IDEAIS PRIMOS EM EXTENSÕES DE ANÉIS*

Miguel Ferrero
Instituto de Matemática
Universidade Federal do Rio Grande do Sul
Av. Bento Gonçalves, 9500
91509-900 - Porto Alegre - RS

INTRODUÇÃO

Existem muitos resultados, propriedades e aplicações que provam que os ideais primos de anéis comutativos são objetos muito importantes na Álgebra Comutativa e na Geometria Algébrica. Como seria então previsível, eles também desempenham um papel muito relevante na Teoria de Anéis não comutativos. Nos últimos 20 anos, muita literatura tem sido dedicada a este tema.

A partir da década de 80, interessei-me pelo assunto e escrevi alguns trabalhos de pesquisa sobre o tema. Em particular, o estudo dos ideais primos em extensões centralizantes de anéis, proporcionou um método para estudar extensões não necessariamente finitamente geradas. Pretendo dedicar estas notas à exposição do método e principais resultados desta série de trabalhos.

Farei justiça à história salientando que meu interesse por um dos problemas que motivaram meus trabalhos veio de uma pergunta feita pela minha colega e amiga Ada Maria de Souza Doering. Ela perguntou se um resultado bem conhecido em anéis comutativos era também verdadeiro em anéis não comutativos. A resposta não era conhecida e levou-me a escrever [F_3], o primeiro artigo da série que estou mencionando.

Como penso que existe muita coisa para ser feita a partir dos trabalhos por mim desenvolvidos, aceitei o desafio de escrever estas notas e proferir um mini-curso na Escola de Álgebra, com a esperança de que algumas pessoas se interessem pelo assunto e possam fazer novas contribuições.

Trabalharemos aqui sempre com anéis não necessariamente comutativos e que possuem unidade. Ideais de anéis são sempre ideais bilaterias, salvo que algo seja dito em contrário. Se I é um ideal de R, indicamos isto por $I \lhd R$. As notações $\subset$ e $\supset$ indicam contenções estritas.

O primeiro capítulo contém resultados prévios, que são necessários para o que segue. O segundo contém os resultados principais.

Para terminar esta introdução, desejo agradecer a colaboração de Alvino Alves Sant'Ana, Alveri Alves Sant'Ana e Luisa Superina de Ferrero, minha es-

*Este trabalho foi feito para ser apresentado em forma de mini-curso na XIII Escola de Álgebra, UNICAMP de 18 a 23 de julho de 1994. Como todos os meus trabalhos, foi apoiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

posa, pela ajuda no trabalho de revisão e correção do manuscrito, que muito ajudaram a melhorar. Finalmente, e muito especialmente, desejo agradecer a Valéria Fernandes Ritter pelo esforço e dedicação manifestados na árdua tarefa de digitação do manuscrito.

Miguel Ferrero
Junho de 1994

CAPÍTULO I - PRÉ-REQUISITOS

§1. IDEAIS PRIMOS

Neste parágrafo, R denota um anel (com unidade) qualquer.

Se R é comutativo, um ideal P de R é dito um ideal primo se para cada par de elementos a e b de R temos que $ab \in P$ implica $a \in P$ ou $b \in P$.

Os ideais primos de anéis comutativos são estudados em qualquer curso de Álgebra Comutativa, onde desempenham um papel importante em vários assuntos; por exemplo, no estudo da estrutura do próprio anel e na geometria algébrica.

Neste parágrafo, estudamos a generalização deste conceito aos anéis não comutativos.

Seja, então, R um anel não necessariamente comutativo. A mais usual e conveniente generalização do conceito definido acima é dada a seguir.

Definição 1.1. Um ideal P de R é dito um ideal primo de R se para ideais A e B de R temos que $AB \subseteq P$ implica $A \subseteq P$ ou $B \subseteq P$.

É fácil verificar que a definição dada coincide com a anterior, no caso em que R é um anel comutativo (Ex. 1).

É bom observar que algumas vezes convém restringir-se a ideais A e B que contêm P. A definição que corresponde a este caso resulta ser equivalente à anterior. O mesmo acontece se A e B são ideais unilaterais. A seguinte proposição estabelece as equivalências mais usuais.

Proposição 1.2. Seja P um ideal de R. As seguintes condições são equivalentes:

(i) P é um ideal primo de R.

(ii) Se A e B são ideais de R tais que $A \supseteq P$, $B \supseteq P$ e $AB \subseteq P$, então $A = P$ ou $B = P$.

(iii) Se I e L são ideais à direita (ou à esquerda) de R tais que $IL \subseteq P$, então $I \subseteq P$ ou $L \subseteq P$.

(iv) Se a, $b \in R$ e $aRb \subseteq P$, então $a \in P$ ou $b \in P$.

Demonstração. A equivalência entre (i) e (ii) é fácil de obter (Ex. 2).

(i)$\longrightarrow$(iii). Se I e L são ideais à direita tais que $IL \subseteq P$, então $(RI)(RL) \subseteq R(IL) \subseteq RP \subseteq P$. Logo, como RI e RL são ideais bilaterais, a relação anterior implica $RI \subseteq P$ ou $RL \subseteq P$. Mas, sendo que R possui unidade, segue que $I \subseteq RI$ e $L \subseteq RL$. Conseqüentemente, $I \subseteq P$ ou $L \subseteq P$.

(iii)$\longrightarrow$(iv). Se $aRb \subseteq P$, então $aRbR \subseteq P$. Logo, $aR \subseteq P$ ou $bR \subseteq P$ e segue que $a \in P$ ou $b \in P$.

(iv)$\longrightarrow$(i). Sejam A e B ideais de R tais que $AB \subseteq P$. Se $A \not\subseteq P$, existe $a \in A \setminus P$. Logo, para cada $b \in B$ temos que $aRb \subseteq AB \subseteq P$ e assim $b \in P$. Conseqüentemente, $B \subseteq P$ e a prova está completa. $\square$

Um anel R é dito primo se (0) é um ideal primo de R. Usando a correspondência biunívoca entre ideais de R que contêm um ideal P e ideais de R/P, segue facilmente que P é um ideal primo de R se, e somente se, R/P é um anel primo (Ex. 3). Também, pelo Exercício 1, um anel comutativo é um anel primo se, e somente se, é um domínio de integridade.

Da Proposição 1.2 segue o seguinte Corolário evidente

Corolário 1.3. As seguintes condições são equivalentes:

(i) R é um anel primo.

(ii) Se I e L são ideais à direita (ou à esquerda) de R tais que $IL = 0$, então $I = 0$ ou $L = 0$.

(iii) Se a, $b \in R$ e $aRb = 0$, então $a = 0$ ou $b = 0$.

Exercícios:

1) Provar que se R é um anel comutativo e P é um ideal de R, então P é um ideal primo no sentido definido aqui se, e somente se, ele é um ideal primo no sentido usual para anéis comutativos. Concluir que um anel comutativo é primo se, e somente se, é um domínio.

2) Provar que as condições (i) e (ii) da Proposição 1.2 são equivalentes (uma parte é evidente e para a outra trocar A e B por $(A + P)$ e $(B + P)$).

3) Provar que P é um ideal primo de R se, e somente se, R/P é um anel primo.

4) Um ideal N de um anel R é dito semi-primo se N é uma intersecção de ideais primos. Provar que se N é semi-primo, então para $a \in R$, $aRa \subseteq N$ implica $a \in N$.

§2. ALGUNS TIPOS DE IDEAIS PRIMOS

Se considerarmos a definição de ideais primos dada para anéis comutativos, poderíamos dar uma outra definição, como segue:

Definição 2.1. Um ideal P de R é dito completamente primo se para a, $b \in R$ temos que $ab \in P$ implica $a \in P$ ou $b \in P$.

Um anel qualquer (não necessariamente comutativo) é chamado um domínio se (0) é um ideal completamente primo, i. e, se $ab = 0$ implica $a = 0$ ou $b = 0$. É claro, então, que P é um ideal completamente primo de R se, e somente se, R/P é um domínio.

Se P é um ideal completamente primo de R, então P é primo. De fato, se $AB \subseteq P$, para $A \lhd R$ e $B \lhd R$, e se $A \nsubseteq P$, tomemos $a \in A \setminus P$ e $b \in B$. Segue que $ab \in AB \subseteq P$ e, conseqüentemente, $b \in P$. Assim, $B \subseteq P$.

A recíproca do fato anterior não é verdadeira. Para ver isso, é suficiente tomar $R = M_n(K)$, o anel das matrizes quadradas de ordem $n \geq 2$ sobre um corpo K. É conhecido que $M_n(K)$ é um anel simples, i. e., não possui ideais bilaterais próprios (ver [Mc], Th. 2.24). Portanto, se A e B são ideais não nulos de R segue que $A = B = R$ e assim $AB = R^2 = R \neq 0$ (pois R possui unidade). Então o ideal (0) de R é um ideal primo. Além disso, (0) não é completamente primo pois R não é um domínio, como é bem conhecido.

Na verdade, os ideais completamente primos são bastante escassos, em geral, e esta é uma das razões pelas quais a definição dada no parágrafo anterior é mais apropriada.

Existem outras duas classes intermediárias de ideais primos entre as duas definidas até aqui, que veremos a seguir.

Dado um subconjunto F de R, o anulador à direita de F é definido por $An_r(F) = \{a \in R : Fa = 0\}$. Se $x \in R$, o anulador à direita de x é simplesmente denotado por $An_r(x)$ em lugar de $An_r(\{x\})$.

Um subconjunto finito F de R é chamado um isolador (à direita) de R se $An_r(F) = 0$, i. e., se $Fa = 0$, $a \in R$, implica $a = 0$.

Definição 2.2. Um anel R é dito fortemente primo (à direita) se todo ideal não nulo de R contém um isolador.

Definição 2.3. Um ideal P de R é dito fortemente primo (à direita) se R/P é um anel fortemente primo.

O Lema a seguir caracteriza um ideal fortemente primo.

Lema 2.4. Seja P um ideal de R. As seguintes condições são equivalentes

(i) P é um ideal fortemente primo.

(ii) Para todo ideal $I \supset P$ existe um subconjunto finito $F \subseteq I$ tal que $Fa \subseteq P$, $a \in R$, implica $a \in P$.

Demonstração. É suficiente passar a R/P e utilizar a correspondência biunívoca entre os ideais de R que contém P e os ideais de R/P. $\square$

Trocando I por $(I + P)$ pode-se provar que a condição (ii) pode ser dada também para ideais $I \nsubseteq P$ em lugar de ideais que contêm P propriamente (Ex. 2).

É conveniente observar também que um conjunto finito F que satisfaz a condição dada em (ii) do Lema 2.4 é chamado um isolador módulo P.

A relação do último conceito com os anteriores é dada na seguinte

Proposição 2.5. (i) Todo ideal fortemente primo é primo.
(ii) Todo ideal completamente primo é fortemente primo.

Demonstração. Basta provar a proposição para o ideal (0).

(i) Suponha que R é fortemente primo. Se $AB = 0$, onde A e B são ideais de R com $A \neq 0$, existe um isolador $F \subseteq A$. Logo, $B \subseteq An_r(F) = 0$.

(ii) Suponhamos que R é um domínio. Se I é um ideal não nulo de R, tome qualquer $0 \neq a \in I$. Por hipótese, $An_r(a) = 0$ e assim $\{a\}$ é um isolador. $\square$

Um ideal à direita H de R é dito essencial se para todo ideal à direita não nulo I de R temos que $I \cap H \neq (0)$.

Por exemplo, se R é um anel primo, todo ideal não nulo H é um ideal essencial como ideal à direita. De fato, se I é um ideal à direita não nulo temos que $(0) \neq IH \subseteq I \cap H$.

Definição 2.6. O ideal singular (à direita) $Z(R)$ de R é definido como o conjunto dos elementos $a \in R$ tais que $An_r(a)$ é um ideal essencial.

A prova da seguinte proposição pode ser encontrada em ([G], pág. 30).

Proposição 2.7. $Z(R)$ é um ideal de R.

Um anel R é dito não singular (à direita) se $Z(R) = 0$. Para nós, o que interessa é a seguinte

Definição 2.8. Um ideal primo P de R é dito não singular se R/P é um anel não singular, i. e., $Z(R/P) = 0$.

É claro que todo ideal primo não singular é primo. Temos também a seguinte

Proposição 2.9. Todo ideal fortemente primo é primo não singular.

Demonstração. Seja R um anel fortemente primo e suponhamos que $Z(R) \neq 0$. Então existe um conjunto finito $F = \{a_1, a_2 ...., a_n\} \subseteq Z(R)$ tal que $An_r(F) = 0$. Mas, para cada i, $An_r(a_i)$ é essencial e por indução segue facilmente que

$\bigcap_{i=1}^{n} An_r(a_i) \neq (0)$. Esta é uma contradição, pois $\bigcap_{i=1}^{n} An_r(a_i) = An_r(F)$. A contradição prova que $Z(R) = 0$.

O caso geral, para um ideal arbitrário P, se obtém passando a R/P. $\square$

Denotamos por $\mathcal{P}(R)$ (resp. $Z(R)$, $\mathcal{S}(R)$, $\mathcal{C}(R)$) a classe de todos os ideais primos (resp. primos não singulares, fortemente primos, completamente primos) de R. Como conclusão dos resultados anteriores temos as seguintes inclusões:

$$\mathcal{P}(R) \supseteq Z(R) \supseteq \mathcal{S}(R) \supseteq \mathcal{C}(R).$$

Exemplos podem ser dados para provar que as inclusões são todas estritas, mas não entraremos em detalhes a este respeito.

Existem outras classes de ideais primos que são muito importantes.

Como é conhecido, um ideal próprio M de R é dito maximal se para todo ideal I tal que $M \subseteq I$ temos que $I = M$ ou $I = R$. É fácil verificar que todo ideal maximal é primo. Mais ainda, todo ideal maximal é fortemente primo. De fato, se M é maximal e I é um ideal tal que $I \supset M$, temos que $I = R$ e assim $\{1\}$ é um isolador módulo M contido em I.

Conseqüentemente, a classe $\mathcal{M}(R)$ de todos os ideais maximais de R é uma classe de ideais fortemente primos, i. e., $\mathcal{S}(R) \supseteq \mathcal{M}(R)$. Esta classe também serve para provar de maneira elementar que todo anel possui ideais primos. Provavelmente, o leitor conhece a seguinte.

Proposição 2.10. Para todo ideal próprio H de R existe um ideal maximal M tal que $H \subseteq M$. Em particular, todo anel possui ideais maximais.

Demonstração. Considere a família $\mathcal{I}$ de todos os ideais I tais que $H \subseteq I \subset R$. É claro que $\mathcal{I}$ é não vazia e é fácil verificar que o Lema de Zorn se aplica. De fato, se $I_1 \subset I_2 \subset ...$ é uma cadeia em $\mathcal{I}$, $\bigcup_j I_j \in \mathcal{I}$, pois $1 \notin \bigcup_j I_j$. Logo, um elemento maximal M de $\mathcal{I}$ é o ideal maximal procurado. Deixamos para o leitor completar os detalhes faltantes da demonstração (Ex. 4). $\square$

Dado um ideal à direita L de R definimos $(R : L)$ por

$$(R : L) = \{x \in R : Rx \subseteq L\}.$$

É fácil verificar que $(R : L)$ é o maior ideal bilateral contido em L (Ex. 5).

Um ideal maximal à direita é definido de forma análoga a um ideal maximal, considerando ideais à direita em lugar de ideais. A seguinte definição é muito importante.

Definição 2.11. Um ideal P de R é dito primitivo (à direita) se existir um ideal maximal à direita L de R tal que $(R : L) = P$.

Um anel R é dito primitivo (à direita) se (0) é um ideal primitivo, i.e., para algum ideal maximal à direita L temos que $(R : L) = 0$. Os anéis primitivos são muito importantes, pois para eles se conhecem teoremas de estrutura muito úteis, mas não entraremos em detalhes nestes aspectos.

É claro que P é um ideal primitivo de R se, e somente se, R/P é um anel primitivo. Um anel comutativo é primitivo se, e somente se, é um corpo. Um anel simples é primitivo e, portanto, todo ideal maximal é primitivo. Todas as afirmações anteriores são fáceis de verificar (Ex. 6).

Vamos definir ainda outra classe de ideais primos, antes de provar que efetivamente os primitivos o são.

Um ideal I de R é dito um nil ideal se cada $x \in I$ é um elemento nilpotente, i. e., existe $n \geq 0$ tal que $x^n = 0$.

Definição 2.12. Um ideal primo P é dito nil semi-simples se o anel R/P não possui nil ideais.

A relação deste conceito com o anterior é dado por

Proposição 2.13. Todo ideal primitivo é primo nil semi-simples.

Demonstração. Como já fizemos outras vezes é suficiente analisar o ideal (0). Suponhamos que R seja um anel primitivo. Logo, existe um ideal maximal à direita L com $(R : L) = 0$. Se A e B são ideais de R tais que $AB = 0$ e $A \neq 0$, então $A \nsubseteq L$. Logo, $A + L = R$ e existem $a \in A$, $x \in L$ tais que $a + x = 1$. Assim, para cada $b \in B$, $b = ab + xb = xb \in L$. Conseqüentemente, $B \subseteq L$ e como $(R : L) = 0$ segue que $B = 0$. Assim R é primo.

Seja agora I um nil ideal de R. Se $I \neq 0$, então $I \nsubseteq L$. Logo, $I + L = R$ e existem $c \in I$, $y \in L$ tais que $c + y = 1$. Portanto, $y = 1 - c$ é inversível em R, já que c é nilpotente (Ex. 7). Segue que $L = R$, absurdo. Assim R não possui nil ideais. $\square$

Se indicamos por $p(R)$ a classe dos ideais primitivos e por $\mathcal{N}(R)$ a classe dos ideais primos nil semi-simples, temos então que $\mathcal{M}(R) \subseteq p(R) \subseteq \mathcal{N}(R) \subseteq \mathcal{P}(R)$. Como no caso tratado anteriormente, as inclusões são todas estritas.

Observação 2.14. Existe ainda uma classe bastante utilizada: a classe dos ideais primos localmente nilpotentes semi-simples, mas não vamos definir esta classe nestas notas.

Exercícios.

1) Completar a prova do Lema 2.4.

2) Provar que um ideal P de R é completamente primo se para todo ideal I de R tal que $I \nsubseteq P$ existe um subconjunto finito $F \subseteq I$ tal que $Fa \subseteq P$, $a \in R$, implica $a \in P$.

3) Provar que a intersecção de um número finito de ideais à direita essenciais é também essencial.

4) Completar a prova da Proposição 2.10.

5) Provar que se L é um ideal à direita de R, então $(R : L)$ é o maior ideal bilateral contido em L.

6) i) Provar que um anel comutativo é primitivo se, e somente se, é um corpo.
ii) Provar que todo anel simples é primitivo e concluir que todo ideal maximal é primitivo.

7) Seja $c \in R$ nilpotente. Mostre que $1 - c$ é inversível em R.

§3. RADICAIS DE ANÉIS

Neste parágrafo não pretendemos estudar radicais de anéis em detalhes. Nosso propósito é dar apenas algumas noções que vão justificar a importância do estudo dos ideais primos de um anel. Por esta razão omitiremos as provas de muitas das afirmações que fazeremos. O leitor interessado pode encontrá-las na bibliografia citada ao final destas notas.

Quando se estuda a estrutura de um anel R algumas vezes é conveniente cancelar certos elementos do mesmo, cujo comportamento não é muito desejável. Isto se consegue agrupando tais elementos dentro de um ideal $\alpha(R)$ de R e estudando o anel $R/\alpha(R)$, cuidando para definir $\alpha(R)$ de modo que $\alpha(R/\alpha(R)) = (0)$. Este ideal $\alpha(R)$ vai ser chamado, então, de um radical de R.

Por exemplo, se R é um anel comutativo e $Nil(R)$ denota o conjunto de todos os elementos nilpotentes de R, temos que $Nil(R)$ é um ideal de R e $Nil(R/Nil(R)) = (0)$. Assim, $Nil(R)$ é um radical de R chamado o nil radical de R. Visto que o anel $R/Nil(R)$ não possui elementos nilpotentes, é mais fácil estudá-lo do que estudar o anel R. A informação obtida para $R/Nil(R)$, poderá fornecer informação sobre R, utilizando técnicas que permitam "levantar" essas informações.

Acontece que praticamente todos os radicais mais populares de um anel R são intersecções de certos tipos de ideais primos. Esta é uma razão muito poderosa, que justifica a importância do estudo dos ideais primos. Vejamos alguns exemplos, começando pelos radicais mais importantes.

O radical primo $\beta(R)$ de R, chamado também nil radical inferior, é a intersecção de todos os ideais primos de R. Podemos caracterizar $\beta(R)$ como veremos a seguir (Corol. 3.2).

Um ideal I de R é dito nilpotente se existir $n \geq 1$ tal que $I^n = 0$. Por outro lado, um ideal L de R é dito semi-primo se satisfizer a seguinte condição: $aRa \subseteq L$, $a \in R$, implica $a \in L$. Dizemos que R é semi-primo se o ideal (0) é semi-primo.

Lema 3.1. As seguintes condições são equivalentes
(i) L é um ideal semi-primo de R.
(ii) R/L não possui ideais nilpotentes não triviais.
(iii) L é uma intersecção de ideais primos.

Demonstração. Passando a R/L podemos supor que $L = 0$.

(i)$\longrightarrow$(ii) Suponhamos que R é semi-primo e seja I um ideal nilpotente não nulo. Assim, existe um inteiro $n \geq 2$ tal que $I^n = 0$ e $I^{n-1} \neq 0$. Tomando $H = I^{n-1}$ temos que $H \neq 0$ e $H^2 = 0$. Seja $0 \neq a \in H$. Então $aRa \subseteq H^2 = 0$, donde $a = 0$, uma contradição. Portanto, R não possui ideais nilpotentes não triviais.

(ii)$\longrightarrow$(i) Se $aRa = 0$, então $(RaR)^2 = RaRaR = 0$. Por hipótese $RaR = 0$ e segue que $a = 0$.

(i)$\longrightarrow$(iii) Seja $H = \bigcap_{i\in\Gamma} P_i$, onde $\{P_i : i \in \Gamma\}$ é a família de todos os ideais primos de R. Se $H = 0$ a prova desta implicação está completa. Suponhamos, então, que $H \neq 0$ e tomemos $0 \neq a \in H$. Por hipótese, existe $r_1 \in R$ tal que $a_1 = a_0 r_1 a_0 \neq 0$, onde $a_0 = a$. Então, existe $r_2 \in R$ tal que $a_2 = a_1 r_2 a_1 \neq 0$. Por indução, construímos uma seqüência $S = \{a_0, a_1, a_2, ...\}$ tal que, para cada i, existe $r_i \in R$ com $a_i = a_{i-1} r_i a_{i-1} \neq 0$. Seja P um ideal de R, maximal com respeito a propriedade $P \cap S = \emptyset$. Assim, $a \notin P$ e a prova estará completa se provarmos que P é primo.

De fato, se A e B são ideais de R tais que $A \supset P$ e $B \supset P$ temos que, pela maximalidade de P, existem i e j com $a_i \in A$ e $a_j \in B$. Suponha que $i \geq j$. Então, $a_{i+1} = a_i r_{i+1} a_i = a_i r_{i+1} a_{i-1} r_i a_{i-1} = a_i r_{i+1} ... a_j \in AB$. Como $P \cap S = \emptyset$ e $a_{i+1} \in AB$ segue que $AB \supset P$ e, conseqüentemente, P é primo, pela Proposição 2.1, (ii).

(iii)$\longrightarrow$(i) É fácil, e fica como exercício (§1, Ex. 4). $\square$

O seguinte corolário dá uma caracterização de $\beta(R)$.

Corolário 3.2. O radical primo $\beta(R)$ é o menor ideal semi-primo de R.

Demonstração. Pela proposição anterior todo ideal semi-primo é uma intersecção de ideais primos. Então, o corolário segue do fato de que $\beta(R)$ é a intersecção de todos os ideais primos de R. $\square$

Corolário 3.3. $\beta(R/\beta(R)) = (0)$.

Demonstração. Seja P um ideal de R contendo $\beta(R)$. Como

$$(R/\beta(R))/(P/\beta(R)) \simeq R/P,$$

segue que P é um ideal primo de R se, e somente se, $P/\beta(R)$ é um ideal primo de $R/\beta(R)$. Conseqüentemente $\beta(R/\beta(R)) = 0$. □

Se um anel é comutativo, a intersecção de todos os ideais maximais de R é chamado o radical de Jacobson de R. Para um anel arbitrário, a intersecção de todos os ideais maximais não parece ser um conceito tão importante. Em seu lugar definimos:

O radical de Jacobson $J(R)$ de R é a intersecção de todos os ideais primitivos de R. Pela definição de ideal primitivo, $J(R)$ é também igual à intersecção dos ideais maximais à direita de R.

O radical de Jacobson é sem dúvida o mais importante dos radicais de um anel, existindo várias caracterizações úteis para ele. Queremos mencionar aqui somente a seguinte

Proposição 3.4. (i) O radical de Jacobson de R é o conjunto de todos os $x \in R$ tais que $1 - xy$ é inversível à direita, para todo $y \in R$.

(ii) O radical $J(R)$ é o maior ideal L de R tal que para cada $x \in L$, $1 - x$ é inversível em R.

O mesmo argumento do Corolário 3.3 prova a seguinte

Proposição 3.5. $J(R/J(R)) = 0$.

O nil radical superior $Nil(R)$ de R é a intersecção de todos os ideais primos nil semi-simples de R.

A prova das seguintes afirmações será omitida aqui. O nil radical superior coincide com a soma de todos os nil ideais de R. Segue que $Nil(R)$ é o maior nil ideal de R e daí resulta que $Nil(R/Nil(R)) = 0$.

Mencionamos antes que todos os radicais mais populares de um anel são intersecções de ideais primos. Considerando as classes definidas no parágrafo anterior obtemos os seguintes radicais.

O nil radical generalizado $N_g(R)$ de R é definido como a intersecção de todos os ideais completamente primos de R.

O radical fortemente primo $s(R)$ de R é igual à intersecção de todos os ideais fortemente primos de R.

O radical singular $z(R)$ de R pode ser definido como a intersecção de todos os ideais primos não singulares de R.

Considerando os resultados do parágrafo anterior temos que $\beta(R) \subseteq z(R) \subseteq s(R) \subseteq N_g(R)$.

Outra razão para que a definição de ideal primo em anéis não comutativos seja aquela dada no parágrafo 1 e não a de ideais completamente primos, é que, com esta última definição o radical que se obtém (i. e., $N_g(R)$) é muito grande e, portanto, não é muito útil.

A intersecção de todos os ideais maximais de R é chamado o radical de Brown-McCoy de R e denotado por $G(R)$.

Os resultados do §2 provam, também, que $\beta(R) \subseteq Nil(R) \subseteq J(R) \subseteq G(R)$.

Finalmente, se R é um anel comutativo, então é fácil ver que $\beta(R) = Nil(R) = z(R) = s(R) = N_g(R)$ e que $J(R) = G(R)$.

Exercícios:

1) Provar que se I e L são nil ideais de R, então $I + L$ é um nil ideal de R (usar $(I + L)/I \simeq L/I \cap L$). Deduzir que a soma de todos os nil ideais de R é um nil ideal máximo.

2) Generalizar o argumento do Corolário 3.3 para mostrar que se I é um ideal de R e $I \subseteq \beta(R)$, então $\beta(R/I) = \beta(R)/I$.

3) Generalizar o exercício anterior para outros radicais. Mostrar que $\alpha(R/\alpha(R)) = 0$ para $\alpha = z$, s, N_g, J, Nil, G.

4) Suponha que R é comutativo. Mostre que:

i) Todo ideal primo é completamente primo.

ii) Todo ideal primo é nil semi-simples.

iii) Todo ideal primitivo é maximal.

iv) Concluir que para este caso, $\beta(R) = Nil(R) = z(R) = s(R) = N_g(R)$ e que $J(R) = G(R)$.

§4. O ANEL DE QUOCIENTES DE MARTINDALE DE UM ANEL PRIMO

Se D é um domínio de integridade comutativo, é conhecido que existe um corpo F que contém D, chamado o corpo de frações de D, tal que para cada $x \in F$ existe um elemento $a \in D$ com $xa \in D$. A existência do corpo de frações de D é um fato extremamente importante e útil para muitos assuntos.

Podemos dar um exemplo relacionado com ideais primos. Se P é um ideal primo não nulo de $D[X]$ com $P \cap D = 0$, existe um único ideal primo P^* de $F[X]$ tal que $P^* \cap D[X] = P$ (ver [K], Th. 36). A correspondência $P \leftrightarrow P^*$ é uma correspondência biunívoca entre o conjunto dos ideais primos P de $D[X]$ tal que $P \cap D = 0$ e o conjunto dos ideais primos de $F[X]$. Como os ideais primos de $F[X]$ podem ser descritos via polinômios irredutíveis, obtemos desta maneira uma descrição dos ideais primos de $D[X]$.

A construção de F a partir de D pode ser estendida aos anéis não comutativos. Isto é o que queremos apresentar neste parágrafo. Vamos nos restringir, para evitar complicações e porque é suficiente para nossos objetivos, ao anel de quocientes (à direita) de Martindale de um anel primo R, definido pela primeira vez por Martindale em [Ma$_2$]. Queremos destacar que existem construções mais gerais, também para anéis não necessariamente primos. O leitor interessado pode consultar ([Mo$_1$], Ch. 3, [L], Sect. 4.3).

Antes de começarmos com a construção note que, se D é um domínio comutativo e F é o corpo de frações de D, dado um elemento $x = a/b \in F$, podemos definir uma aplicação de um ideal não nulo de D em D, como segue. Seja $f_x : bD \to D$ dada por $f_x(bd) = xbd = ad$, para todo $d \in D$. Esta aplicação é um D-homomorfismo. Reciprocamente, se I é um ideal não nulo de D e $f : I \to D$ é um D-homomorfismo, então tomemos $0 \neq b \in D$. Assim, para $a = f(b)$, a aplicação f restrita ao ideal bD verifica $f(bd) = f(b)d = ad = (a/b)bd$, i. e., f está definida como acima por $x = a/b \in F$.

Seja R um ideal primo. Se I é um ideal de R, vamos dizer que uma aplicação $f : I \to R$ é um R-homomorfismo (à direita) se f é aditiva e $f(ar) = f(a)r$, para todo $a \in I$, $r \in R$. Vamos trabalhar no que segue com ideais não nulos I de R e R-homomorfismos $f : I \to R$. O conjunto de todos os ideais não nulos de R será denotado por $\mathcal{I}$. Note que, se I, $J \in \mathcal{I}$, então $IJ \in \mathcal{I}$ e $I \cap J \in \mathcal{I}$.

Denotamos por $\mathcal{Q}$ o conjunto de todos os pares (I, f), onde $I \in \mathcal{I}$ e $f : I \to R$ é um R-homomorfismo (à direita).

Em $\mathcal{Q}$, definimos uma relação de equivalência como segue: se (I, f), $(J, g) \in Q$, dizemos que (I, f) é equivalente a (J, g) ($(I, f) \sim (J, g)$) se existir um ideal não nulo $H \subseteq I \cap J$ tal que $f/H = g/H$. Podemos verificar facilmente que esta relação é realmente uma relação de equivalência e que pode ser definida de maneira equivalente como segue: $(I, f) \sim (J, g)$ se, e somente se, $f/(I \cap J) = g/(I \cap J)$.

Denotemos por Q o conjunto quociente $\mathcal{Q}/\sim$ e por $[I, f]$ a classe de equivalência (I, f), onde $(I, f) \in \mathcal{Q}$. No que segue, dotaremos Q de uma estrutura de anel de modo que poderemos considerar $R \subseteq Q$.

Sejam $[I, f]$, $[J, g]$ dois elementos de Q. Definimos a soma e o produto em Q por:

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

ii) $[I, f][J, g] = [JI, f \circ g]$, onde $f \circ g : JI \to R$ é definida por $(f \circ g)(a) = f(g(a))$ para todo $a \in JI$ (note que esta definição está bem dada, pois $g(JI) \subseteq I$ e assim $f(g(a)) \in R$).

É fácil verificar que estas operações estão bem definidas em Q.

A prova do seguinte teorema é simples, e deixemo-la como exercício para o leitor.

Teorema 4.1. $(Q, +, \cdot)$ é um anel com unidade.

O anel definido acima é denominado anel de quocientes (à direita) de Martindale de R. Com uma construção semelhante podemos definir o anel de quocientes à esquerda.

Vejamos como R pode ser mergulhado em Q. Se $a \in R$, denotamos por a_l a multiplicação à esquerda por a (i. e., $a_l : R \to R$ é definida por $a_l(x) = ax$, para todo $x \in R$). É claro que $[R, a_l]$ é um elemento de Q, o qual denotaremos apenas por a_l.

Teorema 4.2. A aplicação $\psi : R \to Q$ definida por $\psi(a) = a_l$, para cada $a \in R$, é um homomorfismo injetor de anéis.

Demonstração. Como $(a+b)x = ax + bx$ e $(ab)x \simeq a(bx)$, para a, b, $x \in R$, é claro que ψ é um homomorfismo de anéis. Como os anéis têm unidade, é conveniente verificar também que $\psi(1_R) = 1_Q$. Mas isto é claro, pois $1_l = id_R = 1_Q$.

Se $a_l = 0$, então, pela definição de relação de equivalência dada, existe um ideal não nulo I de R, tal que $ax = 0$, para todo $x \in I$. Ou seja, $aI = 0$. Definimos $H = \{b \in R : bI = 0\}$. É claro que H é um ideal de R e que $HI = 0$. Como R é primo, segue que $H = 0$ e, assim, $a = 0$. Logo, ψ é injetor. □

O teorema anterior permite identificar R com sua imagem $\psi(R)$ em Q. Utilizando esta identificação, podemos supor $R \subseteq Q$ e, para $a \in R$, escrever $a_l = a$.

O seguinte lema é necessário no que segue.

Lema 4.3. Se $q = [I, f] \in Q$ e $a \in I$, então o produto qa em Q (i. e., qa_l) é igual a $f(a)$.

Demonstração. Se $x \in R$, temos que $f \circ a_l(x)$ está bem definido e $f \circ a_l(x) = f(ax) = f(a)x$. Assim, as aplicações $f \circ a_l$ e $(f(a))_l$ são iguais em R. Conseqüentemente, $qa = [I, f] \circ a_l = (f(a))_l = f(a)$. □

A seguinte proposição contém as propriedades mais importantes sobre o anel Q, que precisaremos mais adiante.

Proposição 4.4. i) $R \subseteq Q$, via ψ.

ii) Se $I \in \mathcal{I}$ e $f : I \to R$ é um R-homomorfismo (à direita), então existe $q \in Q$, tal que $f(a) = qa$, para todo $a \in I$.

iii) Dados n elementos $q_1, ..., q_n \in Q$, existe um ideal $I \in \mathcal{I}$ tal que $q_i I \subseteq R$, para $i = 1, 2, ..., n$.

iv) Se $q \in Q$ e $I \in \mathcal{I}$ é tal que $qI = 0$ ou $Iq = 0$, então $q = 0$.

v) Todo anel intermediário T (anel com $R \subseteq T \subseteq Q$) é também primo. Em particular, Q é primo.

Demonstração. A parte i) já foi provada acima. Para provar ii) basta tomar $q = [I, f]$. Então, ii) segue do Lema 4.3.

iii) Sejam $q_1 = [I_1, f_1], ..., q_n = [I_n, f_n]$. Pelo Lema 4.3, $q_i I_i \subseteq R$, para $i = 1, ..., n$. Então, tomando $I = \bigcap_{i=1}^{n} I_i \in \mathcal{I}$, temos que $q_i I \subseteq R$ para todo $i = 1, ..., n$.

iv) Se $qI = 0$ e $q = [J, g]$, temos que para cada $a \in I \cap J$, $g(a) = 0$, pelo Lema 4.3. Portanto, $g/I \cap J = 0$ e segue que $q = 0$. Antes de provar a outra parte, vejamos primeiro v).

v) Se $0 \neq q \in T$, $0 \neq p \in T$, por iii) e iv) existe um ideal não nulo I de R tal que $0 \neq qI \subseteq R$ e $0 \neq pI \subseteq R$. Tomemos a, $b \in I$ tal que $qa \neq 0$ e $pb \neq 0$. Assim, como R é primo, $qaRpb \neq 0$. Mas $qTpb \supseteq qaRpb$ e, conseqüentemente, $qTp \neq 0$. Logo, T é primo.

Para completar a prova, suponhamos que $Iq = 0$, onde $I \in \mathcal{I}$. Então, para todo $r \in R$, $Irq \subseteq Iq = 0$. Conseqüentemente, $IRq = 0$. Seja $H \in \mathcal{I}$ tal que $qH \subseteq R$. Segue que $IRqH = 0$ e, como R é primo e $I \neq 0$, $qH = 0$. Assim, pela primeira parte de iv) obtemos $q = 0$. A prova está completa. $\square$

Quando D é um domínio comutativo, o corpo de frações de D é um corpo. No caso geral, existe um resultado correspondente muito importante e útil, mas não diretamente para Q, senão para seu centro. De fato, o anel Q não é um anel nem sequer simples, como pode-se ver estudando alguns exemplos.

O centro de Q, que denotamos por C, é definido como é usual por: $C = \{c \in Q : cq = qc, \forall q \in Q\}$. O lema seguinte caracteriza os elementos de C.

Lema 4.5. Seja $q = [I, f] \in Q$. As seguintes condições são equivalentes

i) $q \in C$

ii) f é um homomorfismo bilateral. ($f(xa) = xf(a)$, para todo $a \in I$, $x \in R$).

iii) $qr = rq$, para todo $r \in R$.

Demonstração. i)$\longrightarrow$iii) É imediato.

iii)$\longrightarrow$ii) Seja $a \in I$. Então $qa = f(a)$ e para $r \in R$ temos que $rf(a) = rqa = qra = f(ra)$. Portanto, f é um homomorfismo também à esquerda.

ii)$\longrightarrow$i) Seja $p = [J, g]$. Então, $qp = [JI, f \circ g]$ e $pq = [IJ, g \circ f]$. Seja $H = JI \cap IJ \neq 0$, e $a = ji \in H$ com $j \in J$ e $i \in I$. Assim, $f \circ g(a) = f(g(ji)) = f(g(j)i) = g(j)f(i) = g(jf(i)) = g \circ f(ji) = g \circ f(a)$. Segue que $f \circ g/H = g \circ f/H$, donde $qp = pq$. Conseqüentemente, $q \in C$. $\square$

Teorema 4.6. C é um corpo.

Demonstração. Seja $c \in C$ um elemento não nulo. Vamos mostrar que existe $d \in C$, tal que $cd = dc = 1$.

Suponhamos que $c = [I, f]$. Então, $I \in \mathcal{I}$ e $0 \neq cI \subseteq R$. É fácil verificar que $J = cI$ é um ideal de R e assim $J \in \mathcal{I}$. Se $i \in I$ e $ci = 0$, segue que $cQi = Qci = 0$ e sendo que Q é primo, temos $i = 0$. Portanto, a aplicação $g : J \to R$ definida por $g(ci) = i$, para todo $i \in I$, é uma aplicação bem definida. É claro que g é um homomorfismo bilateral e, conseqüentemente, $d = [J, g] \in C \subseteq Q$. Além disso, as aplicações $f \circ g$ e $g \circ f$ são as identidades sobre os correspondentes domínios. Logo $cd = dc = 1$. $\square$

O corpo C é denominado o centróide extendido de R. O anel gerado por R e C é igual a RC. Este subanel de Q é particularmente importante, e é chamado o fecho central de R. Podemos verificar que o seu centro é ainda C.

Note que o centro $C(R)$ de R está contido em C. Portanto, C contém o corpo de frações de $C(R)$. Mas, em geral, este corpo de frações não é igual a C.

Exercícios:

1) Provar que a relação definida por: $(I, f) \sim (J, g)$ se, e somente se, existir $0 \neq H \subseteq J \cap J$ é uma relação de equivalência. Provar, ainda, que $(I, f) \sim (J, g)$ se, e somente se, $f/(I \cap J) = g/(I \cap J)$.

2) Provar que a soma e o produto em Q são operações bem definidas.

3) Provar o Teorema 4.1. Especificar os elementos 0_R, 1_R e $-[I, f]$ para $(I, f) \in Q$.

4) Seja $c \in C$ e $I \in \mathcal{I}$, tal que $cI \subseteq R$. Provar que cI é um ideal de R e que a aplicação $cI \to R$ dada por $ci \mapsto i$, para cada $i \in I$, é um homomorfismo bilateral.

5) Seja R um anel simples. Provar que o anel de quocientes de Martindale de R é igual a R.

6) Provar que, se R é um domínio de integridade comutativo, então o corpo de frações de R é igual ao anel de quocientes de Martindale de R.

§5. EXTENSÕES CENTRALIZANTES

Neste parágrafo vamos apresentar as extensões centralizantes de anéis, que serão objeto de estudo no capítulo II, e dar vários exemplos.

Dado um anel R, um anel S (com unidade) é dito uma extensão de R se R e S tem a mesma unidade e R está contido em S.

Na Teoria de Anéis não comutativos aparecem muitos tipos de extensões de anéis, mas vamos nos restringir somente às extensões centralizantes.

Uma extensão $S \supseteq R$ é dita uma extensão centralizante se existir um sistema de elementos $X \subseteq S$, tal que:

i) X é um conjunto R-centralizante, i.e., para todo $x \in X$, $r \in R$, $rx = xr$.

ii) S é gerado como R-módulo (à direita ou à esquerda, logo aos dois lados) por X, ou seja, para todo $s \in S$ existem $x_i \in X$, $r_i \in R$, $i = 1, ..., n$, tal que $s = \sum_{i=1}^{n} r_i x_i$.

Quando S é uma extensão deste tipo vamos denotar $S = R[X]$. É claro que se X satisfaz as condições acima, então $X \cup \{1\}$ também satisfaz as mesmas condições. Logo, podemos sempre supor que $1 \in X$.

O conjunto X é arbitrário, não necessariamente finito. No caso particular em que podemos encontrar um sistema X como o acima, e que seja finito, a extensão chama-se centralizante finita ou simplesmente liberal [RS].

Se S é uma extensão centralizante de R e podemos encontrar um sistema X como o acima (com $1 \in X$) que seja linearmente independente sobre R, vamos dizer que S é uma extensão centralizante livre de R. Ou seja, S é uma extensão centralizante livre de R se existir um sistema R-independente $E = (e_i)_{i \in \Gamma} \subseteq S$, tal que $1 \in E$, $re_i = e_i r$, para todo $r \in R$ e $i \in \Gamma$, e tal que $S = \sum_{i \in \Gamma} Re_i$. Neste caso, é claro que $S = \sum_{i \in \Gamma} \oplus Re_i$.

Exemplo 1. Anéis de polinômios. Seja t uma indeterminada e $S = R[t]$ o anel de polinômios sobre R. Neste caso, temos que $E = \{1, t, t^2, ...\}$ é uma base de S sobre R que é centralizante sobre R. Então, S é uma extensão centralizante livre de R.

O mesmo acontece se considerarmos um anel de polinômios sobre R em um número arbitrário de indeterminadas $(t_i)_{i \in \Gamma}$. Note que o conjunto de indeterminadas não precisa ser finito nem que elas comutem entre si. Por exemplo, o anel de polinômios $S = R[x, y]$ sobre R em duas indeterminadas x e y, onde $xy \neq yx$, é uma extensão centralizante livre de R que tem como base o conjunto E formado por 1 e todos os produtos $x_1 ... x_n$, onde $n \geq 1$ é arbitrário e para cada j, $1 \leq j \leq n$, $x_j = x$ ou $x_j = y$.

Exemplo 2. Anéis de matrizes. Seja n um número natural e seja $S = M_n(R)$ o anel das matrizes quadradas de ordem n sobre R. É conhecido que S é um anel cuja unidade é a matriz $I = (\delta_{ij})$, $\delta_{ij} = 1$ se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$. Então, a aplicação $\varphi : R \to M_n(R)$, $\varphi(r) = rI$,para todo $r \in R$, é um homomorfismo injetor de anéis, que permite considerar $R \subseteq S$.

A matriz elementar E_{ij}é a matriz que tem na linha i e coluna j o elemento

1 e todas as outras entradas nulas. Também é conhecido que S é uma extensão finita centralizante livre de R com base $E = (E_{ij})_{1\leq i\leq n, 1\leq j\leq n}$. Na verdade, para ver que S é uma extensão centralizante livre de R devemos encontrar uma base contendo I. Mas isso é fácil; basta substituirmos em E o elemento E_{11} por $I(= E_{11} + ... + E_{nn})$. É fácil verificar que assim temos uma nova base E' que contém I.

Exemplo 3. Anéis de matrizes infinitas. Usando os anéis $M_n(R)$, $n \geq 2$, podemos construir também um anel de matrizes infinitas que continua sendo uma extensão centralizante livre de R. De fato, cada $A \in M_n(R)$ pode ser pensada como uma matriz infinita (infinitas linhas e colunas) completando com zeros. Assim, podemos pôr $M_\infty(R) = \bigcup_{n\geq 2} M_n(R)$.

Se A, $B \in M_\infty(R)$, então existe $m \geq 2$, tal que A, $B \in M_m(R)$. Logo, as operações nos anéis $M_n(R)$, $n \geq 2$, induzem uma soma e um produto em $M_\infty(R)$. É fácil verificar que estas operações estão bem definidas e dotam $M_\infty(R)$ de uma estrutura de anel sem unidade.

Cada $A \in M_\infty(R)$ é uma matriz infinita, mas que possui todas as suas linhas e colunas nulas, a partir de uma delas, respectivamente. Logo, existe um número finito de elementos não nulos $r_{ij} \in R$, tal que $A = \sum_{i,j} r_{ij}E_{ij}$, onde as matrizes elementares E_{ij} são definidas como antes. Por outro lado, é claro que $rE_{ij} = E_{ij}r$, para todo i, j e $r \in R$. Assim, temos "quase" uma extensão centralizante livre de R.

Para completar a construção basta lembrar que, dado um anel sem unidade qualquer T, existe um anel com unidade T^*, que contém T, construído da maneira seguinte: $T^* = \mathbf{Z} \oplus T$, a soma de T^* é a usual e o produto é dado por

$$(n, t)(m, t') = (nm, nt' + mt + tt'),$$

para todo (n, t), $(m, t') \in T^*$ (a contenção $T \subseteq T^*$ se consegue via $t \mapsto (0, t)$).

Seja $M_\infty(R)^*$ o anel obtido a partir de $M_\infty(R)$ anexando uma unidade I como acima. Agora podemos considerar $R \subseteq M_\infty(R)^*$ como no Exemplo 2 via a aplicação $\varphi : R \to M_\infty(R)^*$, $\varphi(r) = rI$, para todo $r \in R$. É fácil ver que o anel de matrizes infinitas $M_\infty(R)^*$ é uma extensão centralizante livre de R com base $\{E_{ij} : 1 \leq i < \infty, 1 \leq j < \infty\} \cup \{I\}$.

Exemplo 4. Anéis de grupos. Dado um grupo multiplicativo G e um anel (com unidade) R, o anel de grupo RG é definido tendo como conjunto subjacente o conjunto de todas as combinações lineares formais (finitas) $\sum_{g\in G} r_g g$, onde $r_g \in R$ e $r_g = 0$ salvo para um número finito de elementos $g \in G$.

As operações em RG são definidas de maneira natural:

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

e

$$\sum_{g\in G} r_g g \sum_{h\in G} s_h h = \sum_{g,h\in G} (r_g s_h)(gh).$$

É fácil ver que RG é um anel e que contém R via a aplicação $R \to RG$ dada por $r \mapsto re$, onde e é o elemento neutro de G. É claro que, pela própria definição, RG é uma extensão centralizante livre de R, cuja base é $E = (g)_{g\in G}$. Também RG é uma extensão finita de R se, e somente se, G é um grupo finito.

Exemplo 5. Produtos tensoriais sobre corpos. Sejam F um corpo, R e T duas álgebras sobre F. Então é conhecido que o produto tensorial $S = R\otimes_F T$ é uma F-álgebra. Também, se $(e_i)_{i\in\Gamma}$ é uma base de T sobre F, então $E = (1\otimes e_i)_{i\in\Gamma}$ é uma base de S sobre R e que $r(1\otimes e_i) = (1\otimes e_i)r$, para todo $r \in R$, $i \in \Gamma$. Além disso,a aplicação $R \to S$, tal que $r \mapsto r\otimes 1$ é um homomorfismo injetor de anéis. Logo, S é uma extensão centralizante livre de R com base E (para apresentar este exemplo, supomos que o leitor tem suficiente conhecimento sobre produtos tensorias; caso contrário, o leitor pode desconsiderá-lo).

Exemplo 6. Extensões centralizantes não necessariamente livres. O leitor poderá dizer, com justa razão, que em todos os exemplos apresentados a extensão dada é livre sobre R. Mas, é muito fácil construir extensões não necessariamente livres.

De fato, seja S uma extensão centralizante livre qualquer de R e seja I um ideal de S, tal que $I \cap R = 0$. Então, podemos considerar R contido em S/I via a aplicação $R \to S/I$, $r \mapsto \bar{r}$. Também é fácil verificar que se $E = (e_i)_{i\in\Gamma}$ é a base de S sobre R, então $(\bar{e}_i)_{i\in\Gamma}$ é um sistema de geradores centralizantes de S/I sobre R. Logo, S/I é uma extensão centralizante de R, a qual não é livre, em geral, sobre R.

De fato, se I é o ideal de $\mathbf{Z}[t]$ gerado pelo polinômio $(2t-1)$, o quociente $S = \mathbf{Z}[t]/I$ é uma extensão liberal de $\mathbf{Z}$ gerada por 1 e $\bar{t} = t + I$, mas S não é livre sobre $\mathbf{Z}$, pois $2\bar{t} - 1 = \bar{0}$ em S.

<u>Exercícios</u>:

1) Seja R um anel sem unidade e seja $R^* = \mathbf{Z} \oplus R$ o anel definido pelas operações:

$$(n, r) + (m, s) = (n + m, r + s)$$

e

$$(n, r)(m, s) = (nm, ns + mr + rs).$$

Provar que R^* é realmente um anel com unidade (1,0) e que a aplicação natural $\varphi : R \to R^*$ é um homomorfismo injetor de anéis. Além disso, R é, via φ, um ideal de R^* tal que $R^*/R \simeq \mathbf{Z}$.

2) Seja S um anel extensão de R, tal que existe $(x_i)_{i\in\Gamma} \subseteq S$, com $S = \sum_{i\in\Gamma} Rx_i$ e $rx_i = x_i r$, para todo $r \in R$, $i \in \Gamma$. Provar que S^* é uma extensão centralizante de R, onde S^* é definido como no exercício anterior.

3) Seja S uma extensão centralizante de R e I um ideal de S. Então, $I \cap R$ é um ideal de R. Provar que a aplicação natural $R/(I \cap R) \to S/I$ permite considerar S/I uma extensão centralizante de $R/(I \cap R)$.

4) Seja S uma extensão centralizante livre de R com base E e seja I um ideal de R. Provar que $I[E] = \{\sum_j a_j e_j : a_j \in I, e_j \in E\}$ é um ideal de S e que $S/I[E] \simeq (R/I)[E]$ é uma extensão centralizante livre de (R/I).

5) Sejam $n > m$ inteiros e sejam $M_m(R) \to M_n(R) \to M_\infty(R)$ as aplicações evidentes, obtidas completando com zeros. Provar que estas aplicações são homomorfismos injetores de anéis.

6) Seja R um anel e G um semigrupo multiplicativo (com elemento neutro). Construir o anel de semigrupo RG. Observar que este é um novo exemplo de extensão centralizante livre que inclui os exemplos 1 e 4.

§6. IDEAIS PRIMOS EM EXTENSÕES DE ANÉIS

O problema central que estamos considerando nestas notas é a relação existente entre os ideais primos de um anel R e os ideais primos de uma extensão S de R. Apresentado assim, o problema é muito geral. Vejamos alguns dos problemas específicos que podem ser considerados.

Lembremos primeiramente as questões usualmente consideradas na Álgebra Comutativa.

Se $R \subseteq S$ são anéis comutativos e P é um ideal primo de S, é claro que $P \cap R$ é um ideal primo de R. O primeiro problema a considerar é o recíproco deste fato: dado um ideal primo p_0 de R, existe um ideal primo P de S tal que $P \cap R = p_0$. Mais ainda, suponha que $p_0 \subset p_1$ são ideais primos de R e que P_0 é um ideal primo de S tal que $P_0 \cap R = p_0$. Então existe um ideal primo P_1 de S tal que $P_1 \supset P_0$ e $P_1 \cap R = p_1$? Esta questão é conhecida como "going up".

Lembremos que um anel comutativo $S \supseteq R$ é dito uma extensão inteira de R se todo $s \in S$ satisfaz algum polinômio mônico $f(t) \in R[t]$. Ambas as questões acima têm resposta positiva se S é uma extensão inteira de R ([AM], Cap. 5).

Um outro problema que tem resposta positiva para extensões inteiras é conhecido como incomparabilidade ("incomparability") ([AM], Cap. 5). Ele pode ser estabelecido assim: sejam $P_0 \subseteq P_1$ ideais primos de S tais que $P_0 \cap R = P_1 \cap R$. Então é necessariamente $P_0 = P_1$?

As questões anteriores estão na base do conceito de dimensão de Krull de um anel R. Esta dimensão é medida pelo número de elementos de uma cadeia de ideais primos $P_0 \subset P_1 \subset ... \subset P_n$ de R, a mais longa possível. Aparece naturalmente a questão de determinar relações entre as dimensões de Krull de R e S para $S \supset R$.

Uma outra questão interessante e que, em geral, tem uma resposta mais complicada que a do "going up" é o problema do "going down": sejam $p_0 \subset p_1$ ideais primos de R e P_1 um ideal primo de S tal que $P_1 \cap R = p_1$. Então existe um ideal primo P_0 de S tal que $P_0 \subset P_1$ e $P_0 \cap R = p_0$?

Finalmente, seja P um ideal primo de S e $p = P \cap R$ o correspondente ideal primo de R. Suponha que P (ou p) é maximal. Será que isto implica que p (ou P) é também maximal?

Esta última questão tem um significado especial muito interessante em anéis não comutativos. De fato, sejam p e P ideias primos de R e S, respectivamente, tal que $P \cap R = p$. Sabemos que em anéis não comutativos existem muitas classes diferentes de ideais primos. Então podemos perguntar sob que condições teremos a validade de alguma das implicações seguintes: P (resp. p) é de tal tipo especial (por exemplo, fortemente primo, primo não singular, primitivo, etc), então p (resp. P) é do mesmo tipo?

Os problemas anteriores em anéis não comutativos são muito ricos e muita literatura tem sido dedicada a considerá-los. Existe uma complicação inicial no fato de que dado um ideal primo P de S não necessariamente $P \cap R$ é um ideal primo de R, em geral. Então as questões ("going up", incomparabilidade, etc) têm sido adequadamente modificadas para poder ser extendidas aos anéis não comutativos. Uma lista considerável de trabalhos de pesquisa sobre ideais primos em extensões de anéis não comutativos é dada na bibliografia.

Finalmente, existe uma técnica muito útil que já mencionamos antes, para estudar problemas de ideais primos. Consiste no seguinte: seja P um ideal primo de um anel de polinômios $D[t]$, onde D é um domínio de integridade e $P \cap R = 0$. Sabemos que D está contido no seu corpo de frações F. Logo, podemos considerar $D[t] \subset F[t]$. Então existe um único ideal primo P^* de $F[t]$ tal que $P^* \cap D[t] = P$. Mais ainda, a correspondência $P \leftrightarrow P^*$ é biunívoca ([K], Th. 36).

Uma das principais questões, que responderemos no Capítulo II destas notas, é a possibilidade de extender este resultado aos anéis não comutativos.

Vamos restringir-nos aqui às extensões centralizantes de um anel R. Ideais primos em extensões centralizantes têm sido considerados em vários trabalhos, começando pelas extensões finitas ([RS], [R_1]). Finalmente, métodos para estudar o caso geral (onde S não é necessariamente finitamente gerado como R-módulo), foram desenvolvidos por mim em vários trabalhos ([F_3], [F_4], [F_5]). Também os métodos mostraram-se úteis para provar resultados sobre radicais de extensões centralizantes de anéis e produtos tensoriais ([F_6], [FPu]). O objetivo do próximo capítulo destas notas será dedicado a apresentar estes métodos e alguns dos resultados mais importantes obtidos desta maneira.

Para terminar este capítulo, provamos alguns fatos que usaremos no Capítulo II.

Seja $S = R[X]$ uma extensão centralizante de R, com sistema de geradores centralizantes X. Se I é um ideal de R, então denotamos por $I[X]$ o conjunto de todas as somas finitas $\sum_i a_i x_i$, onde $a_i \in I$, $x_i \in X$, para todo i. Então é fácil verificar que $I[X]$ é um ideal de S e que $I[X] = IS = SI$. Conseqüentemente, se I e J são ideais de R, então segue que $I[X]J[X] \subseteq (IJ)[X]$.

É conveniente salientar que se S é livre sobre R com base E e se I é um ideal de R, então $I[E] \cap R = I$.

Lema 6.1. Se P é um ideal primo de S, então $P \cap R$ é um ideal primo de R.

Demonstração. Se A e B são ideais de R tais que $AB \subseteq P \cap R$, segue que $A[X]B[X] \subseteq (AB)[X] \subseteq (P \cap R)[X] \subseteq P$. Agora, como P é primo, obtemos $A[X] \subseteq P$ ou $B[X] \subseteq P$, donde $A \subseteq A[X] \cap R \subseteq P \cap R$ ou $B \subseteq B[X] \cap R \subseteq P \cap R$. $\square$

Não é necessariamente verdade que se p é um ideal primo de R, então $p[X]$ é um ideal primo de S (ver exercícios). Isto é verdadeiro em alguns casos particulares.

Suponhamos que S é uma extensão centralizante livre de R com base E e que P seja um ideal primo de S. Então $P \cap R$ é um ideal primo de R e podemos considerar o ideal $(P \cap R)[E]$ de S. Se denotamos por $\bar{R}$ o anel quociente $R/(P \cap R)$ e por $\bar{S} = S/(P \cap R)[E]$, podemos provar o seguinte

Lema 6.2. Se S é uma extensão centralizante livre de R com base E e se P é um ideal primo de S, então o anel $\bar{S}$ é uma extensão centralizante livre do anel primo $\bar{R}$. Além disso, o ideal $\bar{P} = P/(P \cap R)[E]$ de $\bar{S}$ verifica $\bar{P} \cap \bar{R} = \bar{0}$.

Demonstração. É claro que $\bar{E} = \{\bar{e} = e + (P \cap R)[E]\}$ é um sistema de geradores centralizantes de $\bar{S}$ sobre $\bar{R}$. Também $\bar{R}$ é primo pelo Lema 6.1.

Vejamos que $\bar{E}$ é $\bar{R}$-linearmente independente. Se $\sum_{i=1}^{n} \bar{r}_i \bar{e}_i = \bar{0}$, com $\bar{r}_i \in \bar{R}$, segue que $\sum_{i=1}^{n} r_i e_i \in (P \cap R)[E]$. Como E é R-independente, obtemos facilmente que $r_i \in P \cap R$, para $i = 1, ..., n$. Conseqüentemente, $\bar{r}_i = \bar{0}$ em $\bar{R}$. Logo, $\bar{E}$ é uma base se $\bar{S}$ sobre $\bar{R}$.

Para completar a prova vejamos que $\bar{P} \cap \bar{R} = \bar{0}$. De fato, seja $\bar{a} \in \bar{P} \cap \bar{R}$, com $a \in R$. Sendo que $\bar{a} = a + (P \cap R)[E]$, segue que $a \in P$, pois $(P \cap R)[E] \subseteq P$. Conseqüentemente, $a \in P \cap R$ e assim, $\bar{a} = \bar{0}$.

O Lema 6.2 permite-nos fazer uma redução para estudar P em S. Veremos que para alguns propósitos será suficiente estudar $\bar{P}$ em $\bar{S}$, o qual satisfaz $\bar{P} \cap \bar{R} = 0$. Por esta razão, é conveniente fazermos a seguinte

Definição 6.3. Um ideal I de R é dito R-disjunto se $I \cap R = 0$.

Ideais R-disjuntos serão estudados no próximo capítulo.

Exercícios:

1) Seja R um anel primo. Provar que o anel de polinômios $R[t]$ é também um anel primo.

2) Seja K um corpo e seja $S = K[t]/(t^2)$. Provar que S é uma extensão centralizante livre de K e que S não é um anel primo. Conseqüentemente, o ideal nulo de K é primo e se extende a um ideal de S que não é primo.

3) Seja S uma extensão centralizante livre de R com base E e seja P um ideal primo de S. Provar que $\bar{S}/\bar{P} \simeq S/P$, onde $\bar{S} = S/(P \cap R)[E]$ é uma extensão centralizante livre de $\bar{R} = R/(P \cap R)$ com base $\bar{E}$ e $\bar{P} = P/(P \cap R)[E]$.

4) Sejam S, R e P como no exercício 3. Provar que P é um primo de um dos tipos especiais estudados no §2 se, e somente se, $\bar{P}$ é um ideal de $\bar{S}$ do mesmo tipo.

Capítulo II - IDEAIS PRIMOS EM EXTENSÕES CENTRALIZANTES.

§1. UMA REDUÇÃO

Seja $S = R[X]$ uma extensão centralizante de R. Se P é um ideal primo de S, então $(P \cap R)$ é um ideal primo de R. Assim, o anel $\bar{R} = R/(P \cap R)$ é um anel primo. Além disso, $I = (P \cap R)S = (P \cap R)[X]$ é um ideal de S tal que $I \cap R = P \cap R$. Logo, podemos considerar $\bar{R}$ contido no anel $\bar{S} = S/I$, o qual (é fácil verificar) é uma extensão centralizante de $\bar{R}$ com geradores $\bar{X} = \{x + I : x \in X\}$ (de agora em diante identificaremos $\bar{X}$ com X). É conveniente notar que se S é livre sobre R com base X, então $\bar{S}$ também é livre sobre $\bar{R}$, com a mesma base X.

Como $P \supseteq I$, podemos considerar o ideal $\bar{P} = P/I$ de $\bar{S}$. É fácil verificar que $\bar{P}$ é um ideal primo de $\bar{S}$ tal que $\bar{P} \cap \bar{R} = 0$. Além disso, $\bar{S}/\bar{P} \simeq S/P$.

O argumento acima justifica que, para vários propósitos, em lugar de estudar P como ideal de S possamos estudar $\bar{P}$ em $\bar{S}$. Assim, o estudo reduz-se ao caso de um ideal primo R-disjunto numa extensão centralizante de um anel primo.

Isto mostra que nosso trabalho pode ser restrito a estudar extensões centralizantes de anéis primos e a descrever os ideais primos que são R-disjuntos. É o que faremos a partir de agora, até que algo seja dito em contrário.

§2. CASO LIVRE

Primeiramente, vamos supor que $S = R[E]$ é uma extensão centralizante livre de um anel primo R com base centralizante $E = (e_i)_{i \in \Gamma}$.

Se $x \in S$, existem únicos elementos $r_i \in R$, $e_i \in E$, tal que $x = \sum_i r_i e_i$, onde os elementos r_i são nulos salvo um número finito de índices $i \in \Gamma$. Denotaremos por $x(e_i)$ a i-ésima componente de x, i. e., $x(e_i) = r_i$ para todo $i \in \Gamma$. O suporte de x é definido por $\sup(x) = \{e \in E : x(e) \neq 0\}$. É claro que $\sup(x)$ é um subconjunto finito de E.

Seja I um ideal R-disjunto de S. Um elemento não nulo $x \in I$ é dito de suporte minimal em I se para todo $y \in I$, tal que $\sup(y) \subset \sup(x)$, temos $y = 0$ (ou seja, $\sup(y) = \emptyset$).

Denotamos $M(I)$ o conjunto de todos os elementos x de suporte minimal em I. A minimalidade de I é definida como o conjunto de todos os suportes destes elementos minimais de I. Ou seja, $Min(I) = \{\sup(x) : x \in M(I)\}$. Este conceito de minimalidade é, provavelmente, o conceito mais importante para o funcionamento do método que vamos apresentar.

Para cada $L \in Min(I)$ e $e \in L$, denotamos por $\theta_{L,e}(I)$ o ideal de R formado por 0 e pelos elementos $a \in R$, tais que existe $x \in I$ com $\sup(x) = L$ e $x(e) = a$.

Seja I um ideal R-disjunto de S. O fecho de I é definido por:

$$[I]_R = \{x \in S : \text{ existe } 0 \neq H \lhd R, \text{ tal que } xH \subseteq I\}.$$

Quando não existir possibilidade de confusão, omitiremos o índice R, denotando o fecho simplesmente por $[I]$.

Sendo que S é gerado por R e E, e considerando que os elementos de E são centralizantes sobre R, é fácil verificar que $[I]$ é um ideal de S que contém I. Também $[I]$ é R-disjunto. De fato, se $a \in [I] \cap R$, existe um ideal não nulo H de R tal que $aH \subseteq I \cap R = 0$. Agora, como R é primo segue facilmente que $a = 0$.

Existe uma bela caracterização do ideal $[I]$. Mas, antes, queremos destacar a razão do seu estudo.

Um ideal R-disjunto I é dito fechado se $[I] = I$. Temos a seguinte

Proposição 2.1. Se P é um ideal primo R-disjunto de S, então P é fechado.

Demonstração. Seja $x \in [P]$. Então existe um ideal não nulo H de R tal que $xH \subseteq P$. Note que $HS = H[E]$ é um ideal de S não contido em P, pois $H[E] \cap R = H \neq 0$. Logo, $(SxS)(SHS) = SxHS \subseteq P$ e segue que $x \in P$. Assim, $[P] = P$. $\square$

Como conseqüência da Proposição anterior, vemos que o estudo dos ideais fechados e, por conseguinte, do fecho de um ideal, é um fato fundamental que vai permitir obter informação sobre os ideais primos.

O seguinte teorema dá uma caracterização muito útil de $[I]$.

Teorema 2.2. Seja I um ideal R-disjunto de S. Então, $[I]$ é o maior ideal J de S que satisfaz as condições $J \supseteq I$ e $Min(J) = Min(I)$.

Demonstração. Seja $x = a_1e_1 + ... + a_ne_n \in [I]$ um elemento de suporte minimal em $[I]$. Então, $xH \subseteq I$ para $0 \neq H \lhd R$. Como R é primo, $a_1H \neq 0$. Logo, existe $h \in H$ tal que $a_1h \neq 0$ e temos que $xh = a_1he_1 + ... + a_nhe_n \in I$. Se $a_ih = 0$ para algum $1 < i \leq n$, temos que $\sup(xh) \subset \sup(x)$, o qual é uma contradição pois $xh \in [I]$. Assim, existe um elemento $xh \in I$ cujo suporte é igual a $\sup(x)$.

A recíproca é claramente verdadeira. Ou seja, se $y \in I$ é de suporte minimal em I, existe um elemento em $[I]$ (o próprio y) que tem o mesmo suporte.

Conseqüentemente, $Min([I]) = Min(I)$. Vejamos agora que $[I]$ é maximal com respeito às propriedades $[I] \supseteq I$ e $Min([I]) = Min(I)$.

Seja J um ideal de S tal que $J \supseteq I$ e $Min(J) = Min(I)$ (note que neste caso J é R-disjunto, pois se $1 \in Min(J)$, então $1 \in Min(I)$ e segue que $I \cap R \neq 0$). Sejam $L = \{e_1, ..., e_n\} \in Min(J)$ e $x = a_1e_1 + ... + a_ne_n \in I$ com $\sup(x) = L$. Tomemos $y = b_1e_1 + ... + b_ne_n \in J$, com mesmo suporte L. Então,

$yra_1 - b_1rx = (b_2ra - b_1ra_2)e_2 + ... + (b_nra_1 - b_1ra_n)e_n \in J$, para cada $r \in R$, e como $\sup(yra_1 - b_1rx) \subset L$ temos $yra_1 - b_1rx = 0$. Segue que $yRa_1R \subseteq I$, onde Ra_1R é um ideal não nulo de R, i. e., $y \in [I]$.

O argumento acima prova duas coisas. A primeira é que todo elemento de $M(J)$ está em $[I]$. A segunda é um passo essencial para um raciocínio de indução: para cada $y \in M(J)$ existe um ideal não nulo $H = Ra_1R$, que depende somente de $\sup(y)$, tal que $yH \subseteq I$. Ou seja, se $z \in M(J)$ e $\sup(z) = \sup(y)$, então $zH \subseteq I$ com H também igual a Ra_1R.

Vamos provar por indução que, para todo $y \in J$, existe um ideal não nulo H de R tal que $zH \subseteq I$, para todo $z \in J$ com $\sup(z) \subseteq \sup(y)$. Segue, em particular, que $y \in [I]$ e a prova estará completa.

Seja $y = c_1e_1 + ... + c_me_m \in J$, com $c_i \neq 0$ para $1 \leq i \leq m$. Assim, $\sup(y) = \{e_1, ..., e_m\}$. Se $\sup(y) \in Min(J)$, a afirmação foi provada acima. Então podemos supor que existe um subconjunto próprio de $\sup(y)$, digamos $L = \{e_1, ..., e_t\}$, $t < m$, tal que $L \in Min(J) = Min(I)$. Portanto, existe $x = a_1e_1 + ... + a_te_t \in M(I)$, com $\sup(x) = L$. Pela hipótese de indução, podemos ainda supor que existe um ideal não nulo H de R tal que, para todo $v \in J$ com $\sup(v) \subset \{e_1, ..., e_m\}$, $vH \subseteq I$.

Suponhamos que $z = d_1e_1 + ... + d_me_m \in J$ e $\sup(z) = \sup(y)$. Consideremos $v = zra_1 - d_1rx \in J$, onde $r \in R$. Como $\sup(v) \subseteq \{e_2, .., e_m\}$, segue que $vH \subseteq I$. Portanto, $zRa_1H \subseteq I$, pois $x \in I$ e o ideal não nulo Ra_1H de R é independente de z. $\square$

A Proposição 2.1 e o Teorema 2.2 têm o seguinte interessante

Corolário 2.3. Seja P um ideal primo R-disjunto de S. Então, P é o maior ideal J de S que contém P e que satisfaz $Min(J) = Min(P)$.

Note que o Teorema 2.2 é simétrico, pois o conceito de minimalidade o é. Isto implica que a definição de fecho de um ideal também deve ser simétrica. De fato, se definimos

$$[I]' = \{x \in S : \text{ existe } 0 \neq H \lhd R \text{ tal que } Hx \subseteq I\},$$

podemos provar de maneira semelhante um análogo do Teorema 2.2. Assim, $[I] = [I]'$. Temos então o seguinte

Corolário 2.4. Se I é um ideal R-disjunto de S, então $[I] = \{x \in S : \text{ existe } 0 \neq H \lhd R \text{ tal que } Hx \subseteq I\}$.

Finalmente, é conveniente salientar a seguinte

Observação 2.5. Na prova do Teorema 2.2 fica evidente que dado $y \in [I]$

existe $0 \neq H \lhd R$, tal que, não somente $yH \subseteq I$, como também $zH \subseteq I$ para todo $z \in [I]$ com $\sup(z) \subseteq \sup(y)$.

§3. EXTENSÃO E CONTRAÇÃO DE IDEAIS PRIMOS

Seja $S = R[E]$ uma extensão centralizante livre do anel primo R e seja Q o anel de quocientes (à direita) de Martindale de R. Então o anel $T = Q[E]$ está definido de maneira evidente: seus elementos são as combinações lineares finitas com coeficientes em Q e a multiplicação é induzida pelas multiplicações em Q e S. Assim, T é uma extensão centralizante livre do anel primo Q com base E.

Seja C o centróide extendido de R. Então o conjunto dos elementos $x \in T$, cuja representação na base E é do tipo $x = \sum_{i=1}^{n} c_i e_i$, $c_i \in C$, é um subanel de T. É claro que este subanel é uma extensão centralizante livre do corpo C com mesma base E. Denotamos este anel por $V = C[E]$. Note que V é uma álgebra sobre C e que os elementos de V comutam com os elementos de Q.

Podemos considerar então $S \subseteq T$ e $V \subseteq T$. É conveniente observar também que $T \simeq Q \otimes_C C[E]$. Daí, segue o seguinte resultado, que será utilizado mais adiante.

Lema 3.1. Todo subconjunto de elementos $\Omega \subset C[E]$ que é C-independente, é também Q-independente como subconjunto de $Q[E]$.

Demonstração. É conhecido que se Ω é C-independente, então o conjunto $(1 \otimes \omega)_{\omega \in \Omega}$ é Q-independente em $Q \otimes_C C[E]$. Basta agora passar a T via o isomorfismo natural $T \simeq Q \otimes_C C[E]$. □

Nesta secção vamos mostrar que existe uma correspondência biunívoca entre os ideais primos R-disjuntos de S, os ideais primos Q-disjuntos de T e os primos de V.

Para fazer isso vamos primeiramente estabelecer uma correspondência biunívoca entre ideais fechados, da qual se obtém a correspondência para primos como caso particular.

Infelizmente precisamos desenvolver bastante maquinaria para obter estes resultados. Por estas razões, o que segue nestas notas será a parte técnica mais pesada, mas não poderemos evitá-la.

Comecemos pelo seguinte

Lema 3.2. Seja I um ideal R-disjunto de S, $L \in Min(I)$ e $e \in L$. Então existe um único elemento $m_{L,e} \in V$ tal que $\sup(m_{L,e}) = L$, $m_{L,e}(e) = 1$ e para todo $x \in I$ com $\sup(x) = L$ temos $x = x(e)m_{L,e} = m_{L,e}x(e)$.

Demonstração. Seja $H = \theta_{L,e}(I)$, onde $L = \{e_1, ..., e_n\}$ e $e = e_1$. Se

$a \in H$ existe um único $x \in I$ tal que $x = a_1e_1 + ... + a_ne_n$, onde $a_1 = a$. Logo, a função $f_i : H \to R$ definida por $f_i(a) = a_i$, $i = 1, 2, ..., n$, está bem definida. É fácil ver também que estas funções são R-homomorfismos bilaterais. Pelos resultados da Sec. 3, Cap. I, existem $c_i \in C$ tais que $c_ia = f_i(a) = a_i$, para $i = 1, 2, ..., n$. Definimos $m_{L,e}$ por $m_{L,e} = \sum_{i=1}^{n} c_ie_i \in V$. Claramente, $\sup(m_{L,e}) = L$ e $m_{L,e}(e) = c_1 = 1$ (pois $f_1 = id_H$).

Seja $x = b_1e_1 + ... + b_ne_n \in I$, onde $x(e) = x(e_1) = b_1$. Pela definição de f_i, $c_ib_1 = f_i(b_1) = b_i$ e então, $b_1m_{L,e} = \sum_{i=1}^{n} c_ib_1e_i = \sum_{i=1}^{n} b_ie_i = x$. Analogamente, $m_{L,e}b_1 = x$. □

Dado um ideal R-disjunto I de S, denotamos por $M_C(I)$ o conjunto de todos os elementtos $m_{L,e}$ construídos no lema anterior, onde $L \in Min(I)$ e $e \in L$. Assim $M_C(I) \subseteq V$ e para qualquer $m \in M_C(I)$ existe um ideal não nulo H de R tal que $mH \subseteq I$.

Suponhamos ainda que I é um ideal R-disjunto de S (ou Q-disjunto de T). Um elemento $y \in Q[E]$ é chamado um resto módulo I, se para qualquer $x \in I$ com $\sup(x) \subseteq \sup(y)$ temos necessariamente que $x = 0$. É claro que se y é um resto módulo I, então $y \notin I$ e para todo ideal não nulo H de R, $yH \cap I = 0$.

O seguinte lema estabelece um algoritmo de divisão para $Q[E]$.

Lema 3.3. Seja I um ideal R-disjunto de S e seja $x \in T$. Então existem $q_i \in Q$, $m_i \in M_C(I)$, $i = 1, 2, ..., n$, e $y \in T$ tal que $x = \sum_{i=1}^{n} q_im_i + y$, onde $y = 0$ ou y é um resto módulo I.

Demonstração. Se x é um resto módulo I não há o que provar. Suponhamos o contrário e seja $L = \sup(x)$, $t = |L|$, o número de elementos de L. Então existe $y \in I$ com $L_1 = \sup(y) \subseteq L$ e podemos supor, sem perda de generalidade, que $y \in M(I)$. Logo, pela construção do Lema 3.2, tomando $e_1 \in L_1$ podemos considerar o elemento $m_1 = m_{L_1,e_1} \in M_C(I)$. Assim, $z = x - x(e_1)m_1 \in Q[E]$ satisfaz $z(e_1) = 0$ (pois $m_1(e_1) = 1$) e $L' = \sup(z) \subset \sup(x)$. Conseqüentemente $|L'| \leq t - 1$.

Se z é nulo ou um resto módulo I, a prova estará completa. Caso contrário podemos repetir o argumento começando agora com z. É fácil completar a prova por indução. □

Lema 3.4. Com as mesmas notações acima, $QM_C(I) = \{x \in Q[E]$: existe $0 \neq H \lhd R$ tal que $xH \subseteq I\}$.

Demonstração. Se $x \in QM_C(I)$, então existem $q_i \in Q$, $m_i \in M_C(I)$, $i = 1, ..., n$, tal que $x = \sum_{i=1}^{n} q_im_i$. Sabemos que existem ideais não nulos H_i e J_i de R tais que $q_iH_i \subseteq R$ e $m_iJ_i \subseteq I$, para $i = 1, ..., n$. Sejam $H = \bigcap_{i=1}^{n} Hi \neq 0$ e $J = \bigcap_{i=1}^{n} J_i \neq 0$. Então $q_iH \subseteq R$ e $m_iJ \subseteq I$, para todo $1 \leq i \leq n$. Sendo que $m_i \in C[E]$ temos $xHJ = \sum_{i=1}^{n} q_i m_i HJ \subseteq \sum_{i=1}^{n} q_i H m_i J \subseteq I$, onde HJ é um ideal não nulo de R.

Reciprocamente, suponhamos que $x \in Q[E]$ e $xH \subseteq I$, para $0 \neq H \lhd R$. Pelo Lema 3.3, podemos representar $x = \sum_{i=1}^{n} q_i m_i + y$, onde $q_i \in Q$, $m_i \in M_C(I)$, $1 \leq i \leq n$ e $y = 0$ ou y é um resto módulo I. Pela primeira parte existe $0 \neq J \lhd R$ tal que $(\sum_{i=1}^{n} q_i m_i)J \subseteq I$. Logo $y(H \cap J) \subseteq I$. Como $y = 0$ ou y é um resto módulo I isto implica que $y(H \cap J) = 0$, donde $y = 0$. $\square$

Corolário 3.5. Com as mesmas notações acima, $Q[E]M_C(I) = QM_C(I)$ é um ideal de T.

Demonstração. É claro que $QM_C(I) \subseteq Q[E]M_C(I)$ e este último membro é um ideal à esquerda de T. Se $m \in M_C(I)$ e $e \in E$, existe um ideal não nulo H de R tal que $mH \subseteq I$. Logo $meH = mHe \subseteq Ie \subseteq I$ e $emH \subseteq eI \subseteq I$. Assim, pelo Lema 3.4, $me \in QM_C(I)$ e $em \in QM_C(I)$. Daqui é fácil concluir que $QM_C(I)$ é um ideal bilateral.

Finalmente, se $m \in M_C(I)$ e $x = \sum_{i=1}^{n} q_i e_i \in T$, então $xm = \sum_{i=1}^{n} q_i m e_i \in \sum_{i=1}^{n} QM_C(I)e_i \subseteq QM_C(I)$. Conseqüentemente $Q[E]M_C(I) \subseteq QM_C(I)$. A prova está completa. $\square$

Corolário 3.6. Seja I um ideal R-disjunto de S e $I^* = QM_C(I)$. Então I^* é um ideal $(Q-)$fechado de T e $I^* \cap S = [I]$.

Demostração. Se $y \in T$ e $yJ \subseteq I^*$, para $0 \neq J \lhd Q$, temos $y(J \cap R) \subseteq I^*$, onde $0 \neq J \cap R \lhd R$. Então, pelo Lema 3.4, $y \in QM_C(I) = I^*$. Conseqüentemente, I^* é fechado em T.

Agora, as duas contenções $I^* \cap S \subseteq [I]$ e $[I] \subseteq I^* \cap S$ seguem facilmente do Lema 3.4. $\square$

Proposição 3.7. Seja I um ideal R-disjunto de S (resp. Q-disjunto de T). Então I é fechado se, e somente se, $I = QM_C(I) \cap S$ (resp. $I = QM_C(I_0)$, onde $I_0 = I \cap S$).

Demonstração. Se I é fechado em S , pelo Corolário 3.6, $I = [I] = I^* \cap S = QM_C(I) \cap S$. A recíproca é também clara do Corolário 3.6.

Seja agora I um ideal de T e seja $I_0 = I \cap S$. Então $I^* = QM_C(I_0)$ é fechado e logo se $I = QM_C(I_0)$ segue que I é fechado.

Reciprocamente, suponhamos que I é fechado. Se $m \in M_C(I_0)$, então existe $0 \neq H \lhd R$ tal que $mH \subseteq I_0$. Logo $m(QHQ) = QmHQ \subseteq QI_0Q \subseteq I$, donde $m \in I$. Conseqüentemente, $QM_C(I_0) \subseteq I$. Se existir $x \in I \setminus QM_C(I_0)$, podemos representar, de acordo com o Lema 3.3, $x = \sum_{i=1}^{n} q_i m_i + y$, onde $q_i \in Q$, $m_i \in M_C(I_0)$, $1 \leq i \leq n$, e $y \neq 0$ é um resto módulo I_0. Segue que $y \in I$ e podemos obter uma contradição facilmente. Assim $I = QM_C(I_0)$. $\square$

Dado um ideal fechado I de S, definimos a sua extensão a T por $I^* = QM_C(I)$. Então sabemos que I^* é um ideal fechado de T tal que $I^* \cap S = I$.

Corolário 3.8. A correspondência $I \leftrightarrow I^*$ acima é uma correspondência biunívoca entre os conjuntos de todos os ideais fechados de S e T, respectivamente.

Demonstração. Se A é um ideal fechado de T, então $A = QM_C(A_0)$, com $A_0 = A \cap S$, pela Proposição 3.7. Além disso, $A_0 = A \cap S = QM_C(A_0) \cap S$ é fechado também por 3.7. Logo a correspondência relaciona fechados com fechados.

Para completar a prova basta ver que se A e B são dois ideais fechados de T tais que $A \cap S = B \cap S$, então $A = B$. Mas isto também segue facilmente da Proposição 3.7, pois $A = QM_C(A \cap S) = QM_C(B \cap S) = B$. $\square$

Estamos agora em condições de provar o primeiro teorema central deste parágrafo.

Teorema 3.9. Existe uma correspondência biunívoca entre os seguintes conjuntos:

(i) O conjunto de todos os ideais fechados de S.

(ii) O conjunto de todos os ideais fechados de T.

(iii) O conjunto de todos os ideais de V.

Além disso, esta correspondência associa o ideal fechado I de S com o ideal fechado I^* de T e o ideal K de V se $I^* \cap S = I$ e $I^* \cap V = K$ (equivalentemente $I^* = TK$).

Demonstração. A correspondência entre (i) e (ii) já foi estabelecida no Corolário 3.8.

Se I^* é um ideal fechado de T, então $I^* \cap V$ é um ideal de V, univocamente determinado por I^*. Reciprocamente, seja K um ideal de V e seja $I^* = QK$ a extensão de K a T (é claro que $QK = TK$ é um ideal de T). Então $QK \cap V \supseteq K$ e vamos provar que $QK \cap V = K$.

Suponha que $QK \cap V \supset K$ e seja Ω uma base de K sobre C. Pelo Lema 3.1, Ω é um subconjunto de elementos de T, o qual é Q-linearmente independente. Seja $v \in QK \cap V$ um elemento que não está em K. Então $\Omega' = \Omega \cup \{v\}$ é ainda C-independente, e logo é Q-independente em T. Além disso, $v = \sum_{i=1}^{n} q_i k_i$, $q_i \in Q$, $k_i \in K$. Escrevendo os elementos k_i como combinação linear dos elementos de Ω, obtemos que v está no Q-submódulo de T gerado por Ω. Isto contradiz o fato que Ω' e Q-independente. Assim $QK \cap V = K$.

Para completar a prova basta ver que QK é fechado em T. Seja $K_0 = QK \cap S$ e seja Ω uma base de K sobre C. Então é claro que Ω é uma Q-base de QK. Se $m \in M_C(K_0)$, então existe $0 \neq H \lhd R$ tal que $mH \subseteq K_0 \subseteq QK$. Seja $h \in H$ tal que $mh \neq 0$, e sejam $q_i \in Q$, $v_i \in \Omega$, $i = 1, ..., n$ tais que $mh = \sum_{i=1}^{n} q_i v_i$. Ou seja $\{m\} \cup \Omega$ é um conjunto Q-dependente em T. Segue que $M_C(K_0) \subseteq K$, pois se $M_C(K_0) \nsubseteq K$ podemos escolher $m \in M_C(K_0)$ tal que $\{m\} \cup \Omega$ seja C-independente. Assim $QK \subseteq [QK] = QM_C(K_0) \subseteq QK$, e conseqüentemente, QK é fechado. A prova está completa. $\square$

Agora estamos em condições de provar que a correspondência do Teorema 3.9 é uma correspondência biunívoca entre ideais primos.

Teorema 3.10. A correspondência do Teorema 3.9 é uma correspondência biunívoca entre os seguintes conjuntos:
(i) O conjunto de todos os ideais primos R-disjuntos de S.
(ii) O conjunto de todos os ideais primos Q-disjuntos de T.
(i) O conjunto de todos os ideais primos de V.

Demonstração. Seja I um ideal fechado de S, I^* a extensão de I a T e $I_0 = I^* \cap V$. Devemos provar que se um destes ideais é primo, os outros são também primos. Completamos a prova provando três implicações:

1) I primo $\rightarrow$ I^* primo.

Sejam A e B ideais de T tais que $A \supseteq I^*$, $B \supseteq I^*$ e $AB \subseteq I^*$. Vejamos primeiro que podemos supor que A e B são fechados. De fato, se $x \in [A]$ e $y \in [B]$, existem ideais $0 \neq H \lhd Q$ e $0 \neq J \lhd Q$ com $Hx \subseteq A$ e $yJ \subseteq B$. Assim $HxyJ \subseteq AB \subseteq I^*$. Segue que $xy \in I^*$ pois I^* é fechado. Conseqüentemente, $[A][B] \subseteq I^*$.

Suponhamos então que A e B são fechados. Temos $(A \cap S)(B \cap S) \subseteq I^* \cap S = I$. Logo $(A \cap S) \subseteq I$ ou $B \cap S \subseteq I$. Mas $A \cap S \supseteq I^* \cap S = I$ e $B \cap S \supseteq I$. Assim $A \cap S = I$ ou $B \cap S = I$ e, pela correspondência biunívoca do Teorema 3.9, segue que $A = I^*$ ou $B = I^*$.

2) I^* primo $\rightarrow$ I_0 primo.

Se A e B são ideais de V tais que $AB \subseteq I_0$, segue que $(QA)(QB) = QAB \subseteq QI_0 = I^*$. Logo $QA \subseteq I^*$ ou $QB \subseteq I^*$. Assim $A = QA \cap V \subseteq I^* \cap V = I_0$ ou $B = QB \cap V \subseteq I^* \cap V = I_0$.

3) I_0 primo $\rightarrow$ I primo.

Sejam A e B ideais de S tais que $A \supseteq I$, $B \supseteq I$ e $AB \subseteq I$. Como na parte 1), podemos supor que A e B são fechados. Assim $A = QM_C(A) \cap S$ e $B = QM_C(B) \cap S$. Se $x \in M_C(A)$ e $y \in M_C(B)$, existem ideais $H \neq 0$, $J \neq 0$ de R tais que $xH \subseteq A$ e $yJ \subseteq B$. Assim $xyQHJQ = QxHyJQ \subseteq QABQ \subseteq QIQ \subseteq I^*$. Como I^* é fechado segue que $xy \in I^* \cap V = I_0$.

Assim $VM_C(A)VM_C(B) \subseteq V(M_C(A)M_C(B)) \subseteq I_0$. Logo $VM_C(A) \subseteq I_0$ ou $VM_C(B) \subseteq I_0$. Conseqüentemente, $A = QM_C(A) \cap S \subseteq QI_0 \cap S = I$ ou $B = QM_C(B) \cap S = QI_0 \cap S = I$. A prova está completa. $\square$

Observação: Se $S = R[t]$ é um anel de polinômios sobre o anel primo R, os ideais fechados e primos R-disjuntos de S foram estudados em [F_3]. Os resultados obtidos foram os precursores dos aqui apresentados. Mas existem algumas particularidades específicas para anéis de polinômios. Por exemplo, o conjunto $M_C(I)$ definido neste parágrafo pode reduzir-se a um único polinômio mônico $f_\circ \in C[t]$. Assim, se I é um ideal R-disjunto, $[I] = Q[t]f_\circ \cap R[t]$. Logo, I é fechado se, e somente se, $I = Q[t]f_\circ \cap R[t]$, para algum polinômio mônico $f_\circ \in C[t]$. Finalmente, o ideal fechado $I = Q[t]f_\circ \cap R[t]$ é primo se, e somente se, $f_\circ$ é irredutível em $C[t]$.

§4. CASO GERAL

Seja agora $S = R[X]$ uma extensão centralizante (não necessariamente livre) do anel primo R. O propósito desta secção é estender os resultados da secção anterior.

A definição de fecho de um ideal R-disjunto de S é a mesma dada no §2. Ou seja, se I é um ideal R-disjunto de S, então definimos

$$[I] = \{x \in S : \text{ existe } 0 \neq H \lhd R \text{ tal que } xH \subseteq I\}.$$

É claro que $[I]$ é um ideal R-disjunto de S. O ideal I é dito fechado se $[I] = I$.

Como no §2, provamos facilmente que todo ideal primo R-disjunto de S é fechado.

Vamos precisar também do seguinte

Lema 4.1. Sejam S e S' duas extensões centralizantes do anel primo R e seja $\varphi : S' \to S$ um homomorfismo sobrejetor de anéis tal que $\varphi(r) = r$, para todo $r \in R$. Se I é um ideal R-disjunto de S, então $[\varphi^{-1}(I)] = \varphi^{-1}([I])$.

Demonstração. Se $x \in [\varphi^{-1}(I)]$, existe $0 \neq H \lhd R$ tal que $xH \subseteq \varphi^{-1}(I)$. Então, para cada $a \in H$, $\varphi(xa) = \varphi(x)a \in I$. Assim $\varphi(x)H \subseteq I$ e segue que $\varphi(x) \in [I]$. Conseqüentemente, $x \in \varphi^{-1}([I])$. A contenção contrária $\varphi^{-1}([I]) \subseteq [\varphi^{-1}(I)]$ é semelhante. $\square$

Sejam $\varphi : S' \to S$ como acima. Então é conhecido que existe uma correspondência biunívoca entre os ideais de S e os ideais de S' que contêm $Ker\varphi$. Como φ é um R-homomorfismo, é fácil ver que esta correspondência respeita ideais R-disjuntos, i. e., um ideal I de S é R-disjunto se, e somente se, $\varphi^{-1}(I)$ é R-disjunto.

Do Lema 4.1 temos o seguinte

Corolário 4.2. Sejam $\varphi : S' \to S$ como acima. Então a correspondência biunívoca canônica estabelece uma correspondência biunívoca entre os ideais fechados (resp. primos R-disjuntos) de S e os ideais fechados (resp. primos R-disjuntos) de S' que contém $Ker\varphi$.

Demonstração. A primeira parte segue diretamente do Lema 4.1. Para a segunda basta observar que se P é um ideal R-disjunto de S, então a aplicação natural $S' \xrightarrow{\varphi} S \xrightarrow{\pi} S/P$, onde π é a projeção canônica, é um epimorfismo com núcleo $\varphi^{-1}(P)$. Logo $S'/\varphi^{-1}(P) \simeq S/P$ e segue que P é primo se, e somente se, $\varphi^{-1}(P)$ é primo. $\square$

Seja $X = (x_i)_{i\in\Gamma}$. Para cada $i \in \Gamma$, seja t_i uma indeterminada e denotemos por S' o anel de polinômios sobre R nas indeterminadas (que não necessariamente comutam entre si) $(t_i)_{i\in\Gamma}$, onde $rt_i = t_i r$, para todo $r \in R$, $i \in \Gamma$.

A aplicação $\varphi : S' \to S$ definida por $\varphi(t_i) = x_i$, para todo $i \in \Gamma$, e $\varphi(r) = r$, para $r \in R$, é um homomorfismo sobrejetor. Assim $S \simeq S'/Ker\varphi$ e existe uma correspondência biunívoca entre os ideais (resp. ideais R-disjuntos, fechados, primos R-disjuntos) de S e de S' que contém $Ker\varphi$. Esta correspondência associa um ideal I de S com o ideal $\varphi^{-1}(I)$ de S'.

Na secção 3 provamos um teorema de correspondência biunívoca entre ideais fechados e ideais primos disjuntos de $S = R[E]$, $T = Q[E]$ e $V = C[E]$. Os anéis T e V foram naturalmente definidos como objetos canônicos associados a S, naquele caso. Vamos definir agora estes objetos para as extensões não necessariamente livres que estamos considerando neste parágrafo.

Seja $T' = Q[t_i]_{i\in\Gamma}$ a extensão canônica associada a S', definida como no §3. É fácil ver que T' é o anel de polinômios sobre Q nas indeterminadas $(t_i)_{i\in\Gamma}$. Analogamente, $V' = C[t_i]_{i\in\Gamma}$. Pelos resultados da secção anterior sabemos que existem correspondências biunívocas entre ideais fechados e ideais primos de S', T' e V', respectivamente.

O ideal $[0]_S$ é um ideal fechado de S. Então $J = \varphi^{-1}([0]_S)$ é um ideal fechado de S' e segue que existe um ideal (Q-disjunto) fechado J^* de T' tal que $J^* \cap S' = J$. Além disso, $J_0 = J^* \cap V'$ é um ideal de V' e $J^* = QJ_0$.

Definimos a "extensão canônica" de S por $T = T'/J^*$. É claro que T é uma extensão centralizante livre de Q com geradores centralizantes $(e_j + J^*)_j$, onde e_j é um produto qualquer das indeterminadas $(t_i)_{i\in\Gamma}$.

Vamos definir uma aplicação canônica $j : S \to T$. Para isso denotamos por $\pi : T' \to T$ a projeção canônica e por $i : S' \to T'$ a inclusão natural.

Se $x \in S$, existe $y \in S'$ tal que $\varphi(y) = x$. Então $\pi_\circ i(y) \in T$ e definimos $j(x) = \pi_\circ i(y)$. Note que se $x = 0$, então $y \in J$. Logo $i(y) \in J^*$ e segue que $\pi_\circ i(y) = 0$. Assim $j : S \to T$ é uma aplicação bem definida. É fácil verificar que j é um homomorfismo de anéis tal que $j(r) = r$, para todo $r \in R$, e que $j(x_i) = t_i + I^*$, para todo $i \in \Gamma$.

O anel T definido acima é, por definição, a "extensão canônica" de S a uma extensão centralizante de Q. Note porém, que $j : S \to T$ não é uma injeção. De fato, é fácil verificar que $Ker\ j = [0]_S$ pela definição de J. Isto não deverá ser um obstáculo para que a correspondência biunívoca procurada seja estabelecida, sendo que todo ideal fechado de S contém $[0]_S$, como é fácil verificar.

Para completar a preparação do cenário definimos a C-álgebra associada por $V = V'/I_0$. É fácil ver que $V = C[e_j + I_0]_j$, onde e_j é como acima um produto qualquer das indeterminadas $(t_i)_{i\in\Gamma}$, e que $V \subseteq T$.

Usando as correspondências provadas no §3 é fácil obter os seguintes teoremas.

Teorema 4.3. Seja S uma extensão centralizante do anel primo R e sejam T e V como acima. Então existe uma correspondência biunívoca entre os seguintes conjuntos

(i) O conjunto de todos os ideais fechados de S.

(ii) O conjunto de todos os ideais fechados de T.

(iii) O conjunto de todos os ideais de V.

Mais ainda, esta correspondência associa o ideal fechado I de S com o ideal fechado de I^* de T e o ideal K de V, se $j^{-1}(I^*) = I$ e $I^* \cap V = K$ (ou equivalentemente $I^* = QK$).

Demonstração. É suficiente aplicar o Teorema 3.10 e a correspondência biunívoca do Corolário 4.2 para as aplicações do diagrama seguinte:

$$\begin{array}{ccc} S' & \xrightarrow{\varphi} & S \\ \downarrow i & & \downarrow j \\ T' & \xrightarrow{\pi} & T \\ \uparrow & & \uparrow \\ V' & \xrightarrow{\pi/V'} & V \end{array}$$

(note que φ, π e π/V' são sobrejetoras). $\square$

Teorema 4.4. A correspondência do Teorema 4.3 é uma correspondência biunívoca entre os seguintes conjuntos.

(i) O conjunto de todos os ideais primos R-disjuntos de S.

(ii) O conjunto de todos os ideais primos Q-disjuntos de T.

(iii) O conjunto de todos os ideais primos de V.

Demonstração. Sejam $P \lhd S$, $P^* \lhd T$ e $P_0 = P^* \cap V \lhd V$ ideais fechados correspondentes. Como as aplicações horizontais do diagrama acima são sobrejetoras, P é primo de S se, e somente se, $\varphi^{-1}(P)$ é primo de S', P^* é primo de

T se, e somente se, $\pi^{-1}(P^*)$ é primo de T' e P_0 é primo de V se, e somente se, $\pi^{-1}(P_0)$ é primo de V'. Logo o resultado segue do Teorema 3.11.

§5. APLICAÇÕES

Vários resultados podem ser obtidos como aplicação das secções anteriores. Nesta secção veremos apenas alguns deles, pois não queremos nos estender muito. O leitor interessado pode consultar a bibliografia para outras aplicações.

No que segue, $S = R[X]$ é sempre uma extensão centralizante do anel R (não necessariamente primo) sendo X um sistema de geradores centralizantes.

A primeira clase de resultados responde as questões do tipo seguinte: seja P um ideal primo de S e seja $P' = P \cap R$ um ideal primo de R. Será que P é de um determinado tipo (por exemplo, fortemente primo, primo não singular, primitivo, etc) se, e somente se, P' é do mesmo tipo?

A segunda classe de resultados que queremos mencionar aqui estuda o seguinte problema: suponha que R é primo, que P é um ideal primo de S e que $P \cap R = 0$. Usando a mesma notação da secção anterior, seja P_0 o correspondente ideal primo de V, isto é, único ideal primo de V tal que $P = j^{-1}(QP_0)$. Será que P é de um determinado tipo especial se, e somente se, P_0 é do mesmo tipo? Quando isto acontecer, o correspondente radical de S definido por esta classe de ideais primos poderá ser determinado via o correspondente radical de V. E isto é muito bom, pois sendo V uma álgebra sobre um corpo, é natural esperar que os seus radicais sejam mais fáceis de calcular que os radicais de S.

Se P é um ideal primo de S, então, como antes, para estudar S/P podemos passar a estudar $\bar{P} = P/(P \cap R)S$, que é um ideal primo de $\bar{S} = S/(P \cap R)S$, sendo $\bar{S}$ uma extensão centralizante de $\bar{R}$. Este ideal é $\bar{R}$-disjunto: $\bar{P} \cap \bar{R} = 0$. Estamos assim no caso estudado nas secções anteriores.

Note que se P' é um ideal primo de R e P é um ideal de S, maximal com respeito à propriedade $P \cap R = P'$, então P é primo, como é fácil verificar.

Vamos começar pelo seguinte

Teorema 5.1. Seja P' um ideal primo de R e seja P um ideal de S que é maximal com respeito à propriedade $P \cap R = P'$. Então P' é fortemente primo (resp. não singular) se, e somente se, P é fortemente primo (resp. não singular).

Demonstração. Pela observação acima podemos supor que $P' = 0$, então R é primo e P é R-disjunto. O teorema ficará provado pelos dois lemas seguintes. □

Lema 5.2. Seja S uma extensão centralizante do anel primo R e seja P um ideal primo de S tal que $P \cap R = 0$. Se P é fortemente primo (resp. não singular), então R é fortemente primo (resp. não singular).

Demonstração. Vamos provar somente o primeiro caso, deixando o outro para o leitor.

Suponhamos, então, que P é fortemente primo e seja I um ideal não nulo de R. O conjunto $I[X]$ de todos os elementos $x = \sum_{i=1}^{n} a_i x_i$, $a_i \in I$, $x_i \in X$, $i = 1, ..., n$, é um ideal de S. Como $I[X] \cap R \neq 0$, $I[X] \nsubseteq P$. Logo existe um subconjunto finito $F \subseteq I[X]$ tal que $Fy \subseteq P$, $y \in S$, implica $y \in P$.

Seja $F = \{z_1, ..., z_m\}$, $z_i = \sum_j a_{ij} x_j$, $a_{ij} \in I$. Então consideramos o subconjunto finito $F_0 = \{a_{ij}\} \subseteq I$. Se $F_0 a = 0$, $a \in R$, segue que $z_i a = 0$ para todo $1 \leq i \leq m$. Assim $Fa = 0 \subseteq P$ e, conseqüentemente, $a \in P \cap R = 0$. Assim F_0 é um isolador de R contido em I, donde R é fortemente primo. $\square$

Lema 5.3. Seja S uma extensão centralizante do anel primo R e seja P um ideal de S que é maximal com respeito à propriedade $P \cap R = 0$. Se R é fortemente primo (resp. primo não singular), então P é também fortemente primo (resp. primo não singular).

Demonstração. Como no Lema anterior, vamos provar somente um caso. Escolhemos agora o segundo. Logo, vamos supor que R é primo não singular e vamos provar que P é não singular.

Pela secção 4 basta provar o resultado quando $S = R[E]$ é uma extensão centralizante livre de R. Suponhamos então que este é o caso e, por absurdo, vamos supor que o ideal singular $Z(S/P) \neq 0$. Então existe um ideal não nulo I de S tal que $Z(S/P) = I/P$, onde $I \supset P$. Pela maximalidade de P, $I \cap R \neq 0$ e tomemos $0 \neq a \in I \cap R$. Assim o anulador $An_r(a + P)$ é um ideal essencial à direita de R/P.

Sejam J um ideal à direita não nulo de R e $J[E]$ o ideal à direita de S gerado por J. Como $(J[E] + P)/P \neq 0$, existe um elemento $x = \sum_{i=1}^{n} a_i e_i$, $a_i \in J$, para $1 \leq i \leq n$, tal que $x \notin P$ e $ax \in P$. Podemos escolher um tal elemento x com suporte minimal.

Se x é um resto módulo P, segue que $ax = 0$. Assim $aa_i = 0$, para $1 \leq i \leq n$ e portanto $An_r(a) \cap J \neq 0$.

Se x não é um resto módulo P procedemos como segue. Sejam P^* e $P_0 = P^* \cap V$ os ideais primos associados a P em $Q[E]$ e $V = C[E]$, respectivamente. Seja $0 \neq y \in P$ tal que $\sup(y) = \{e_1, e_2, ..., e_t\} \subseteq \sup(x)$, $t \leq n$, e suponhamos y de suporte minimal em P. Então existe $m = e_1 + e_2 c_2 + ... + e_t c_t \in M_C(P) \subseteq P^*$, tal que $y = y(e_1)m$. Seja $0 \neq H \lhd R$ tal que $mH \subseteq P$. Para cada $h \in H$, $z_h = xh - a_1 mh \in S$ e $\sup(z_h) \subseteq \{e_1, ... e_n\}$. Além disso, $az_h = axh - aa_1 mh \in P^* \cap S = P$. Também podemos escolher $h \in H$ tal que $z_h \notin P$. De fato, se $z_h \in P$, para todo $h \in H$, segue da relação acima que $xH \subseteq P$ e logo $x \in P$, uma contradição.

Conseqüentemente, para algum $h \in H$, $\sup(z_h) \subset \sup(x)$, $z_h \notin P$ e $az_h \in P$. Isto é ainda uma contradição, pela minimalidade de $\sup(x)$. A prova está completa. $\square$

Os dois lemas anteriores provam o Teorema 5.1. Além disso, o Lema 5.2 tem como conseqüência evidente o seguinte

Corolário 5.4. Seja P um ideal fortemente primo (resp. primo não singular) de S. Então $P \cap R$ é um ideal fortemente primo (resp. primo não singular) de R.

A recíproca do Corolário anterior vale sob certa condição adicional. Existe um exemplo na literatura provando que não vale sempre, para o caso fortemente primo [FJP].

Teorema 5.5. Seja P um ideal primo de S tal que $P \cap R$ é fortemente primo (resp. primo não singular). Suponha que o sistema de geradores X é finito ou que seus elementos comutam entre si. Então P é também fortemente primo (resp. primo não singular).

Demonstração. Vamos provar o caso fortemente primo. Como antes, podemos supor que $P \cap R = 0$, i. e., R é fortemente primo. Além disso, podemos supor que $S = R[E]$ é uma extensão centralizante livre de R, onde E é uma base finita ou cujos elementos comutam entre si.

Seja $I \supset P$ um ideal de S. Vamos provar que I contém um isolador módulo P. Como P é fechado, existe um elemento de suporte minimal $x \in I$ que é um resto módulo P (caso contrário $Min(I) = Min(P)$). Seja $x = a_1e_1 + ... + a_ne_n$. Sabemos que existe $m = e_1 + c_2e_2 + ... + c_ne_n \in M_C(I)$ tal que $my(e_1) = y$, para todo $y \in I$ com $\sup(y) = \sup(x)$ (note que se $I \cap R \neq 0$, então x pode ser escolhido em $I \cap R$ e então $m = 1$).

Seja $J = \{b \in R$: existe $y \in I$ com $\sup(y) \subseteq \sup(x)$ e $y(e_1) = b\}$. Então J é um ideal não nulo de R e, conseqüentemente, existe um subconjunto finito $F = \{b_1, b_2, ..., b_t\} \subset J$ tal que $Fa = 0$, $a \in R$, implica $a = 0$.

Para cada $1 \leq i \leq t$, seja $y_i = b_ie_1 + a_{i2}e_2 + ... + a_{in}e_n \in I$, onde $y_i(e_1) = b_i$. Então $y_i = mb_i$, para $1 \leq i \leq t$. Nosso objetivo é encontrar um isolador em S módulo P que esteja contido em I. Vamos considerar dois casos:

Caso 1. Se os elementos de E comutam entre si, é suficiente tomar como isolador $\{y_i\}_{1 \leq i \leq t}$.

De fato, seja $z \in S$ tal que $y_iz \in P$, para todo $i = 1, ..., t$. Pelos resultados do §3, podemos escrever $z = \sum_{j=1}^{l} q_jm_j + v$, onde $m_j \in M_C(P)$, $q_j \in Q$, $1 \leq j \leq l$ e $v = 0$ ou v é um resto módulo P. Se $v = 0$, então $z \in P^* \cap S = P$ e a prova está completa.

Suponha $v \neq 0$. Sendo que $y_iz \in P$ segue que $y_iv \in P^*$, $1 \leq i \leq t$, pois

$\sum_{j=0}^{n} q_j m_j \in P^*$. Assim $mb_iv \in P^*$ e como os elementos de E comutam entre si segue que $mQ[E]b_iv = Q[E]mb_iv \subseteq P^*$. Como P^* é primo e m é um resto módulo P^*, obtemos $b_iv \in P^*$, para $1 \leq i \leq t$. Seja H um ideal não nulo de R tal que $vH \subseteq S$. Segue que $b_ivH \subseteq P^* \cap S = P$. Mas $\sup(b_ivh) \subseteq \sup(v)$, para $h \in H$, e v é um resto módulo P^*. Assim $b_ivH = 0$. Como $R[E]$ é livre sobre R e $F = \{b_1, ..., b_t\}$ é um isolador em R, a última relação implica facilmente que $v = 0$. A contradição completa a prova deste caso.

Caso 2. Se E é finito, então basta tomar $\{y_ie\}_{1 \leq i \leq t, e \in E}$.

De fato, seja $z \in S$ com $y_iez \in P$, para todo $1 \leq i \leq t$, $e \in E$. Como antes, segue que $z = \sum_{j=1}^{l} q_j m_j + v$, onde podemos supor que $v \neq 0$ é um resto módulo P.

Ainda como acima, $mb_iev \in P^*$, para $1 \leq i \leq t$, $e \in E$. Assim $mQ[E]b_iv \subseteq P^*$. Segue que $b_iv \in P^*$ e a prova pode ser completada como no Caso 1. □

Para terminar esta mostra de aplicações dos métodos desenvolvidos aqui, vamos mencionar brevemente a seguinte proposição e suas conseqüências. A prova da proposição será omitida (ver [F_6] e Proposição 1.21 de [FPu]).

Proposição 5.6. Sejam R um anel primitivo, $S = R[X]$ uma extensão centralizante de R, P um ideal primo R-disjunto de S e P_0 o correspondente ideal de V. Se P_0 é primitivo, então P é primitivo.

O radical de Jacobson de um anel A será denotado por $J(A)$. Dizemos que A é um anel (Jacobson) semisimples se $J(A) = 0$.

Corolário 5.7. Sejam R um anel primitivo e $S = R[X]$ uma extensão centralizante de R. Então $J(S) \subseteq j^{-1}(QJ(V))$, onde $j : S \to T$ é a aplicação canônica. Em particular, se S é livre sobre R, então $J(S) \subseteq QJ(V) \cap S$.

Demonstração. Como $J(S)$ é a intersecção de todos os ideais primitivos, pela Proposição 5.6 segue que $J(S) \subseteq j^{-1}(QP_0)$, para todo ideal primitivo P_0 de V. Logo $J(S) \subseteq \cap j^{-1}(QP_0) = j^{-1}(Q(\cap P_0)) = j^{-1}(QJ(V))$. □

Corolário 5.8. Sejam R um anel semisimples e $S = R[E]$ uma extensão centralizante livre de R. Suponha que $C[E]$ é um anel semisimples, para todo corpo C que é o centróide extendido de um fator primitivo de R. Então S é um anel semisimples.

Demonstração. Por hipótese, existe uma família de ideais primitivos $(P_i)_{i \in L}$ de R tais que $\bigcap_{i \in L} P_i = 0$. Então o anel $\bar{R}_i = R/P_i$ é um anel primitivo e

$\bar{S}_i = S/P_i[E] \simeq \bar{R}[E]$ é uma extensão centralizante livre do anel primitivo $\bar{R}$. Pela hipótese, $J(\bar{C}[E]) = 0$, onde $\bar{C}$ é o centróide extendido de $\bar{R}$. Assim $J(\bar{S}_i) = QJ(\bar{C}[E]) \cap \bar{R}[E] = 0$, e segue que o ideal nulo de $J(\bar{S}_i)$ é intersecção de ideais primitivos de $\bar{S}_i$. Então, pela correspondência biunívoca entre ideais de $\bar{S}_i$ e ideais de S que contém $P_i[E]$, segue que $P_i[E]$ é uma intersecção de ideais primitivos de S. Como $\bigcap_i P_i[E] = 0$ resulta que $J(S) = 0$. $\square$

Em [FPu], resultados do tipo 5.6, 5.7 e 5.8 são obtidos para várias outras propriedades radicais tais como o radical fortemente primo, o radical singular, o radical de Brown-McCoy e o nilradical superior.

§6. COMENTÁRIOS FINAIS

Os resultados expostos nestas notas são mais gerais. Em [F$_5$] estudamos o caso de um bimódulo sobre um anel primo, definindo os submódulos fechados e se provando resultados que correspondem aos apresentados aqui para ideais fechados. Os resultados para ideais primos de extensões centralizantes são obtidos como caso particular.

Na verdade, em [F$_5$], estudamos não somente ideais primos de extensões centralizantes, mas também de extensões intermediárias. Uma extensão intermediária W de R é definida como sendo qualquer anel tal que $R \subseteq W \subseteq S$, onde S é uma extensão centralizante de R. Muitos dos resultados aqui apresentados são obtidos para ideais de um anel intermediário.

Aplicações à teoria de módulos são obtidos também em [F$_5$]. Submódulos não singulares e fortemente fechados são estudados de modo semelhante aos obtidos aqui para ideais primos não singulares e fortemente primos.

Queremos mencionar também que em [FPu] são aplicados os mesmos métodos apresentados aqui para estudar ideais primos e radicais de produtos tensoriais $A \otimes_D B$, onde A e B são álgebras sobre um anel comutativo D.

Não seria justo terminar estas notas sem mencionar os excelentes trabalhos de Robson-Small e Robson sobre ideais primos em extensões centralizantes finitas ([RS], [R$_1$]). Estes trabalhos são bem anteriores aos meus e poderiam ser considerados precursores dos mesmos. Neles são estudadas as questões já mencionadas de “lying over”, incomparabilidade, “going up” e “going down”. A maioria destas questões tem resposta afirmativa para extensões centralizantes finitas, generalizando os resultados conhecidos na Álgebra Comutativa para extensões inteiras.

Finalmente, uma continuação natural desta linha de pesquisa é o estudo dos ideais primos em extensões normalizantes. Uma extensão $S \supseteq R$ é dita uma extensão normalizante de R se existir um sistema de geradores $(x_i)_{i \in L}$ de S como R-módulo, tal que $Rx_i = x_i R$, para todo $i \in L$. As extensões normalizantes finitas, i. e., onde L é finito, têm sido também exaustivamente estudadas, mas quase nada foi feito ainda no caso geral. O estudo deste caso é um dos próximos desafios nesta área.

BIBLIOGRAFIA

[A] S. A. Amitsur, Radicals of polynomial rings, Canad. J. Math 8 (1956), 355- 361.

[AM] M. F. Atiyah and I G. Macdonald, Introduction to Commutative Algebra, Addison - Wesley (1969), New York.

[B_1] A. D. Bell, When are all prime ideals in an Ore extension Goldie?, Comm. Algebra 13 (8) (1985), 1743-1762.

[B_2] G. Bergman, Homogeneous elements and prime ideals in $\mathbf{Z}$-graded rings, preprint.

[BR] S. S. Bedi and J. Ram, Jacobson radical of skew polynomial rings and skew group rings, Israel J. Math. 35 (1980), 327-338.

[CCG] R. Carbajo, E. Cisneros and M. I. González, The prime radical of a skew group ring, Rev. Unión Mat. Argent. 32 (1985), 87-92.

[CFG] E. Cisneros, M. Ferrero and M. I. González, Prime ideals of skew polynomial rings and skew Laurent polynomial rings, Math. J. Okayama Univ. 32 (1990), 61-72.

[Ch] W. Chin, Prime ideals in differential operator rings and crossed products of infinite groups, J. Algebra 106 (1987), 78-104.

[D] N. J. Divinsky, "Rings and Radicals", Math. Exp. 14, Univ. of Toronto Press (1965), Toronto.

[F_1] M. Ferrero, Radicals of skew polynomial rings and skew Laurent polynomial rings, Math. J. Okayama Univ. 29 (1987), 119-126.

[F_2] M. Ferrero, The strongly prime radical of an Ore extension, Comm. Algebra 17 (2) (1989), 351-376.

[F_3] M. Ferrero, Prime and principal closed ideals in polynomial rings, J. Algebra 134 (1990), 45-59.

[F_4] M. Ferrero, Closed and prime ideals in free centred extensions, J. Algebra, 148 (1992), 1-16.

[F_5] M. Ferrero, Centred bimodules over prime rings: closed submodules and applications to ring extensions, J. Algebra, a aparecer.

[F_6] M. Ferrero, Semisimplicity of free centred extensions, Canad. Math. Bull, a aparecer.

[FCG] M. Ferrero, E. Cisneros and M. I. González, Ore extensions and Jacobson rings, Comm. Algebra 21 (11) (1993), 3963-3976.

[FJP] M. Ferrero, E. Jespers and E. Puczyłowski, Prime ideals of graded rings and related matters, Comm. Algebra 18 (11) (1990), 3819-3834.

[FK] M. Ferrero and K. Kishimoto, On differential rings and skew polynomials, Comm. Algebra 13 (2) (1985), 285-304.

[FKM] M. Ferrero, K. Kishimoto and K. Motose, On radicals of skew polynomial rings of derivation type, J. London Math. Soc. (2) 28 (1983), 8-16.

[FM] M. Ferrero and J. Matczuk, Prime ideals in skew polynomial rings of derivation type, Comm. Algebra 18 (3) (1990), 689-710.

[FPa] M. Ferrero and M. M. Parmenter, A note on Jacobson rings and polynomial rings, Proc. Amer. Math. Soc. 104, n$\underline{o}$ 4 (1989), 281-286.

[FPu] M. Ferrero and E. Puczyłowski, Prime ideals and radicals of centred extensions and tensor products, a aparecer.

[G] K. R. Goodearl, Ring theory, nonsingular rings and modules, Marcel Dekker, (1976), New York.

[GM] A. W. Goldie and G. Michler, Ore extensions and polyciclic group rings, J. London Math. Soc. (2), 9 (1974), 337-345.

[GW] K. R. Goodearl and R. B. Warfield Jr., Primitivity in differential operator rigs, Math Z. 180 (1982), 503-523.

[HL] D. Handelman and J. Lawrence, Strongly prime rings, Trans. Amer. Math. Soc. 211 (1975), 209-223.

[HR_1] A. G. Heinicke and J. C. Robson, Normalizing extensions: Prime ideals and incomparability, J. Algebra 72 (1981), 237-268.

[HR_2] A. G. Heinicke and J. C. Robson, Normalizing extensions: nilpotency, J. Algebra 76 (1982), 459-470.

[HR_3] A. G. Heinicke and J. C. Robson, Intermediate normalizing extensions, Trans. Amer. Math. Soc. 282 (1984), 645-667.

[J_1] D. A. Jordan, Noetherian Ore extensions and Jacobson rings, J. London Math. Soc. (2), 10 (1975), 281-291.

[J_2] D. A. Jordan, Primitive Ore extensions, Glasgow Math. J. 18 (1977), 93-97.

[K] I. Kaplansky, Commutative rings, The University of Chicago Press, (1974), Chicago.

[KO] K. Krempa and J. Okninski, Group rings which are Jacobson rings, Archiv Math. 44 (1985), 20-25.

[L] J. Lambek, Lectures on rings and modules, Chelsea Pu. Co, New York (1976).

[LP_1] M. Lorenz and D. S. Passman, Centers and prime ideals in group algebras of polycyclic-by-finite groups, J. Algebra 57 (1979), 355-386.

[LP_2] M. Lorenz and D. S. Passman, Prime ideals in crossed products of finite groups, Israel J. Math. 33 (1979), 89-132.

[LP_3] M. Lorenz and D. S. Passman, Prime ideals in group algebras of polycyclic-by-finite groups, Proc. London Math. Soc. 43 (1981), 520-543.

[Ma_1] Manuel Malásquez, Prime ideals in crossed products of abelian groups, Comm. Algebra 22 (5) (1994), 1861-1876.

[Ma_2] W. S. Martindale, Prime rings satisfying a generalized polynomial identity, J. Algebra 12 (1969), 576-584.

[Mc] N. H. McCoy, The theory of rings, MacMillan Co, New York.

[Mo_1] S. Montgomery, Fixed rings of finite automorphism groups of associative rings, Lectures Notes in Math. 818, Springer Verlag (1980). Berlin.

[Mo_2] S. Montgomery, Prime ideals in fixed rings, Comm. Algebra 9 (1981), 423-449.

[Mo_3] S. Montgomery, Prime ideals and group actions in non-commutative algebras, Contemp. Math. Vol 88 (1989), 103-124.

[MP_1] S. Montgomery and D. S. Passman, Crossed products over prime rings, Israel J. Math 31 (1978), 224-256.

[MP_2] S. Montgomery and D. S. Passman, Prime ideals in fixed rings of free algebras, Comm. Algebra 15 (1987), 2209-2234.

[MS] S. Montgomery and L. S. Small, Integrality and prime ideals in fixed rings of PI rings, J. Pure Appl. Algebra 31 (1984), 185-190.

[NO] C. Nastasescu and F. Van Oystaeyen, The strongly prime radical of graded rings, Bull. Soc. Math. Belgique, Ser. B 36 (1984), 243-251.

[P_1] D. S. Passman, Prime ideals in normalizing extensions, J. Algebra 73 (1981), 556-572.

[P_2] D. S. Passman, Semiprime and prime crossed productcs, J. Algebra 83 (1983), 158-178.

[P_3] D. S. Passman, Prime ideals in enveloping rings, Trans. Amer. Math. Soc. 302 (1987), 535-560.

[P_4] D. S. Passman, Prime ideals in polycyclic crossed products, Trans. Amer. Math. Soc. 301 (1987), 737-759.

[P_5] D. S. Passman, Prime ideals in restricted enveloping rings, Comm. Algebra 16 (1988), 1411-1436.

[PPS] M. M. Parmenter, D. S. Passman and P. N. Stewart, The strongly prime radical of crossed products, Comm. Algebra 12 (9) (1984), 1099-1113.

[PS] K. R. Pearson and W. Stephenson, A skew polynomial ring over a Jacobson ring need not be a Jacobson ring, Comm. Algebra 5 (8) (1977), 783-794.

[PSW] K. R. Pearson, W. Stephenson and J. F. Watters, Skew polynomials and Jacobson rings, Proc. London Math. Soc. (3) 42 (1981), 559-576.

[R_1] J. C. Robson, Prime ideals in intermediate extensions, Proc. London

Math. Soc. (3), 44 (1982), 372-384.

[R_2] L. H. Rowen, Ring theory, Vol. I-II, Academic Press, Inc. (1988), San Diego, CA.

[RS] J. C. Robson and L. W. Small, Liberal Extensions, Proc. London Math. Soc. (3), 42 (1981), 87-103.

[S] A. A. Sant'Ana, Ideais primos e fechados em extensões de anéis, UFRGS, dissertação de mestrado (1992).

[W_1] R. B. Warfield, Jr., Prime ideals in ring extensions, J. London Math. Soc. (2) 28 (1983), 453-460.

[W_2] J. F. Watters, Polynomial extensions of Jacobson rings, J. Algebra 36 (1975), 302-308.