temos que: $q_1 \cap q_2 = (q_1^* \cap R[X]) \cap (q_2^* \cap R[X]) = (q_1^* \cap q_2^*) \cap R[X]$.

(iv) Temos que: $K_1 \cap K_2 = (Q[X]K_1 \cap C[X]) \cap (Q[X]K_2 \cap C[X]) =$
$= (Q[X]K_1 \cap Q[X]K_2) \cap C[X] = (q_1^* \cap q_2^*) \cap C[X]$.

(v) Por (iii) $q_1 \cap q_2 = (q_1^* \cap q_2^*) \cap R[X]$. Pelo ítem anterior e a correspondência de 3.1.5, $q_1 \cap q_2 = Q[X](K_1 \cap K_2) \cap R[X]$. A prova está completa.

Utilizando 3.1.5, obtemos uma fácil generalização de 4.2.4.

Corolário 4.2.5 *Sejam $q_1, ..., q_t$ ideais fechados de $R[X]$, $q_1^*, ..., q_t^*$ ideais fechados de $Q[X]$ e $K_1, ..., K_t$ ideais de $C[X]$ satisfazendo $q_i = q_i^* \cap R[X]$ e $q_i^* = Q[X]K_i$, para $i = 1, ..., t$. Então:*
(i) $\cap_{i=1}^t q_i^* = (\cap_{i=1}^t q_i)^*$
(ii) $\cap_{i=1}^t Q[X]K_i = Q[X](\cap_{i=1}^t K_i)$
(iii $(\cap_{i=1}^t q_i)^* \cap C[X] = \cap_{i=1}^t K_i$

Em anéis Noetherianos comutativos, para mostrar que todo ideal admite "decomposição primária", mostramos que todo ideal admite uma decomposição em intersecção de ideais irredutíveis e depois que todo ideal irredutível é primário. A partir do conceito de ideal irredutível, obtemos a decomposição minimal. A seguir, generalizamos também este conceito à $R[X]$ e mostramos que a correspondência de 3.1.5 (de $R[X]$ para $C[X]$) preserva ideais irredutíveis.

Definição 4.2.6 *Seja q um ideal fechado de $R[X]$. Dizemos que q é um ideal irredutível em $R[X]$ se, para quaisquer ideais fechados q_1, q_2 de $R[X]$ tais que $q = q_1 \cap q_2$, temos $q = q_1$ ou $q = q_2$.*

Proposição 4.2.7 *Sejam q um ideal fechado de $R[X]$ e K o ideal de $C[X]$ tal que $q = Q[X]K \cap R[X]$. Então, q é irredutível em $R[X]$ se e somente se K é irredutível em $C[X]$.*

Demonstração : Suponhamos que q é redutível em $R[X]$, ou seja, $q = q_1 \cap q_2$ onde q_i é um ideal fechado de $R[X]$ e $q_i \neq q$, para $i = 1$ e 2. Sejam K_1 e K_2 os ideais de $C[X]$ tais que $q_i = Q[X]K_i \cap R[X]$ ($i = 1$ e 2). Temos, por 4.2.5(ii),

$$Q[X]K \cap R[X] = q = q_1 \cap q_2 = (Q[X]K_1 \cap R[X]) \cap (Q[X]K_2 \cap R[X]) =$$

$$= (Q[X]K_1 \cap Q[X]K_2) \cap R[X] = Q[X](K_1 \cap K_2) \cap R[X].$$

Pela correspondência de 3.1.5, $K_1 \cap K_2 = K$. Também, $K \neq K_1$ e $K \neq K_2$, pois $q \neq q_1$ e $q \neq q_2$. Logo K é redutível em $C[X]$, o que é uma contradição. De modo semelhante, podemos demonstrar a recíproca.

Uma decomposição primária de um ideal fechado $I \in R[X]$ é expressar I como uma intersecção finita de ideais primários de $R[X]$, do tipo $I = \cap_{i=1}^{n} q_i$ (onde q_i é um ideal primário de $R[X]$, $1 \leq i \leq n$, com $n \in \mathbb{N}$). Dado I um ideal de um anel qualquer A, o radical de I é a intersecção de todos os ideais primos de A que contém I. O radical de I será denotado por $\sqrt{I}$. Dizemos que a decomposição primária é minimal se $\sqrt{q_i} \neq \sqrt{q_j}$ para quaisquer $1 \leq i, j \leq n$ tais que $i \neq j$ e $q_i \not\supseteq \cap_{j \neq i} q_j$ ($1 \leq i \leq n$).

Seja q um ideal fechado de $R[X]$ e consideremos o ideal K de $C[X]$ tal que $q = Q[X]K \cap R[X]$. Então $\sqrt{q} = Q[X]\sqrt{K} \cap R[X]$. De fato, sabemos que $C[X]$ é Noetheriano e portanto existe um número finito de ideais primos minimais $P_1, ..., P_r$ de $C[X]$ tais que $P_j \supseteq K$ ($1 \leq j \leq r$). Assim, $\sqrt{K} = \cap_{j=1}^{r} P_j$. Além disso, existe $n \in \mathbb{N}$ satisfazendo $\sqrt{K}^n \subseteq K$. Logo, $(P_1 \cdot ... \cdot P_r)^n \subseteq (\cap_{j=1}^{r} P_j)^n \subseteq K$.

Agora consideremos os ideais primos $R-disjuntos$ $p_j = Q[X]P_j \cap R[X]$ de $R[X]$ $(1 \leq j \leq r)$. Temos que para cada $j = 1, 2, ..., r$, p_j é um ideal primo $R-disjunto$ que contém q, e por 3.1.5, $(p_1 \cdot ... \cdot p_r)^n \subseteq q$. Dado um ideal primo F qualquer de $R[X]$ tal que $F \supseteq q$, temos que F contém $(p_1 \cdot ... \cdot p_r)^n$. Conseqüentemente, F contém p_{i_0} $(1 \leq i_0 \leq r)$. Assim, para obter $\sqrt{q}$, podemos considerar apenas os ideais primos $R-disjuntos$ de $R[X]$ que contém q, isto é, $\sqrt{q} = \cap_{j=1}^{r} p_j$. O resultado agora é evidente, por 4.2.5.

Estas observações, demonstram o seguinte

Lema 4.2.8 *Seja q um ideal fechado de $R[X]$. Então $\sqrt{q}$ é dado por uma intersecção finita de ideais primos $R-disjuntos$ de $R[X]$. Além disso, $\sqrt{q}$ é nilpotente módulo q.*

Lema 4.2.9 *Seja q um ideal primário de $R[X]$. Então $\sqrt{q}$ é um ideal primo de $R[X]$.*

Demonstração : Seja K o ideal de $C[X]$ tal que $q = Q[X]K \cap R[X]$, e portanto $\sqrt{q} = Q\sqrt{K} \cap R[X]$. Como $C[X]$ é comutativo, temos que $\sqrt{K}$ é um ideal primo (ver teorema 4.1 de [1]). Logo, por 3.1.7, temos que $\sqrt{q}$ é um ideal primo de $R[X]$.

A seguir, definimos o que é um ideal *L-primário* e mostramos que toda decomposição primária de um ideal fechado I de $R[X]$ pode ser reduzida à uma decomposição primária minimal.

Definição 4.2.10 *Seja q um ideal fechado de $R[X]$. Dizemos que q é L-primário se q é um ideal primário de $R[X]$ e $\sqrt{q} = L$.*

Lema 4.2.11 *Sejam q_1 e q_2 dois ideais L-primários de $R[X]$. Então $q_1 \cap q_2$ é L-primário.*

Demonstração : Por 3.1.5 e 4.2.5, temos que $\sqrt{q_1 \cap q_2} = L$. Resta provar que $\sqrt{q_1 \cap q_2}$ é um ideal primário de $R[X]$. Sejam $a \in R[X]$ e I um ideal fechado de $R[X]$ tais que $aI \subseteq q_1 \cap q_2$ e $a \notin q_1 \cap q_2$. Sem perda de generalidade, podemos supor que $a \notin q_1$. Como q_1 é um ideal primário de $R[X]$, existe $n \in \mathrm{N}$ satisfazendo $I^n \subseteq q_1 \subseteq L$. Sejam K_2 o ideal de $C[X]$ tal que $q_2 = QK_2 \cap R[X]$ e $K = \sqrt{K_2}$. Como $C[X]$ é Noetheriano, existe $m \in \mathrm{N}$ tal que $K^m \subseteq K_2$. Assim, $L^m \subseteq q_2$, conseqüentemente, $I^{nm} \subseteq q_1 \cap q_2$. Logo, $q_1 \cap q_2$ é um ideal *L-primário*.

Assim, dada uma decomposição primária de um ideal de $R[X]$, podemos supor que esta é minimal. De fato, basta substituir os ideais primários que tenham mesmo radical, pela intersecção destes (4.2.11).

Teorema 4.2.12 *Seja I um ideal fechado de $R[X]$. Então existe um número finito de ideais primários $q_1, q_2, ..., q_n$ de $R[X]$ tais que $I = \cap_{i=1}^{n} q_i$ é uma decomposição primária minimal. Além disso, a família de ideais primos $\{\sqrt{q_i}\}_{i=1}^{n}$ é unicamente determinada por I.*

Demonstração : Seja K o ideal de $C[X]$ tal que $I = Q[X]K \cap R[X]$. Como $C[X]$ é Noetheriano, K admite uma decomposição primária minimal em $C[X]$. Seja $K = \cap_{i=1}^{n} K_i$ esta decomposição, onde K_i é P_i-*primário*, para todo $i \in \Lambda = \{1, 2, ..., n\}$ e $n \in \mathbb{N}$. Desde que esta decomposição é minimal, temos $P_i \neq P_j$ para quaisquer $i, j \in \Lambda$ tais que $i \neq j$. Assim, temos, por 4.2.5,

$$I = Q[X]K \cap R[X] = Q[X](\cap_{i=1}^{n} K_i) \cap R[X] =$$

$$= (\cap_{i=1}^{n} Q[X]K_i) \cap R[X] = \cap_{i=1}^{n} Q[X]K_i \cap R[X].$$

Para $i \in \Lambda$, seja $q_i = Q[X]K_i \cap R[X]$. Desde que para todo $i \in \Lambda$, K_i é primário de $C[X]$, obtemos que q_i é primário de $R[X]$ (4.2.3). Assim, dado um ideal fechado I de $R[X]$, I admite uma decomposição primária em $R[X]$ do tipo $I = \cap_{i=1}^{n} q_i$, com q_i um ideal primário de $R[X]$ para $1 \leq i \leq n$. Podemos supor que esta decomposição é minimal (por 4.2.7 e 4.2.11).

Suponhamos agora que $I = \cap_{j=1}^{s} q'_j$, onde q'_j é um ideal primário de $R[X]$ $(1 \leq j \leq s)$. Então os ideais K'_j de $C[X]$ tais que $q'_j = QK'_j \cap R[X]$ $(1 \leq j \leq s)$, são primários de $C[X]$, e vale $K = \cap_{j=1}^{s} K'_j$. Mas $C[X]$ é Noetheriano, portanto, reordenando os fatores (se necessário), temos que $s = n$ e $\sqrt{K_j} = \sqrt{K'_j}$ $(1 \leq j \leq n)$. Conseqüentemente, $\sqrt{q'_j} = \sqrt{q_j}$ $(1 \leq j \leq n)$, pois $\sqrt{q'_j} = Q\sqrt{K'_j} \cap R[X] = Q\sqrt{K_j} \cap R[X] = \sqrt{q_j}$ $(1 \leq j \leq n)$. A prova está completa.

Nota Final

Esta dissertação estuda os ideais primos e fechados de uma extensão livre centralizante $S = R[E]$, de um anel com unidade R. Os resultados obtidos, bem como as técnicas usadas aqui, podem ser aplicadas para relacionar certas propriedades dos ideais primos P de R com os ideais primos P^* de S, tais que $P^* \cap R = P$. Em [6] (secções 3 e 4), M.Ferrero mostra que as propriedades que caracterizam os anéis e ideais fortemente primos, não singulares e primitivos, são preservadas, sob certas condições, quando tomamos ideais primos P e P^* como acima.

Lembramos que um anel R é dito fortemente primo, se qualquer ideal não nulo I de R contém um subconjunto finito F de R que satisfaz a seguinte propriedade: se $r \in R$ e $Fr = 0$, então $r = 0$. F é chamado isolador (à direita) para I em R. Um ideal $I \lhd R$ é dito fortemente primo, se o anel $\frac{R}{I}$ é fortemente primo.

Um ideal I de R dito essencial à direita, se para todo ideal não nulo à direita J de R temos $J \cap I \neq 0$. O ideal singular (à direita) de um anel R é definido por $S(R) = \{a \in R \mid An_R(a)$ é um ideal essencial à direita de $R\}$, onde, $An_R(a)$ denota o anulador à direita de $a \in R$ (De fato podemos provar que $S(R)$ é um ideal). Um anel R é chamado não singular (à direita) se $S(R) = 0$ e um ideal primo P de R é dito não singular se $\frac{R}{P}$ é um anel não singular. Daqui em diante, escreveremos "não singular" para denotar "não singular à direita".

A seguir, enunciamos quatro resultados de [6], que são obtidos como aplicações dos resultados desenvolvidos nesta dissertação. Como antes, $R[E]$ denota uma extensão livre centralizante de R.

Teorema 1: Sejam R um anel fortemente primo e P um ideal de $R[E]$ o qual é maximal com respeito à propriedade $P \cap R = 0$. Então P é um ideal fortemente primo.

Teorema 2: Sejam R um anel primo não singular e P um ideal de $R[E]$ o qual é maximal com respeito à propriedade $P \cap R = 0$. Então P é um ideal não singular.

Teorema 3: Sejam R um anel qualquer e $S = R[E]$ uma extensão livre centralizante de R ($E = \{e_i\}_{i \in \Omega}$). Se E é finito ou $e_ie_j = e_je_i$, para quaisquer $i, j \in \Omega$, então qualquer ideal primo de R é fortemente primo (respectivamente não singular) se e somente se o mesmo é verdadeiro para S.

Um ideal I de R é dito primitivo (à direita) se satisfaz a propriedade de existir um ideal maximal à direita M tal que $(M : R) = \{x \in R \mid Rx \subseteq M\} = I$, ou seja, I é o maior ideal (bilátero) de R contido em M). Um anel é chamado primitivo (à direita), se o ideal 0 é primitivo (à direita).

Teorema 4: Sejam R um anel primitivo (à direita) e P um ideal de $S = R[E]$ maximal com respeito à propriedade $P \cap R = 0$. Então P é um ideal primitivo (à direita) de S.

Observamos que, em [6], o teorema 4 é provado para uma extensão $S = R[E]$ livre e normalizante sobre R (isto é, $e_iR = Re_i$ $\forall i \in \Omega$).

Finalmente, queremos observar que, em [7], os resultados desta dissertação são generalizados. Neste outro trabalho, M.Ferrero define submódulos fechados de um bimódulo sobre um anel primo R. Agora, não é mais necessário que este módulo seja livre. Conseqüentemente, generaliza os resultados expostos nesta dissertação. Além disso, não somente se generalizam os resultados anteriores para extensões não necessariamente livres, como também se obtém resultados em anéis intermediários (isto é, subanéis de S que contenham R). Estes novos resultados são obtidos com técnicas análogas às utilizadas nesta dissertação.

Bibliografia

[1] M. F. ATIYAH and I. G. MACDONALD, Introduction to commutative algebra, Reading, Addison-Wesley,1969.

[2] D. BURTON, A first course in rings and ideals, Reading, Addison-Wesley, 1968.

[3] E. CISNEROS, M. FERRERO and M. I. GONZÁLEZ, Prime ideals in skew polynomial rings and skew Laurent polynomial rings, Math. J. Okayama Univ., 32, 61-72 (1990).

[4] M. FERRERO, Ideais primos e maximais em anéis comutativos de polinômios, Atas da X Escola de Álgebra, Rio de Janeiro, SBM, 1990.

[5] M. FERRERO, Prime and principal closed ideals in polynomial rings, J.Algebra, 134, 45-59 (1990).

[6] M. FERRERO, Closed and prime ideals in free centred extensions, J.Algebra, 148, 1-16 (1992).

[7] M. FERRERO, Centred bimodules over prime rings: closed submodules and applications to rings extensions, a ser publicado.

[8] M. FERRERO and K. KISHIMOTO, On differential rings and skew polynomials, Communications in Algebra, 13(2) 285-304 (1985).

[9] M. FERRERO and J. MATCZUK, Prime ideals in skew polynomial rings of derivation type, Communication in Algebra, 18(3) 689-710 (1990).

[10] I. N. HERSTEIN, Topics in algebra, Waltham, Blaisdell, 1964.

[11] A. JONES, Notas de algebra, São Paulo, IME-USP, 1979.

[12] J. LAMBEK, Lectures on rings and modules, N.York, Chelsea, 1976.

[13] A. LEROY and J. MATCZUK, Prime ideals of Öre extensions, Communications in Algebra, 19(7) 1893-1907 (1991).

[14] W. S. MARTINDALE, Prime rings satysfying a generalized polynomial identity, J.Álgebra, 12, 576-584 (1969).

[15] N. H. McCOY, The theory of rings, N.York, Macmillan, 1969.

[16] C. P. MILIES, Anéis de grupos, IV Escola de Álgebra, São Paulo, SBM, 1976.

[17] M. M. PARMENTER, D. S. PASSMANN and P. N. STEWART, The strongly prime radical of crossed products, Communications in Algebra, 12(9) 1099-1113 (1987).

[18] P. RIBENBOIM, Rings and modules, N.York, Interscience, 1969.

[19] L. H. ROWEN, Ring theory, vol.1, San Diego, Academic Press, 1988.

[20] B. STENSTRÖM, Rings and modules of quotients, Lectures Notes in Mathematics, 237.

[21] B. STENSTRÖM, Rings of quotients, Berlin, Springer-Verlag, 1975.

[22] O. ZARISKI and P. SAMUEL, Commutative algebra, vol.1, Princeton, Van Nostrand, 1958.