IDENTIDADES POLINOMIAIS
DE
ANÉIS FINITOS

Nair Alexandre Fernandes

DISSERTAÇÃO APRESENTADA AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA UNIVERSIDADE DE SÃO PAULO
PARA OBTENÇÃO DO GRAU DE MESTRE
EM MATEMÁTICA

ORIENTADOR: PROF.DR. FRANCISCO CÉSAR POLCINO MILIES

Durante a elaboração deste trabalho a autora recebeu apoio financeiro do CNPq e da FINEP.

São Paulo, Outubro de 1978

À minha mãe

PREFÁCIO

Dado um anel R finito de ordem n , que técnicas usar para estabelecer alguns resultados sobre sua estrutura, e desta forma obter uma classificação de todos os anéis finitos de ordem n ?

Uma olhada para o grupo aditivo de R reduz o problema para o caso em que n é uma potência de um primo p , desde que a decomposição do grupo aditivo de um anel em seus p -subgrupos de Sylow induz uma soma direta de anel.

A partir disto um caminho que surge naturalmente é determinar (a menos de isomorfismos) os anéis finitos de ordem p^k . Entretanto, em [7], cap.V, R.L.Kruse e D.T. Price, considerando apenas anéis nilpotentes, mostram que o número de anéis nilpotentes, não isomorfos dois a dois, de ordem p^k cresce muito rapidamente com k . É interessante observar que se R é um anel, não nulo, sem elementos nilpotentes distintos do elemento nulo, então, R é isomorfo a um produto direto de um número finito de corpos, sendo, portanto, comutativo.

Agora, anel comutativo é um caso particular de anel com identidade polinomial.

Isto, parece sugerir um outro caminho: o estudo de anéis com identidades polinomiais, incluindo o estudo de tais identidades.

Seguindo esta idéia nosso trabalho apresenta um teorema obtido por R.L.Kruse em [6] sobre as identidades polinomiais de um anel finito.

Os capítulos 1, 2 e 3 contêm conceitos e resultados
(iii)

que são utilizados na demonstração deste teorema.

No capítulo 1, essencialmente, apresentamos dois teoremas, devidos a J.Lewin [8], referentes a subanéis de índice finito em anéis finitamente gerados. No que segue utilizaremos estes resultados apenas para o caso particular de ideais.

No capítulo 2 estudamos as variedades de anéis, que constituem as ferramentas básicas para o que apresentaremos em continuação; introduzimos conceitos e resultados para anéis, análogos a alguns apresentados para grupos no livro de Hanna Neumann [9].

No capítulo 3 destacamos os conceitos de anel crítico e de variedade de Cross, bem como alguns resultados relacionados a tais conceitos, e que desempenham um papel importante na demonstração do resultado principal.

No capítulo 4 apresentamos a demonstração do resultado principal; incluímos, também, um exemplo de variedade de Cross, e uma extensão do resultado principal, bem como uma tentativa no sentido de estender um pouco mais este último resultado.

Tanto o capítulo 3, como o capítulo 4, são baseados no trabalho de R.L.Kruse [6].

Agradecemos às várias pessoas que de uma forma ou de outra nos auxiliaram neste trabalho.

Em particular,

à amiga Maria Lúcia Sobral Singer, pelo espontâneo e constante incentivo, bem como por inúmeras conversas proveitosas;

à equipe da Biblioteca que com gentil presteza nos auxiliou em nossas pesquisas;

aos professores Francisco Miraglia Neto e Héctor Alfredo Merklen Goldschmidt, por sugestões que contribuíram para que alguns dos resultados fossem apresentados de uma forma mais clara;

ao professor Francisco César Polcino Milies, pela sugestão do tema desta dissertação, bem como pela dedicação com que orientou este trabalho.

Nair Alexandre Fernandes

ÍNDICE

Introdução	(vii)
Capítulo 1 SUBANÉIS DE ÍNDICE FINITO EM ANÉIS FINITAMEN TE GERADOS.....	1
Capítulo 2 VARIEDADES DE ANÉIS	10
Conceitos básicos	10
Anéis relativamente livres	13
Variedades como classes fechadas de anéis ..	17
Variedades geradas por uma classe finita de anéis finitos	25
Os anéis n -gerados e as identidades em n in- determinadas de uma variedade.....	36
Capítulo 3 ANÉIS CRÍTICOS E VARIEDADES DE CROSS.....	40
Anéis críticos	40
Variedades de Cross	60
Capítulo 4 IDENTIDADES POLINOMIAIS DE CERTOS ANÉIS.....	64
O resultado principal	64
Um exemplo de variedade de Cross	77
Uma extensão de resultado principal	78
Uma observação final	88
Referências Bibliográficas	95

INTRODUÇÃO

Seja Z um conjunto cujos elementos chamaremos *indeterminadas*. Uma n -upla de elementos em Z , que denotaremos por $z_1 z_2 \dots z_n$, é chamada um *monômio*. O número de indeterminadas em um monômio diz-se o *grau* do monômio. Por definição, o *produto* de dois monômios $t_1 t_2 \dots t_n$ e $y_1 y_2 \dots y_n$ é o monômio $t_1 t_2 \dots t_n y_1 y_2 \dots y_n$.

Indicaremos por M o conjunto dos monômios, e por $\mathbb{Z}$ o conjunto dos números inteiros. Nestas condições, chamaremos *anel livre* gerado pelo conjunto Z ao anel $F[Z]$ das funções $f: M \rightarrow \mathbb{Z}$ tais que o conjunto $\sigma(f) = \{z \in M: f(z) \neq 0\}$ é finito, com a adição e a multiplicação de dois elementos $f, g \in F[Z]$ definidas por:

$$(f+g)(z) = f(z) + g(z), \quad \forall z \in M$$

$$(fg)(z) = \sum_{uv=z} f(u) g(v), \quad \forall z \in M$$

Dado $z \in M$ vamos identificá-lo com o elemento $f_z \in F[Z]$ tal que, $f_z(z) = 1$, e $f_z(z') = 0$, se $z \neq z'$. Neste caso também diremos que f_z é um *monômio*. Assim, se f é um elemento não nulo de $F[Z]$, então, f pode ser escrito de uma única forma como uma combinação linear de monômios com coeficientes in-

(vii)

teiros não nulos. O máximo entre os graus destes monômios diz-se o grau de f .

É importante observar que dados um anel livre $F[Z]$ gerado por um conjunto Z , e um anel R , toda função $\alpha: Z \rightarrow R$ pode ser estendida a um único homomorfismo $\bar{\alpha}: F[Z] \rightarrow R$ da forma óbvia.

O posto de $F[Z]$ é a cardinalidade de Z . Quando Z for um conjunto enumerável $X = \{x_1, x_2, \dots\}$ chamaremos *anel livre dos polinômios* nas indeterminadas $x_1, x_2, \dots$, ao anel livre gerado por X , e o denotaremos por $\mathbb{Z}[X]$.

Se $f \in \mathbb{Z}[X]$ e $x_1, x_2, \dots, x_n$ são as indeterminadas que comparecem em f , então, f pertence ao subanel, que denotaremos por $\mathbb{Z}[x_1, x_2, \dots, x_n]$, gerado pelo conjunto finito $\{x_1, x_2, \dots, x_n\}$. De acordo com isto, escrevemos $f = f(x_1, x_2, \dots, x_n)$ e, dados um anel R e um homomorfismo $\alpha: \mathbb{Z}[X] \rightarrow R$, escrevemos $\alpha(f) = f(r_1, r_2, \dots, r_n)$, onde $r_i = \alpha(x_i)$, para $i = 1, 2, \dots, n$.

Dizemos que um polinômio $f = f(x_1, x_2, \dots, x_n)$ é uma *identidade polinomial* ou, simplesmente, uma *identidade* de um anel R se $\alpha(f) = 0$, para todo $\alpha \in \text{Hom}(\mathbb{Z}[X], R)$ ou, equivalentemente, se $f(r_1, r_2, \dots, r_n) = 0$, para quaisquer elementos $r_1, r_2, \dots, r_n$ em R .

Dado um conjunto de polinômios V , dizemos que um polinômio f é uma *consequência* de V se, para todo anel R tal que os polinômios de V são identidades de R , tem-se que f é uma identidade de R .

Dizemos que um conjunto de polinômios U , é *finitamente baseado* se existe um conjunto finito de polinômios U' contido em U tal que todo polinômio de U é uma consequência de U' .

O resultado principal deste nosso trabalho é o seguinte teorema obtido por R.L.Kruse [6]:

(ix)

TEOREMA 1 - *O conjunto das identidades de todo anel finito é finitamente baseado.*

Como em [6], uma vez demonstrado, estenderemos este resultado para obter:

TEOREMA 2 - *Se um anel R contém um ideal nilpotente N tal que R/N é finito, então, o conjunto das identidades de R é finitamente baseado.*

CAPÍTULO 1

SUBANÉIS DE ÍNDICE FINITO EM ANÉIS

FINITAMENTE GERADOS

Dado um anel R denotaremos por R^+ o grupo aditivo de R . Se R for um anel finito, a ordem de R , que indicaremos por $|R|$, é a ordem de R^+ . Dado um subanel S de R , chamaremos o índice de S em R , e denotaremos por $[R:S]$ ao índice de S^+ em R^+ .

Nosso objetivo, neste capítulo, é estudar subanéis de índice finito em anéis finitamente gerados. Os resultados principais que apresentaremos são os seguintes teoremas devidos a J.Lewin [8].

TEOREMA 1.1 - *Um anel finitamente gerado contém somente um número finito de subanéis de um dado índice finito.*

TEOREMA 1.2 - *Um subanel de índice finito em um anel finitamente gerado é finitamente gerado.*

Iniciamos com a demonstração do seguinte

LEMA 1.3 - *Seja R um anel e S um subanel de R tal que $[R:S] = m$, para algum inteiro positivo m . Se o número de elementos em S é maior que $(m+1)^{(m+1)^2}$, então, S contém um ideal não nulo de R .*

Demonstração - Seja $U = \{u_1, u_2, \dots, u_m\}$ um conjunto

completo de representantes das classes que S^+ determina em R^+ .

Para facilitar as notações introduziremos o símbolo u_0 que irá operar multiplicativamente como a identidade, isto é, para todo $r \in R$, os produtos da forma $u_0 r$ e ru_0 indicam, simplesmente, o elemento r . Chamaremos este símbolo uma *unidade formal* do anel R .

Seja $Q = \{0, 1, 2, \dots, m\}$. Para todo par $(i, j) \in Q \times Q$ e $s \in S$, o elemento $u_i s u_j$ pode ser escrito como um elemento de U mais um elemento de S . Definimos, então, para cada $s \in S$, uma função

$$f_s: Q \times Q \rightarrow Q$$

de forma que, para todo par $(i, j) \in Q \times Q$, $f_s(i, j)$ é o índice tal que

$$u_i s u_j = u_{f_s(i, j)} + s_{ij}, \quad s_{ij} \in S; \quad 0 \leq i, j \leq m.$$

Agora, existem somente $(m+1)^{(m+1)^2}$ funções de $Q \times Q$ em Q e o número de elementos em S é maior que $(m+1)^{(m+1)^2}$; logo, existem dois elementos distintos s_1 e s_2 em S , para os quais $f_{s_1} = f_{s_2}$.

Finalmente, consideremos o ideal I (não nulo) de R gerado por $s_1 - s_2$. Provaremos que $I \subseteq S$.

Para isto, observemos que, pela escolha de s_1 e s_2 ,

$$u_i (s_1 - s_2) u_j \in S, \quad \forall i, j, \quad 0 \leq i, j \leq m.$$

De fato, para todo par $(i, j) \in Q \times Q$,

$$u_i s_1 u_j = u_{f_{s_1}(i, j)} + s_{1ij} \quad \text{e} \quad u_i s_2 u_j = u_{f_{s_2}(i, j)} + s_{2ij}$$

onde s_{1ij} e s_{2ij} são elementos em S ; logo,

$$u_i s_1 u_j - u_i s_2 u_j = s_{1ij} - s_{2ij} \in S, \quad \forall i, j, \quad 0 \leq i, j \leq m.$$

Além disto, para todo $r \in R$, desde que $r = u_i + s$, para

algum i , $1 \leq i \leq m$, e algum $s \in S$, temos que

$$r(s_1 - s_2) = u_i(s_1 - s_2) + s(s_1 - s_2) \in S.$$

Da mesma forma, $(s_1 - s_2)r$ e $r_1(s_1 - s_2)r_2$ também são elementos em S , para quaisquer elementos r , r_1 e r_2 em R .

Portanto, $I \subseteq S$. $\square$

O próximo resultado permitirá restringir nossa atenção a ideais.

LEMA 1.4 - Sejam R um anel e S um subanel de R tal que $[R:S] = m$, para algum inteiro positivo m . Então, existe um ideal I de R tal que

$$I \subseteq S \text{ e } [R:I] \leq m(m+1)^{(m+1)^2}.$$

Demonstração - Seja $F = \{I_\lambda : \lambda \in \Lambda\}$, a família dos ideais de R contidos em S . Então F contém um elemento maximal I . De fato, I é o conjunto das somas finitas $\sum r_\lambda$, onde $r_\lambda \in I_\lambda$.

Sejam $\bar{R} = R/I$ e $\bar{S} = S/I$. Como $[\bar{R}:\bar{S}] = m$, segue-se do lema 1.3 que, se o número de elementos em $\bar{S}$ é maior que $(m+1)^{(m+1)^2}$, então $\bar{S}$ contém um ideal não nulo de $\bar{R}$, o que contradiz a definição de I . Assim, $|\bar{S}| \leq (m+1)^{(m+1)^2}$ e portanto,

$$|R/I| = |\bar{R}| = m|\bar{S}| \leq m(m+1)^{(m+1)^2}. \quad \square$$

Observemos agora que, se I é um ideal de $F = \mathbb{Z}[x_1, x_2, \dots, x_n]$ e U é um conjunto completo de representantes das classes que I^+ determina em F^+ , então, U pode ser escolhido com a seguinte propriedade:

(*) se $f \in U$ tem grau k , para algum inteiro positivo k , então para todo inteiro l , com $1 \leq l \leq k$, existe $g \in U$ tal que g tem grau l .

De fato, construímos U tomando representantes de grau mínimo em cada uma das classes que I^+ determina em F^+ . Provaremos que U , assim construído, satisfaz a propriedade (*).

Suponhamos, por absurdo, que existem $u \in U$ de grau k

e um inteiro ℓ , $1 \leq \ell < m$, tal que U não possui elementos de grau ℓ . Nestas condições, se d é um inteiro maior ou igual a ℓ , mostraremos usando indução sobre d que todo monômio de grau d é congruente módulo I^+ a um polinômio de grau menor que ℓ .

Com efeito, se $d = \ell$ e f é um monômio de grau ℓ , então, como U não contém elementos de grau ℓ , segue-se que f é congruente módulo I^+ a um polinômio de grau menor que ℓ .

Suponhamos, agora que monômios de grau $d \leq \ell$ são congruentes módulo I^+ a polinômios de grau menor que ℓ , e provemos que isto também ocorre para um monômio g de grau $d+1$.

Ora, neste caso, $g = x_i g_1$, para algum i , $1 \leq i \leq n$, e algum monômio g_1 , de grau d . Assim, pela hipótese de indução, existe um polinômio h de grau menor que ℓ tal que

$$g_1 + I = h + I,$$

logo,

$$x_i g_1 + I = x_i h + I,$$

onde $x_i h$ é um polinômio de grau menor ou igual a ℓ . Portanto, $x_i h$ é uma combinação linear de monômios de grau menor ou igual a ℓ com coeficientes inteiros; conseqüentemente, pela hipótese de indução, existe um polinômio h_1 de grau menor que ℓ tal que

$$x_i h + I = h_1 + I.$$

Desta forma, U não possui elementos de grau maior que ℓ , o que contraria o fato de existir u em U de grau $k > \ell$ e prova, então, que U satisfaz a propriedade (*).

Disto resulta que, se $[F:I] = m$, para algum inteiro positivo m , então, um conjunto completo de representantes das classes que I^+ determina em F^+ com a propriedade (*) possui apenas polinômios de grau menor ou igual a m .

Observemos, finalmente, que se R é um anel gerado por um conjunto com n elementos, para algum inteiro positivo

n , então, R é isomorfo a um anel quociente de $\mathbb{Z}[x_1, x_2, \dots, x_n]$. De fato, seja $\{r_1, r_2, \dots, r_n\}$ um conjunto de geradores de R , e seja

$$\alpha: \{x_1, x_2, \dots, x_n\} \rightarrow \{r_1, r_2, \dots, r_n\}$$

uma bijeção. Então, o homomorfismo $\bar{\alpha}: \mathbb{Z}[x_1, x_2, \dots, x_n] \rightarrow R$ que estende α é um epimorfismo e, portanto, temos que

$$R \cong \frac{\mathbb{Z}[x_1, x_2, \dots, x_n]}{\ker(\bar{\alpha})}$$

Estamos agora em condições de provar uma primeira versão do teorema 1.1, se em lugar de subanéis considerarmos ideais.

LEMA 1.5 - *Um anel finitamente gerado contém somente um número finito de ideais de um dado índice finito.*

Demonstração - Seja R um anel gerado por um conjunto finito com n elementos, e seja I um ideal de R tal que $[R:I] = m$, para algum inteiro positivo m .

Pelas observações anteriores podemos assumir $R = \mathbb{Z}[x_1, x_2, \dots, x_n]$ e considerar $U_I = \{u_1, u_2, \dots, u_m\}$ um conjunto completo de representantes das classes que I^+ determina em R^+ com a propriedade (*).

Para cada $r \in R$, associamos uma permutação γ_I^r do conjunto $Q = \{1, 2, \dots, m\}$ definida de forma tal que, para cada i , $1 \leq i \leq m$, tem-se

$$(r+u_i) + I = u_{\gamma_I^r(i)} + I.$$

Observemos que γ_I^r está bem definida, e que é de fato uma permutação de Q . Observemos também que a aplicação γ_I^r que a cada $r \in R$ associa γ_I^r é um homomorfismo de R^+ no grupo simétrico S_m . Com efeito, indicando por $\circ$ a operação em S_m , temos

$$\gamma_I^{(r_1+r_2)} = \gamma_I^{r_1} \circ \gamma_I^{r_2}, \quad \forall r_1, r_2 \in R.$$

Para verificarmos isto, seja $i \in Q$. Então, $\gamma_I^{(r_1+r_2)}(i) = j \in Q$, tal que

$$(r_1+r_2+u_i) + I = u_j + I.$$

Por outro lado, $\gamma_I^{r_2}(i) = j_1 \in Q$ tal que

$$(r_2+u_i) + I = u_{j_1} + I,$$

e $\gamma_I^{r_1}(j_1) = j_2 \in Q$, tal que

$$(r_1+u_{j_1}) + I = u_{j_2} + I;$$

logo,

$$u_j + I = (r_1+r_2+u_i) + I = (r_1+u_{j_1}) + I = u_{j_2} + I, \text{ por}$$

tanto, $j = j_2$ e, conseqüentemente,

$$\gamma_I^{(r_1+r_2)}(i) = (\gamma_I^{r_1} \circ \gamma_I^{r_2})(i), \quad \forall i \in Q.$$

Além disto, $\ker(\gamma_I) = I$. De fato, dado $r \in I$, temos que

$$(r+u_i) + I = u_i + I, \quad \forall i \in Q;$$

logo, $\gamma_I^r(i) = i$, para todo $i \in Q$ e, portanto, $r \in \ker(\gamma_I)$. Por outro lado, dado $r \in \ker(\gamma_I)$ é claro que existe $i \in Q$, tal que $\gamma_I^r(i) = i$; logo, pela definição de γ_I^r , segue-se que $r \in I$. Assim, se I_1 e I_2 são dois ideais distintos de índice m em R , então, $\gamma_{I_1} \neq \gamma_{I_2}$.

Observemos agora que γ_I é completamente determinado por seus valores em U_I , uma vez que, para todo $r \in R$, podemos escrever $r = u_i + s$ para algum i , $1 \leq i \leq m$, e algum $s \in I$ e portanto temos que

$$\gamma_I(r) = \gamma_I(u_i) \circ \gamma_I(s) = \gamma_I(u_i).$$

Então, Γ_I é completamente determinado por seus valores no subgrupo A_m de R^+ dos polinômios de grau menor ou igual a m .

Como A_m é gerado pela união dos conjuntos

$$A_j = \{x_{i_1} x_{i_2} \dots x_{i_j} : 1 \leq i_1, i_2, \dots, i_j \leq n\}, 1 \leq j \leq m,$$

temos que A_m é finitamente gerado; logo, existem somente um número finito de homomorfismos de A_m em S_m , donde resulta que R contém apenas um número finito de ideais de índice m . $\square$

Demonstração do teorema 1.1 - Seja R um anel finitamente gerado e S um subanel de R tal que $[R:S] = m$, para algum inteiro positivo m .

Pelo lema 1.4, existe um ideal I de R tal que $I \subseteq S$ e $[R:I] \leq m(m+1)^{(m+1)^2}$ e, pelo lema 1.5, o número de ideais J de R tais que $[R:J] \leq m(m+1)^{(m+1)^2}$ é finito.

Sendo, então $J_1, J_2, \dots, J_\ell$ tais ideais, temos que, para todo $i=1, 2, \dots, \ell$, J_i pode estar contido em apenas um número finito de subanéis de R , uma vez que R/J_i é um anel finito e, portanto, contém apenas um número finito de subanéis; consequentemente, R contém apenas um número finito de subanéis de índice m . $\square$

Também para a prova do teorema 1.2, provamos antes um caso particular dado pelo seguinte:

LEMA 1.6 - *Um ideal de índice finito em um anel finitamente gerado é finitamente gerado como anel.*

Demonstração - Como no lema 1.5 é suficiente considerarmos anéis livres gerados por um conjunto finito.

Sejam, então, $R = \mathbb{Z}[x_1, x_2, \dots, x_n]$ e I um ideal de R tal que $[R:I] = m$, para algum inteiro positivo m . Sejam, ainda, $U = \{u_1, u_2, \dots, u_m\}$ um conjunto completo de representantes das classes que I^+ determina em R^+ , A o subgrupo de R^+ gerado por U e u_0 uma unidade formal de R definida como no lema

1.3.

Desde que, para todo $f \in R$, podemos escrever $f = u_i + r$, para algum i , $1 \leq i \leq m$, e algum $r \in I$, temos em particular que

$$x_i = u_{j(i)} + r_i, \quad r_i \in I; \quad 1 \leq j(i) \leq m; \quad i = 1, 2, \dots, n \quad (1)$$

e

$$u_i u_j = u_{k(i,j)} + s_{ij}, \quad s_{ij} \in I; \quad 1 \leq k(i,j) \leq m; \quad i, j \in \{1, 2, \dots, m\} \quad (2)$$

Consideremos

$$T = \left\{ u_i r_p u_\ell, u_i s_{jk} u_\ell : p \in \{1, 2, \dots, m\}; i, j, k, \ell \in \{0, 1, \dots, n\} \right\}$$

Então, o subanel J gerado por T é de fato um ideal, pois, para todo $t \in T$ e todo i , $1 \leq i \leq n$, facilmente verifica-se usando as relações (1) e (2), que tx_i e $x_i t$ são elementos em J .

Seja agora g um monômio arbitrário em R . Por indução sobre o grau de g , e considerando mais uma vez as relações (1) e (2), é simples provar que existem inteiros n_i , $1 \leq i \leq m$, e $r \in J$ tais que

$$g = \sum_{i=1}^m n_i u_i + r.$$

Portanto, para todo $f \in R$, existem inteiros m_i , $1 \leq i \leq m$, e $s \in J$ tais que

$$f = \sum_{i=1}^m m_i u_i + s.$$

Como $J \subseteq I$, temos que, se $f \in I$, então $\sum_{i=1}^m m_i u_i \in I$; logo,

$f \in (A \cap I) + J$, e, conseqüentemente, $I = (A \cap I) + J$.

Por outro lado, J e $(A \cap I)^+$, como subgrupo de Λ , que é abeliano e finitamente gerado, são ambos finitamente gerados como anéis. Assim, I é finitamente gerado como anel. $\square$

Demonstração do teorema 1.2 - Seja R um anel finitamente gerado, e seja S um subanel de R tal que $[R:S] = m$, pa

ra algum inteiro positivo m .

Pelo lema 1.4, existe um ideal I de R tal que $I \subseteq S$ e $[R:I] \leq m(m+1)^{(m+1)^2}$. Assim, pelo lema 1.6, I é finitamente gerado como anel.

Por outro lado, $[S:I] \leq [R:I]$; logo, S contém um ideal finitamente gerado de índice finito, portanto, é finitamente gerado. $\square$

CAPÍTULO 2

VARIEDADES DE ANÉIS

Este capítulo poderia ser desenvolvido num contexto mais geral de álgebra universal, e parte do que apresentaremos pode ser encontrada desta forma no livro de P.M.Cohn [2]. Entretanto para este trabalho, vamos desenvolvê-lo apenas para anéis, de forma análoga à apresentação dada por Hanna Neumann em [9] para grupos.

Tanto as variedades, quanto também os métodos empregados no seu estudo constituem poderosas ferramentas na teoria dos grupos. Nos capítulos que seguem teremos oportunidade de comprovar este fato na teoria de anéis.

CONCEITOS BÁSICOS

DEFINIÇÃO 2.1 - Dado um conjunto de polinômios V , chamaremos *variedade de anéis* determinada por V à classe dos anéis R tais que os polinômios de V são identidades de R .

Vejamos algumas classes de anéis que são variedades.

EXEMPLO 2.2 - Consideremos o polinômio $f = x_1 x_2 - x_2 x_1$. Então, a variedade de anéis determinada por $\{f\}$ é a classe dos anéis comutativos.

Antes de continuarmos com mais alguns exemplos, lem

brems que um anel R diz-se *nilpotente*, se existe um inteiro positivo n tal que o produto de quaisquer n elementos em R é zero. O menor de tais inteiros é chamado *expoente* de R e denotado por $\exp(R)$.

Lembremos também que a *característica* de um anel R , indicada por $\text{car}(R)$, é o menor inteiro positivo c tal que $cr=0$, para todo $r \in R$, ou zero, se tal inteiro não existir.

EXEMPLO 2.3 - Seja n um inteiro positivo e consideremos o polinômio $g = x_1 x_2 \dots x_n$. Então, a variedade de anéis determinada por $\{g\}$ é a classe dos anéis nilpotentes de expoente menor ou igual a n .

EXEMPLO 2.4 - Seja c um inteiro positivo e consideremos o polinômio $h = cx$. Então, a variedade de anéis determinada por $\{h\}$ é a classe dos anéis cuja característica divide c .

DEFINIÇÃO 2.5 - Dados um anel R e um conjunto de polinômios U , denotaremos por $U(R)$ o ideal de R gerado pelo conjunto

$$\{\alpha(u) : u \in U, \alpha \in \text{Hom}(\mathbb{Z}[X], R)\}.$$

PROPOSIÇÃO 2.6 - Seja B uma variedade de anéis determinada por um conjunto de polinômios V . Então, um anel R pertence a B se, e somente se, $V(R) = \{0\}$.

Demonstração - Se R é um anel em B , então, para todo $f \in V$ e todo $\alpha \in \text{Hom}(\mathbb{Z}[X], R)$, temos que $\alpha(f) = 0$; logo, os geradores do ideal $V(R)$ são nulos e, conseqüentemente, $V(R) = \{0\}$.

Para a recíproca, seja R um anel tal que $V(R) = \{0\}$. Então, para todo $f \in V$ e todo $\alpha \in \text{Hom}(\mathbb{Z}[X], R)$, temos que $\alpha(f) = 0$. Assim, todo polinômio em V é uma identidade de R , logo $R \in B$. $\square$

DEFINIÇÃO 2.7 - Seja f um polinômio, e seja B uma variedade de anéis determinada por um conjunto de polinômios

V. Então, dizemos que f é uma identidade de B , se f é uma identidade de todo anel em B .

Observemos que, se W é o conjunto das identidades de B , então, $V \subseteq W$ e a variedade determinada por W é B .

Vejamos em continuação outras propriedades de W .

PROPOSIÇÃO 2.8 - *Seja B uma variedade de anéis determinada por um conjunto de polinômios V , e seja W o conjunto de suas identidades. Então W é um ideal de $\mathbb{Z}[X]$ e, para todo $\theta \in \text{End}(\mathbb{Z}[X])$, $\theta(W) \subseteq W$.*

Demonstração - É uma verificação imediata que W é um ideal de $\mathbb{Z}[X]$.

Para a segunda parte, sejam $f = f(x_1, x_2, \dots, x_n) \in W$ e $\theta \in \text{End}(\mathbb{Z}[X])$. Provaremos que $\theta(f) \in W$. Para isto, sejam $R \in B$, $\alpha \in \text{Hom}(\mathbb{Z}[X], R)$, e consideremos o homomorfismo $\beta: \mathbb{Z}[X] \rightarrow R$, definido de forma tal que

$$\beta(x_i) = \alpha(\theta(x_i)), \quad 1 \leq i \leq n.$$

Nestas condições, $\alpha(\theta(f)) = \beta(f)$. Como $\beta(f) = 0$, pois f é uma identidade de R , temos que $\alpha(\theta(f)) = 0$. Portanto, $\theta(f) \in W$. $\square$

PROPOSIÇÃO 2.9 - *Seja B uma variedade de anéis determinada por um conjunto de polinômios V , e seja W o conjunto de suas identidades. Então, $W = V(\mathbb{Z}[X])$.*

Demonstração - Como $V \subseteq W$, pela proposição anterior, temos que $\theta(f) \in W$, para todo $f \in V$ e todo $\theta \in \text{End}(\mathbb{Z}[X])$. Assim, os geradores do ideal $V(\mathbb{Z}[X])$ pertencem a W e como, também pela proposição anterior, W é um ideal de $\mathbb{Z}[X]$, segue-se que $V(\mathbb{Z}[X]) \subseteq W$.

Para a inclusão contrária, observemos que o anel $\mathbb{Z}[X]/V(\mathbb{Z}[X])$ pertence a B e que além disso, suas identidades são exatamente os polinômios de $V(\mathbb{Z}[X])$.

Portanto, $W = V(\mathbb{Z}[X])$. $\square$

Introduzimos a seguir o conceito de subvariedade.

DEFINIÇÃO 2.10 - Dada uma variedade de anéis B determinada por um conjunto de polinômios V , dizemos que uma classe de anéis B' é uma *subvariedade* (*subvariedade própria*) de B , se $B' \subseteq B$ ($B' \subset B$) e B' é uma variedade, isto é, existe um conjunto de polinômios U tal que B' é a variedade de anéis determinada por U .

EXEMPLO 2.11 - Sejam m e n inteiros positivos tais que $m < n$, e sejam B a variedade dos anéis nilpotentes de expoente menor ou igual a n e B' a variedade dos anéis nilpotentes de expoente menor ou igual a m . Nestas condições, claramente, B' é uma subvariedade de B . Além disso, B' é própria, uma vez que o anel $S_n = 2.\mathbb{Z}_2^n \subseteq \mathbb{Z}_2^n$ é nilpotente de expoente n ; logo, pertence a B e não pertence a B' .

EXEMPLO 2.12 - Consideremos o polinômio $t = x_1 x_2 - x_3 x_1$, e seja B a variedade de anéis determinada por $\{t\}$. Claramente, B é uma subvariedade da variedade dos anéis comutativos e, além disso, B é própria. De fato, se R é um anel não nulo, com unidade em particular, comutativo, então $f(1,1,0) \neq 0$ em R , portanto, $R \notin B$.

PROPOSIÇÃO 2.13 - Se B é uma variedade de anéis determinada por um conjunto de polinômios V , e B' é uma subvariedade de B determinada por um conjunto de polinômios U , então, $V(\mathbb{Z}[X]) \subseteq U(\mathbb{Z}[X])$.

Demonstração - Pela proposição 2.9, $V(\mathbb{Z}[X])$ e $U(\mathbb{Z}[X])$ são os conjuntos das identidades de B e B' , respectivamente.

Assim, como uma identidade de B é também uma identidade de B' , segue-se a tese. $\square$

ANÉIS RELATIVAMENTE LIVRES

Dado um anel livre $F[Z]$ gerado por um conjunto Z , toda função $\alpha: Z \rightarrow F[Z]$ pode ser estendida a um endomorfismo de $F[Z]$. Usaremos esta propriedade dos anéis livres para defi-

nir uma nova classe de anéis.

DEFINIÇÃO 2.14 - Dizemos que um anel R é *relativamente livre* se contém um conjunto de geradores H tal que toda função $\alpha: H \rightarrow R$ pode ser estendida a um endomorfismo de R .

TEOREMA 2.15 - Dado um anel R , são equivalentes:

- (i) R é um anel relativamente livre;
- (ii) R contém um conjunto de geradores G tal que, para todo polinômio $f = f(x_1, x_2, \dots, x_n)$, se existem n elementos distintos $g_1, g_2, \dots, g_n$ em G , com $f(g_1, g_2, \dots, g_n) = 0$, então f é uma identidade de R ;
- (iii) R é isomorfo a um anel de forma $F/U(F)$ onde F é um anel livre e U é um conjunto de polinômios;
- (iv) R é isomorfo a um anel quociente F/J de um anel livre F tal que todo endomorfismo de F induz um endomorfismo de F/J , isto é, para todo $\alpha \in \text{End}(F)$, existe $\alpha^* \in \text{End}(F/J)$ tal que $\alpha^*(f+J) = \alpha(f) + J$, para todo $f \in F$.

Demonstração - (i) $\implies$ (ii) - Seja H um conjunto de geradores de R que satisfaz a condição da definição 2.14 e suponhamos que $f = f(x_1, x_2, \dots, x_n)$ é um polinômio tal que existem n elementos distintos $h_1, h_2, \dots, h_n$ em H com $f(h_1, h_2, \dots, h_n) = 0$. Nestas condições, provemos que f é uma identidade de R .

Para isto, sejam $r_1, r_2, \dots, r_n$ elementos quaisquer em R e $\alpha: H \rightarrow R$ a função tal que

$$\alpha(h_i) = r_i, \quad 1 \leq i \leq n.$$

Então, estendendo α a um endomorfismo $\bar{\alpha}$ de R , temos que:

$$\begin{aligned} f(r_1, r_2, \dots, r_n) &= f(\alpha(h_1), \alpha(h_2), \dots, \alpha(h_n)) = \\ &= \bar{\alpha}(f(h_1, h_2, \dots, h_n)) = 0. \end{aligned}$$

Portanto, f é uma identidade de R e, assim, (ii) é verificado

se tomarmos $G = H$.

(ii) $\implies$ (iii) - Seja F um anel livre gerado por um conjunto Z que tem o mesmo cardinal de G , e seja $\phi: Z \rightarrow G$ uma bijeção. Então, ϕ pode ser estendida a um epimorfismo $\bar{\phi}: F \rightarrow R$ e, sendo $T = \ker(\bar{\phi})$, temos que $R \cong F/T$. Provaremos que $T = U(F)$, para algum conjunto de polinômios U .

Para isto observemos que $\theta(T) \subseteq T$, para todo $\theta \in \text{End}(F)$. De fato, dado $t \in T$, existe $h = h(x_1, x_2, \dots, x_n) \in \mathbb{Z}[X]$ tal que $t = h(z_1, z_2, \dots, z_n)$, onde $z_1, z_2, \dots, z_n$ são n elementos distintos em Z . Assim, se $\bar{\phi}(t) = 0$, então $h(\phi(z_1), \phi(z_2), \dots, \phi(z_n)) = 0$, onde $\phi(z_1), \phi(z_2), \dots, \phi(z_n)$ são n elementos distintos em G ; logo, da hipótese, vem que h é uma identidade de R . Portanto, dado $\theta \in \text{End}(F)$, temos que

$$\bar{\phi}(\theta(t)) = h(\bar{\phi}(\theta(z_1)), \bar{\phi}(\theta(z_2)), \dots, \bar{\phi}(\theta(z_n))) = 0;$$

consequentemente, $\theta(T) \subseteq T$.

Seja agora U o conjunto dos polinômios $g = g(x_1, x_2, \dots, x_m)$ tais que existem m elementos distintos $z_1, z_2, \dots, z_m$ em Z com $g(z_1, z_2, \dots, z_m) \in T$, e provemos que $T = U(F)$.

Com efeito, dado $t \in T$, existe $h = h(x_1, x_2, \dots, x_n) \in \mathbb{Z}[X]$ tal que $t = h(z_1, z_2, \dots, z_n)$, onde $z_1, z_2, \dots, z_n$ são n elementos distintos em Z . Desta forma $h \in U$ e, portanto, $t \in U(F)$, donde segue que $T \subseteq U(F)$.

Para a inclusão contrária, seja $g = g(x_1, x_2, \dots, x_m)$ um polinômio em U , e sejam $f_1, f_2, \dots, f_m$ elementos quaisquer em F . Então existem m elementos distintos $z_1, z_2, \dots, z_m$ em Z com $g(z_1, z_2, \dots, z_m) \in T$, e seja $\theta \in \text{End}(F)$ tal que $\theta(z_i) = f_i, 1 \leq i \leq m$. Assim,

$$g(f_1, f_2, \dots, f_m) = g(\theta(z_1), \theta(z_2), \dots, \theta(z_m)) = \theta(g(z_1, z_2, \dots, z_m))$$

e, como $\theta(T) \subseteq T$, temos que $g(f_1, f_2, \dots, f_m) \in T$, donde resulta que $U(F) \subseteq T$.

(iii) $\implies$ (iv) - Basta tomar $J = U(F)$ e observar que $\theta(U(F)) \subseteq U(F)$, para todo $\theta \in \text{End}(F)$.

(iv) $\implies$ (i) - Seja Z um conjunto de geradores de F . Então, $Z' = \{z + J : z \in Z\}$ é um conjunto de geradores de F/J . Provaremos que Z' satisfaz a condição da definição 2.14.

Para isto, seja α uma função de Z' em F/J . Como todo elemento em F/J pode ser escrito na forma

$$f(z_1, z_2, \dots, z_n) + J, \text{ onde } f = f(x_1, x_2, \dots, x_n) \in \mathbb{Z}[X]$$

e $z_1, z_2, \dots, z_n$ são elementos em Z , fixemos uma tal representação para $\alpha(z+J)$, para cada $z \in Z$. Com isto, definamos uma função $\alpha_1: Z \rightarrow F$ de forma tal que $\alpha(z+J) = \alpha_1(z) + J$, para todo $z \in Z$, e estendamos α_1 a um endomorfismo $\bar{\alpha}_1$ de F .

Da hipótese, $\bar{\alpha}_1$ induz um endomorfismo de F/J que, pela definição de $\bar{\alpha}_1$ coincide com α em Z' , donde, então, segue-se (i). $\square$

Usaremos este teorema para mostrarmos que a classe dos anéis relativamente livres é mais ampla que a classe dos anéis livres.

EXEMPLO 2.16 - Sejam y uma indeterminada e $\mathbb{Z}[y]$ o anel livre dos polinômios em y . Seja, ainda, U o subconjunto de $\mathbb{Z}[X]$ formado pelo polinômio $f = x^2$. Então, pelo teorema anterior o anel $R = \mathbb{Z}[y]/U(\mathbb{Z}[y])$ é relativamente livre, e observando que todo monômio de $\mathbb{Z}[y]$, com grau maior ou igual a 2, pertence a $U(\mathbb{Z}[y])$, temos que

$$R = \{ny + U(\mathbb{Z}[y]) : n \in \mathbb{Z}\}.$$

Provaremos que nestas condições R não pode ser livre.

Inicialmente, observemos que todo anel livre F contém um conjunto infinito inumerável F' linearmente independente sobre $\mathbb{Z}$. De fato, basta tomar uma indeterminada t em F e considerar $F' = \{t^i : i=1, 2, \dots\}$.

Por outro lado, dois elementos em R são sempre linearmente dependentes sobre $\mathbb{Z}$.

Isto e a observação anterior implicam que R não pode ser livre.

A importância dos anéis relativamente livres, neste contexto, vem do seguinte:

TEOREMA 2.17 - *Seja B uma variedade de anéis determinada por um conjunto de polinômios V . Então um anel R pertence a B se, e somente se, R é isomorfo a um anel quociente de um anel relativamente livre da forma $F/V(F)$, onde F é um anel livre de posto conveniente.*

Demonstração - Sejam R um anel em B e G um conjunto de geradores de R . Sejam, ainda, F um anel livre gerado por um conjunto Z com a mesma cardinalidade de G e $\alpha: Z \rightarrow G$ uma bijeção. Nestas condições, α pode ser estendido a um epimorfismo $\bar{\alpha}: F \rightarrow R$ e, assim, temos que $R \cong \frac{F}{\ker(\bar{\alpha})}$. Além disso, como

$$\bar{\alpha}(V(F)) = V(\bar{\alpha}(F)) = V(R) = \{0\},$$

segue-se que $V(F) \subseteq \ker(\bar{\alpha})$, donde resulta $R \cong \frac{F/V(F)}{\ker(\bar{\alpha})/V(F)}$.

Para a recíproca, basta observar que $F/V(F) \in B$ e que todo anel quociente de um anel em B pertence a B . $\square$

DEFINIÇÃO 2.18 - *Seja B uma variedade de anéis determinada por um conjunto de polinômios V . Então, chamamos B -anel livre a todo anel relativamente livre da forma $F/V(F)$, onde F é um anel livre de posto arbitrário.*

Se o posto de F for um inteiro positivo n ou infinito enumerável, denotaremos o B -anel livre $F/V(F)$, respectivamente, por $F_n(B)$ ou $F_\infty(B)$.

VARIEDADES COMO CLASSES FECHADAS DE ANÉIS

Inicialmente, lembremos que o *produto cartesiano* de uma família de anéis $\{A_\lambda : \lambda \in \Lambda\}$ é o anel que denotaremos por $c\pi A_\lambda$ de todas as funções ϕ definidas em Λ tais que $\phi(\lambda) \in A_\lambda$, com a adição e a multiplicação de dois elementos $\phi, \psi \in c\pi A_\lambda$ definidas por

$$(\phi + \psi)(\lambda) = \phi(\lambda) + \psi(\lambda), \quad \forall \lambda \in \Lambda$$

e

$$(\phi \psi)(\lambda) = \phi(\lambda) \psi(\lambda), \quad \forall \lambda \in \Lambda.$$

As funções ϕ em $c\pi A_\lambda$ tais que o conjunto $\sigma(\phi) = \{\lambda \in \Lambda : \phi(\lambda) \neq 0\}$ é finito, formam um subanel que chamaremos *produto direto* da família $\{A_\lambda : \lambda \in \Lambda\}$ e denotaremos por πA_λ .

Se os anéis da família $\{A_\lambda : \lambda \in \Lambda\}$ são todos isomorfos a um dado anel A , denotaremos o produto cartesiano por A^Λ e o produto direto por $A^{(\Lambda)}$.

A propriedade do produto cartesiano mais importante neste contexto é a seguinte:

PROPOSIÇÃO 2.19 - *Um polinômio f é uma identidade do produto cartesiano (produto direto) de uma família de anéis $\{A_\lambda : \lambda \in \Lambda\}$ se, e somente se, f é uma identidade de A_μ , para todo $\mu \in \Lambda$.*

Demonstração - Seja f uma identidade de $c\pi A_\lambda (\pi A_\lambda)$. Como, para cada $\mu \in \Lambda$, A_μ é isomorfo ao subanel πB_λ de $c\pi A_\lambda (\pi A_\lambda)$, onde $B_\mu = A_\mu$ e $B_\lambda = \{0\}$, para $\lambda \neq \mu$, segue-se que f é uma identidade de A_μ , para todo $\mu \in \Lambda$.

Para a recíproca, seja $f = f(x_1, x_2, \dots, x_n)$ uma identidade de A_μ , para todo $\mu \in \Lambda$, e sejam $\phi_1, \phi_2, \dots, \phi_n$ elementos quaisquer em $c\pi A_\lambda (\pi A_\lambda)$. Então, para todo $\mu \in \Lambda$,

$$f(\phi_1, \phi_2, \dots, \phi_n)(\mu) = f(\phi_1(\mu), \phi_2(\mu), \dots, \phi_n(\mu)),$$

e como $\phi_1(\mu), \phi_2(\mu), \dots, \phi_n(\mu)$ são elementos em A_μ , temos que

$f(\phi_1(\mu), \phi_2(\mu), \dots, \phi_n(\mu)) = 0$; logo, $f(\phi_1, \phi_2, \dots, \phi_n) = 0$ e, portanto, f é uma identidade de $c\pi A_\lambda(\pi A_\lambda)$. $\square$

Para o que segue, dada uma classe de anéis X , denotaremos por:

sX , a classe dos anéis isomorfos a subanéis de anéis em X ;

qX , a classe das imagens homomorfas de anéis em X ;

cX , a classe dos produtos cartesianos de anéis em X ;

dX , a classe dos produtos diretos de um número finito de anéis em X .

DEFINIÇÃO 2.20 - Uma classe de anéis X diz-se *fechada* se $qX \subseteq X$, $sX \subseteq X$, e $cX \subseteq X$.

DEFINIÇÃO 2.21 - O *fecho* de uma classe de anéis X que denotaremos por $\bar{X}$, é a classe dos anéis R tais que, para algum inteiro positivo n , $R \in \ell_1 \ell_2 \dots \ell_n X$ onde ℓ_i é igual a s , q , ou c , para todo $i=1, 2, \dots, n$.

Observemos que $\bar{X}$ é uma classe fechada, e que está contida em toda classe fechada que contenha X . Mais adiante veremos que $\bar{X} = qscX$.

Nosso próximo objetivo é mostrar que os conceitos de classes fechadas e variedades de anéis coincidem. Isto será provado em vários passos.

PROPOSIÇÃO 2.22 - Toda variedade de anéis é uma classe fechada.

Demonstração - Seja B uma variedade de anéis. Então, é imediato que $sB \subseteq B$ e que $qB \subseteq B$. Além disso, pela proposição 2.19, temos também que $cB \subseteq B$; logo, B é uma classe fechada. $\square$

Usaremos esta proposição para exibir uma classe de anéis que não é uma variedade.

EXEMPLO 2.23 - A classe dos anéis nilpotentes não é uma variedade. Isto segue da proposição anterior e do fato que produto cartesiano de anéis nilpotentes não é necessariamente um anel nilpotente.

Para verificarmos esta última afirmação, lembremos que um elemento r de um anel diz-se *nilpotente* se existe um inteiro positivo n tal que $r^n = 0$. Claramente, todo elemento de um anel nilpotente é nilpotente.

Consideremos agora a família de anéis

$$\{S_k = 2 \cdot \mathbb{Z}_{2^k} \subseteq \mathbb{Z}_{2^k} : k=1, 2, \dots\}$$

Então, para cada $k=1, 2, \dots$, S_k é um anel nilpotente, mas o produto cartesiano $S = \prod S_k$ não é nilpotente, uma vez que o elemento $(2, 2, \dots, 2, \dots) \in S$ (isto é, a função $\phi \in S$ tal que $\phi(k) = 2 \in S_k$, para todo $k=1, 2, \dots$) não é nilpotente.

PROPOSIÇÃO 2.24 - Se B é uma variedade de anéis e X é a classe dos B -anéis livres, então, $B = \bar{X}$. Ainda mais, $B = qX$.

Demonstração - Da observação que segue à definição 2.21, e da proposição 2.22, temos que $\bar{X} \subseteq B$.

Por outro lado, pelo teorema 2.17, $B \subseteq qX$.

Portanto,

$$qX \subseteq \bar{X} \subseteq B \subseteq qX \subseteq \bar{X},$$

donde segue-se a tese. $\square$

Para os próximos resultados, sejam C uma classe fechada de anéis, W o conjunto das identidades de todo anel em C , e B a variedade de anéis determinada por W . Nestas condições, nosso objetivo é demonstrar que $B = C$.

PROPOSIÇÃO 2.25 - Existe um anel $A \in C$ tal que o conjunto de suas identidades é W .

Demonstração - Seja $\tilde{W} = \mathbb{Z}[X] \setminus W$. Se $\tilde{W} = \emptyset$, então, $A = \{0\}$. Caso contrário, para cada $f = f(x_1, x_2, \dots, x_n) \in \tilde{W}$, existe um anel $C_f \in C$, e existem elementos $a_1^f, a_2^f, \dots, a_n^f$ em C_f tais que $f(a_1^f, a_2^f, \dots, a_n^f) \neq 0$.

Seja A_f o subanel de C_f gerado pelos elementos $a_1^f, a_2^f, \dots, a_n^f$, e seja $A = c \cap A_f$. Então, é claro que $A \in C$; logo, os polinômios de W são identidades de A .

Além disso, se $f \in W$, f não é uma identidade de A_f ; consequentemente, pela proposição 2.19, também não é uma identidade de A .

Assim, o conjunto das identidades de A é precisamente W . $\square$

TEOREMA 2.26 - *Seja A um anel tal que o conjunto de suas identidades é W . Seja Λ um conjunto de índices e consideremos*

$$A^* = A^{A(\Lambda)}$$

(isto é, A^* é o produto cartesiano de uma família de anéis isomorfos a A e indexada por $A(\Lambda)$). Para cada $\lambda \in \Lambda$, seja $g_\lambda \in A^*$ definida de forma tal que

$$g_\lambda(\phi) = \phi(\lambda), \quad \forall \phi \in A(\Lambda).$$

Nestas condições, o subanel H de A^* gerado pelo conjunto $G = \{g_\lambda \in A^* : \lambda \in \Lambda\}$ é isomorfo ao B -anel livre $L/W(L)$, onde L é o anel livre gerado por G .

Demonstração - Inicialmente provemos que o conjunto U dos polinômios $g = g(x_1, x_2, \dots, x_m)$ tais que existem m elementos distintos $g_{\lambda_1}, g_{\lambda_2}, \dots, g_{\lambda_m}$ em G , com $g(g_{\lambda_1}, g_{\lambda_2}, \dots, g_{\lambda_m}) = 0$ está contido em W .

De fato, seja g um tal polinômio. Então, para todo $\phi \in A(\Lambda)$, temos que:

$$\begin{aligned} 0 &= g(g_{\lambda_1}, g_{\lambda_2}, \dots, g_{\lambda_m})(\phi) = g(g_{\lambda_1}(\phi), g_{\lambda_2}(\phi), \dots, g_{\lambda_m}(\phi)) = \\ &= g(\phi(\lambda_1), \phi(\lambda_2), \dots, \phi(\lambda_m)) \end{aligned}$$

Desta forma, observando que, para quaisquer elementos $a_1, a_2, \dots, a_m$ em A , existe $\phi \in A(\Lambda)$ tal que $\phi(\lambda_i) = a_i$, $1 \leq i \leq m$, segue-se

que $g \in W$ e, portanto, $U \subseteq W$.

Assim, se $g \in U$, pela proposição 2.19, g é uma identidade de A^* e, portanto, uma identidade de H . Então, pelo teorema 2.15, H é um anel relativamente livre. Além disso, conforme a prova de (ii) $\implies$ (iii) do mesmo teorema, temos que $H \cong F/U(F)$, onde F é um anel livre de posto igual a cardinalidade de G .

Finalmente, como $F \cong L$, resta apenas provar que $U(F) = W(F)$.

Para isto, sejam $h = h(x_1, x_2, \dots, x_n) \in W$ e $f_1, f_2, \dots, f_n$ elementos quaisquer em F . Então, como h é uma identidade de H , consequentemente, uma identidade de $F/U(F)$, temos que $h(f_1, f_2, \dots, f_n) + U(F) = U(F)$, donde resulta que $h(f_1, f_2, \dots, f_n) \in U(F)$; logo, $W(F) \subseteq U(F)$.

Por outro lado, como $U \subseteq W$, temos que $U(F) \subseteq W(F)$.

Portanto, $U(F) = W(F)$. $\square$

COROLÁRIO 2.27 - *Seja A um anel tal que o conjunto de suas identidades é W . Então, todo B -anel livre pertence a $\{\bar{A}\}$.*

Demonstração - Seja F um anel livre e consideremos o B -anel livre $F/W(F)$. Então, pelo teorema anterior, $F/W(F)$ é isomorfo a um subanel de $A^* = A^{\Lambda(\Lambda)}$, onde Λ é um conjunto de índices com cardinalidade igual ao posto de F ; logo, $F/W(F) \in \{\bar{A}\}$. $\square$

COROLÁRIO 2.28 - *Seja A um anel tal que o conjunto de suas identidades é W . Então, $B = \{\bar{A}\}$.*

Demonstração - Da proposição 2.22, B é uma classe fechada, e da hipótese $A \in B$; logo, $\{\bar{A}\} \subseteq B$.

Para a inclusão contrária, basta considerar o corolário anterior, e a proposição 2.24.

Portanto, $B = \{\bar{A}\}$. $\square$

TEOREMA 2.29 - *Toda classe fechada de anéis C é uma*

variedade. Mais precisamente, é a variedade de anéis B determinada pelo conjunto W dos polinômios que são identidades de todo anel em C .

Demonstração - Pela proposição 2.24, existe um anel $A \in C$ tal que o conjunto de suas identidades é W . Logo, pelo corolário 2.27, $B = \{\bar{A}\}$ e, portanto, $B \subseteq C$.

Por outro lado, se R é um anel em C , então os polinômios de W são identidades de R ; logo, $R \in B$ e, consequentemente, $C \subseteq B$.

Portanto, $B = C$. $\square$

COROLÁRIO 2.30 - Sejam X uma classe de anéis, e W o conjunto das identidades de todo anel em X . Então, $\bar{X}$ é a variedade de anéis determinada por W . Ainda mais, W é o conjunto de suas identidades.

Demonstração - Pelo teorema anterior, basta provar que o conjunto W' das identidades de todo anel em X é igual a W .

Para isto, seja $f \in W'$. Então, é claro que f é uma identidade de todo anel em X ; logo, $f \in W$ e, portanto, $W' \subseteq W$.

Para a inclusão contrária, se R é um anel em $\bar{X}$, então, para algum inteiro positivo n , $R \in \mathcal{L}_{\mathcal{L}_1 \mathcal{L}_2 \dots \mathcal{L}_n X}$, onde $\mathcal{L}_i$ é igual a q, s , ou c , para cada $i = 1, 2, \dots, n$. Além disso, por indução sobre n , é fácil provar que, se $f \in W$, então, f é uma identidade de todo anel em $\mathcal{L}_{\mathcal{L}_1 \mathcal{L}_2 \dots \mathcal{L}_n X}$, para todo inteiro positivo n ; logo, f é uma identidade de todo anel em $\bar{X}$, e consequentemente, $W \subseteq W'$.

Portanto, $W = W'$. $\square$

TEOREMA 2.31 - Para toda classe de anéis X , $\bar{\bar{X}} = qscX$.

Demonstração - Seja W o conjunto das identidades de todo anel em X . Então, pelo corolário anterior, $\bar{X}$ é a variedade

de determinada por W , e W é o conjunto de suas identidades.

Seja $\tilde{W} = \mathbb{Z}[X] \setminus W$. Se $\tilde{W} = \emptyset$, então, X só contém o anel nulo e a tese segue-se imediatamente.

Caso contrário, para todo $f \in \tilde{W}$, existe um anel $A_f \in X$ tal que f não é uma identidade de A_f , e consideremos $A = \prod A_f$. Então, $A \in X$ e, além disso, W é o conjunto das identidades de A .

Assim, pelo teorema 2.26, todo $\bar{X}$ - anel livre é isomorfo a um subanel de um produto cartesiano de cópias de A ; logo, pertence a $\text{sc}X = \text{sc}X$. Portanto, pela proposição 2.24, $X \subseteq \text{qsc}X$.

Finalmente, como a inclusão contrária é imediata, segue-se que $\bar{X} = \text{qsc}X$. $\square$

DEFINIÇÃO 2.32 - Dada uma classe de anéis X , chamaremos *variedade gerada por X* , e denotaremos por $\text{var}(X)$ ao fecho de X . Em particular, dado um anel R indicaremos por $\text{var}(R)$ a variedade gerada por $\{R\}$.

TEOREMA 2.33 - *Toda variedade de anéis é gerada pela classe de seus anéis finitamente gerados.*

Demonstração - Seja B uma variedade determinada por um conjunto de polinômios V , e seja W o conjunto de suas identidades. Então, pela proposição 2.22, B é uma classe fechada, e pela observação que segue à definição 2.7, B é a variedade determinada por W .

Nestas condições, conforme a prova da proposição 2.25, existe um anel $A \in B$ tal que A é um produto cartesiano de anéis finitamente gerados de B e, ainda mais, W é o conjunto de suas identidades. Portanto, pelo corolário 2.28, $B = \text{var}(A)$, o que implica que B é gerada pela classe de seus anéis finitamente gerados.

COROLÁRIO 2.34 - *Toda variedade de anéis B é gerada*

pela classe de seus B -anéis livres $F_n(B)$, para $n=1,2,\dots$.

Demonstração - Do teorema anterior, B é gerada pela classe de seus anéis finitamente gerados.

Por outro lado, se R é um anel em B gerado por um conjunto finito com n elementos, então, conforme a prova do teorema 2.17, R é isomorfo a um anel quociente do B -anel livre $F_n(B)$, donde segue-se a tese. $\square$

COROLÁRIO 2.35 - Toda variedade de anéis B é gerada pelo seu B -anel livre $F_\infty(B)$.

Demonstração - Pelo teorema 2.33, B é gerada pela classe de seus anéis finitamente gerados.

Por outro lado, se R é um anel finitamente gerado de B e F é um anel livre de ponto infinito enumerável, então, existe um epimorfismo $\alpha: F \rightarrow R$; logo, $R \cong F/\ker(\alpha)$. Além disso, indicando por V um conjunto de polinômios que determina B , temos que $V(F) \subseteq \ker(\alpha)$, conseqüentemente, $R \cong \frac{F/V(F)}{\ker(\alpha)/V(F)}$. Assim, R é isomorfo a um anel quociente de $F_\infty(B)$, donde segue-se a tese. $\square$

VARIEDADES GERADAS POR UMA CLASSE FINITA DE ANÉIS FINITOS.

Nesta seção reunimos resultados muito úteis para o que apresentaremos a seguir.

TEOREMA 2.36 - Seja A um anel finito, e seja $B = \text{var}(A)$. Então, para todo inteiro positivo n , o B -anel livre $F_n(B)$ é finito. Mais precisamente,

$$|F_n(B)| \leq |A| |A|^n$$

Demonstração - Seja W o conjunto das identidades de A . Então, pelo corolário 2.30, B é a variedade determinada

por W , e W é o conjunto de suas identidades.

Nestas condições, pelo teorema 2.26, para todo inteiro positivo n , o B -anel livre $F_n(B)$ é isomorfo a um subanel de $A^{A^{(n)}}$, donde segue-se a tese. $\square$

COROLÁRIO 2.37 - *Seja X uma classe finita de anéis finitos, e seja $B = \text{var}(X)$. Então, para todo inteiro positivo n , o B -anel livre $F_n(B)$ é finito.*

Demonstração - Seja A o produto cartesiano dos anéis de X . Então, A é finito e, além disso, é simples verificar que $B = \text{var}(A)$.

Portanto, do teorema anterior, segue-se a tese. $\square$

TEOREMA 2.38 - *Sejam X uma classe finita de anéis finitos, $B = \text{var}(X)$, e R um anel finito em B . Então, $R \in \text{qs}dX$, isto é, R é uma imagem homomorfa de um subanel de um produto direto de um número finito de anéis em X .*

Demonstração - Seja A o produto cartesiano dos anéis de X . Então, A é finito e $B = \text{var}(A)$.

Por outro lado, desde que R é finito, conforme a demonstração do teorema 2.17, existe um inteiro positivo n tal que R é isomorfo a um anel quociente do B -anel livre $F_n(B)$.

Finalmente, conforme a demonstração do teorema 2.36, $F_n(B)$ é isomorfo a um subanel de $A^{A^{(n)}}$; logo, $F_n(B) \in \text{sd}X$ e, portanto, $R \in \text{qs}dX$. $\square$

Para o próximo conceito, lembremos que um anel R diz-se *localmente finito* se todo subanel finitamente gerado de R é finito.

DEFINIÇÃO 2.39 - Dizemos que uma variedade de anéis é *localmente finita* se todos os seus anéis são localmente finitos. Mais geralmente, dizemos que uma variedade de anéis tem a *propriedade P* se todos os seus anéis tem a propriedade P .

TEOREMA 2.40 - *Seja X uma classe finita de anéis finitos, e seja $B = \text{var}(X)$. Então, B é localmente finito.*

Demonstração - Seja R um anel em B , e seja S um subanel finitamente gerado de R . Então, S é um anel em B e, conforme a demonstração do teorema 2.17, existe um inteiro positivo n tal que S é isomorfo a um anel quociente do B -anel livre $F_n(B)$.

Por outro lado, pelo corolário 2.37, $F_n(B)$ é finito; logo, S é finito e, portanto, R é localmente finito, donde resulta que B é localmente finita. $\square$

Dado um anel finito pertencente a uma variedade gerada por um número finito de anéis finitos, o próximo resultado dá propriedades do anel a partir de propriedades dos anéis geradores. Tal resultado faz parte do trabalho de R. L. Kruse [6] e antes de apresentá-lo vamos lembrar alguns conceitos da teoria de anéis que serão utilizados.

Sejam R um anel e M um R -módulo à direita. Dizemos que M é *irredutível* se:

$$(i) \quad MR = \{\sum_i m_i r_i : m_i \in M, r_i \in R\} \neq \{0\};$$

(ii) M não contém submódulo próprio diferente do submódulo nulo. Evidentemente, (i) implica $M \neq \{0\}$.

O *anulador* de um R -módulo à direita M é o conjunto

$$\text{anl}(M) = \{r \in R : mr = 0, \forall m \in M\}.$$

Se $\text{anl}(M) = \{0\}$, M diz-se um R -módulo *fiel*.

Um anel R diz-se *primitivo* se existe um R -módulo fiel irredutível.

Seja R um anel e indiquemos por I o conjunto dos R -módulos irredutíveis. Então, o *radical de Jacobson* de R , que denotaremos por $J(R)$, é o conjunto

$$\cap \{\text{anl}(M) : M \in I\}$$

Se $J(R) = \{0\}$, R diz-se *semi-simples*. Se $I = \emptyset$ fica entendi-

do que $J(R) = R$ e, neste caso, dizemos que R é um *anel radical*.

Um anel R diz-se *simples* se:

(i) $R^2 \neq \{0\}$

(ii) R não contém ideal próprio diferente do ideal nulo. Claramente, (i) implica $R \neq \{0\}$.

Dizemos que um anel R é *artiniano*, ou que satisfaz a *condição de cadeia descendente* (para ideais à direita) se, para toda sequência descendente de ideais à direita.

$$I_1 \supseteq I_2 \supseteq \dots I_k \supseteq \dots$$

existe um inteiro positivo n tal que $I_n = I_{n+1} = I_{n+2} = \dots$.

Finalmente chama-se *fator* de um anel R a qualquer anel de forma S/T , onde S é um subanel de R e T é um ideal de S . O fator diz-se *próprio* a menos que $S=R$ e $T = \{0\}$.

TEOREMA 2.41 - *Sejam X uma classe finita de anéis finitos, $B = \text{var}(X)$, e R um anel finito em B . Nestas condições dados inteiros positivos c, d, e , tem-se que:*

(i) *se a característica de todo anel em X divide c , então, $\text{car}(R)$ divide c ;*

(ii) *se a ordem de todo fator primitivo de todo anel em X divide d então a ordem de todo fator primitivo de R divide d ;*

(iii) *se os fatores nilpotentes de todo anel em X tem expoente menor ou igual a e , então, os fatores nilpotentes de R tem expoente menor ou igual a e .*

Na demonstração serão utilizados certos conceitos e resultados, que passamos a definir e enunciar, semelhantes a alguns bem conhecidos da teoria dos grupos. Não apresentaremos as demonstrações dos resultados, mas podemos obtê-las diretamente por analogia com as demonstrações para grupos, e es

tas podem ser encontradas, por exemplo, no livro de L.H. Jacy Monteiro [5].

Sejam R um anel e $\mathcal{R}$ o conjunto de todos os subanéis de R , ordenado por inclusão.

Dizemos que uma sequência decrescente $(R_i)_{0 \leq i \leq s}$ (com $s \geq 1$) de elementos de $\mathcal{R}$ é uma *sequência normal* de R se:

$$(i) \quad R_0 = R \text{ e } R_s = \{0\};$$

(ii) para todo i , com $0 \leq i \leq s-1$, R_{i+1} é um ideal de R_i .

Representaremos a sequência normal $(R_i)_{0 \leq i \leq s}$ na forma:

$$R_0 = R \supseteq R_1 \supseteq \dots \supseteq R_s = \{0\}$$

ou, simplesmente, por (R_i) . O número s é denominado *comprimento* da sequência normal (R_i) e, para cada i , com $0 \leq i \leq s-1$, R_i/R_{i+1} diz-se um *fator* da sequência normal (R_i) . Se $R_i \neq R_{i+1}$, para $i=0,1,\dots,s-1$, diremos que a sequência normal (R_i) é *estritamente decrescente*.

Seja

$$R'_0 = R \supseteq R'_1 \supseteq \dots \supseteq R'_t = \{0\}$$

uma outra sequência normal do anel R .

Se (R'_j) é uma subsequência (respectivamente, subsequência própria) diremos que a sequência normal (R_i) é *mais fina* (respectivamente, *estritamente mais fina*) do que a sequência (R'_j) , e que (R_i) é um *refinamento* (respectivamente, *refinamento próprio*) de (R'_j) .

Diremos que a sequência normal (R_i) é *equivalente* à sequência normal (R'_j) se:

$$(i) \quad s=t;$$

(ii) existe uma permutação σ de $\{0,1,\dots,s-1\}$ tal que:

$$R_i/R_{i+1} \cong R'_{\sigma(i)}/R'_{\sigma(i)+1},$$

para $i=0,1,\dots,s-1$.

TEOREMA 2.42 (Schreier) - *Duas seqüências normais de um mesmo anel tem refinamentos equivalentes.*

Diz-se que uma seqüência normal estritamente decrescente $(A_i)_{0 \leq i \leq n}$ de um anel R é uma seqüência de composição de R se (A_i) não admite refinamento próprio estritamente decrescente.

TEOREMA 2.43 - *Uma seqüência normal estritamente decrescente de um anel R , não nulo, é uma seqüência de composição de R se, e somente se, nenhum dos seus fatores contém ideal próprio diferente do ideal nulo.*

TEOREMA 2.44 - *Todo anel finito, não nulo, admite uma seqüência de composição.*

TEOREMA 2.45 - (Jordan-Hölder) - *Se um anel R , não nulo, admite uma seqüência de composição, então, duas seqüências de composição de R são equivalentes.*

Se um anel R , não nulo, admite uma seqüência de composição $(A_i)_{0 \leq i \leq n}$, então, o número n é denominado comprimento do anel R , e diremos que A_i/A_{i+1} , para $i=0,1,\dots,n-1$, são os fatores de composição do anel R . Em virtude do teorema de Jordan-Hölder, a noção de comprimento de um anel R não depende da particular seqüência de composição (A_i) considerada em R e, além disso, os fatores de composição de R são determinados de modo único (a menos de isomorfismos).

Continuando com resultados que serão utilizados na demonstração do teorema 2.41, vamos destacar alguns da teoria de anéis.

TEOREMA 2.46 - *Se R é um anel artiniano, então, o radical de Jacobson de R é nilpotente.*

Para uma demonstração deste resultado ver [4, pág.38, teor.1].

TEOREMA 2.47 - *Sejam R um anel e I um ideal de R tal que R/I é nilpotente. Então, $\exp(R/I) \leq \exp(J(R))$.*

Demonstração - O anel $R/J(R)$ é artiniano e semi-simples. Então, pelo teorema de Wedderburn-Artin(ver[4,pág. 40]), deve ser da forma

$$R/J(R) = \bigoplus_{i=1}^n R_i,$$

onde cada R_i , para $i=1,2,\dots,n$, é um ideal de R isomorfo ao anel das transformações lineares de um espaço vetorial de dimensão finita sobre um anel com divisão.

Como cada um destes anéis tem unidade, segue-se que $R/J(R)$ tem unidade, que denotaremos por $\bar{e}$; conseqüentemente, $R/J(R)$ é gerado como ideal por $\bar{e}$. Além disso, desde que, pelo teorema anterior, $J(R)$ é nilpotente, existe um idempotente $e \in R$ tal que $e + J(R) = \bar{e}$ (ver [4, pág.54, prop.3 e prop. 4]).

Nestas condições, R é gerado como ideal pelo conjunto $\{e\} \cup J(R)$. De fato, dado $r \in R$, temos que

$$r + J(R) \in \frac{R}{J(R)} = \frac{R}{J(R)} (e + J(R)) ;$$

logo, existe $s \in R$ tal que:

$$r + J(R) = (s + J(R)) (e + J(R))$$

o que implica $r = s e + t$, para algum $t \in J(R)$.

Por outro lado, como R/I é nilpotente, todo idempotente de R pertence a I. Com efeito, se $n = \exp(R/I)$, dado um idempotente $u \in R$, temos que:

$$I = (u+I)^n = u^n + I = u+I$$

e, assim, $u \in I$. Em particular, $e \in I$; logo, $R = I + J(R)$ e, portanto,

$$\frac{R}{I} = \frac{I+J(R)}{I} \approx \frac{J(R)}{I \cap J(R)},$$

o que implica a tese. $\square$

TEOREMA 2.48 - Sejam R_1 e R_2 anéis finitos, cujos fatores nilpotentes tem expoente menor ou igual a um inteiro positivo e . Então, todo fator nilpotente do produto direto $\prod_{i=1}^2 R_i$ tem expoente menor ou igual a e .

Demonstração - Sejam S um subanel de $\prod_{i=1}^2 R_i$ e T um ideal de S tal que S/T é nilpotente. Como S é finito e, consequentemente, artiniano, pelo teorema anterior, temos que $\exp(S/T) \leq \exp(J(S))$. Basta, então, considerar S um subanel nilpotente de $\prod_{i=1}^2 R_i$, e provar que $\exp(S) \leq e$.

Para isto, sejam p_1 e p_2 as projeções de S em R_1 e R_2 , respectivamente. Então, $S_1 = p_1(S)$ é um fator nilpotente de R_1 , $S_2 = p_2(S)$ é um fator nilpotente de R_2 e, além disso, $S \subseteq \prod_{i=1}^2 S_i$; logo, $\exp(S)$ é menor ou igual ao máximo entre $\exp(S_1)$ e $\exp(S_2)$ e, portanto, $\exp(S) \leq e$. $\square$

COROLÁRIO 2.49 - Seja $\{R_i : 1 \leq i \leq n\}$ uma família finita de anéis finitos, cujos fatores nilpotentes tem expoente menor ou igual a um inteiro positivo e . Então, todo fator nilpotente do produto direto $\prod_{i=1}^n R_i$ tem expoente menor ou igual a e .

Demonstração - A tese segue por indução sobre n , e do teorema anterior. $\square$

Finalmente, estamos em condições de provar o teorema 2.41.

Demonstração do teorema 2.41.

(i) O polinômio cx é uma identidade de todo anel X ; logo, pelo corolário 2.30, cx é também uma identidade de B e, portanto, uma identidade de R , donde resulta que $\text{car}(R) \mid c$.

Observemos que, nesta parte da demonstração, não é necessário que X seja uma classe finita, e nem que seus anéis sejam finitos.

(ii) Seja P um fator primitivo de R . Então, P é um anel finito em B e, portanto, pelo teorema 2.38, temos que $P \cong S/T$, onde S é um subanel de um produto direto $\prod_{i=1}^k S_i$ de um número finito de anéis em X , e T é um ideal de S .

Como S/T é primitivo, segue-se $S/T \neq \{0\}$; logo, $\prod_{i=1}^k S_i$ é um anel finito não nulo e, portanto, pelo teorema 2.44, admite uma sequência de composição. Seja, então,

$$J_0 = \prod_{i=1}^k S_i \supseteq J_1 \supseteq \dots \supseteq J_r = \{0\}$$

uma tal sequência, e provemos que pode ser escolhida de forma tal que os seus fatores são isomorfos a fatores de composição dos anéis S_i , $1 \leq i \leq k$.

Para isto basta observarmos que, para cada $i=1,2,\dots,k$, S_i é um anel finito que pode ser considerado não nulo; logo, pelo teorema 2.44, admite uma sequência de composição

$$J_{i0} = S_i \supseteq J_{i1} \supseteq \dots \supseteq J_{ir_i} = \{0\}$$

Então, a sequência,

$$\pi S_{\ell}^k = \pi S_{\ell}^{k-1} \times J_{k0} \supseteq \pi S_{\ell}^{k-1} \times J_{k1} \supseteq \dots \supseteq \pi S_{\ell}^{k-1} \times J_{kr_k} \supseteq$$

$$\supseteq \pi S_{\ell}^{k-2} \times J_{k-1,0} \times J_{kr_k} \supseteq \pi S_{\ell}^{k-2} \times J_{k-1,1} \times J_{kr_k} \supseteq \dots \supseteq \pi S_{\ell}^{k-2} \times$$

$$\times J_{k-1,r_{k-1}} \times J_{kr_k} \supseteq \dots \supseteq J_{10} \times \pi J_{\ell r_{\ell}}^k \supseteq J_{11} \times \pi J_{\ell r_{\ell}}^k \supseteq$$

$$\supseteq \dots \supseteq \pi J_{\ell r_{\ell}}^k = \{0\}$$

é uma sequência de composição de πS_i^k com a propriedade desejada, uma vez que:

$$\frac{\pi S_{\ell}^j \times J_{j+1,i}}{\pi S_{\ell}^j \times J_{j+1,i+1}} \cong \frac{J_{j+1,i}}{J_{j+1,i+1}},$$

para $j = 1, 2, \dots, k-1$ e $i = 0, 1, \dots, r_{j+1}-1$.

Consideremos, agora, as sequências normais de S

$$J_0 \cap S = S \supseteq J_1 \cap S \supseteq \dots \supseteq J_r \cap S = \{0\} \text{ e } S \supseteq T \supseteq \{0\}$$

Pelo teorema de Schreier estas sequências admitem refinamentos equivalentes. Então, observando que S/T é simples, pois é isomorfo a P que é finito primitivo (ver[4 pág. 39, teor.1]), seja

$$\begin{aligned} J_0 nS &= S \supseteq J_1 nS \supseteq \dots \supseteq J_i nS = F_{i0} \supseteq F_{i1} \supseteq \dots \supseteq F_{in_i} = \\ &= J_{i+1} nS \supseteq \dots \supseteq J_r nS = \{0\} \end{aligned}$$

um refinamento de $(J_i nS)_{0 \leq i \leq r}$ tal que

$$\frac{S}{T} \approx \frac{F_{ij}}{F_{i,j+1}},$$

para algum i , $0 \leq i \leq r$, e algum j , $0 \leq j \leq n_i - 1$.

Fazendo, $P_1 = F_{ij}/F_{i,j+1}$, $P_2 = (J_i nS)/(J_{i+1} nS)$, e

$P_3 = J_i/J_{i+1}$, provemos que $|P_1|$ divide $|P_2|$, que $|P_2|$ divide $|P_3|$, e que $|P_3|$ divide d , donde seguirá a tese.

Como $J_i nS \supseteq F_{ij} \supseteq F_{i,j+1} \supseteq J_{i+1} nS$, temos que

$$\left| \frac{J_i nS}{J_{i+1} nS} \right| = \left| \frac{J_i nS}{F_{ij}} \right| \left| \frac{F_{ij}}{F_{i,j+1}} \right| \left| \frac{F_{i,j+1}}{J_{i+1} nS} \right|$$

e, portanto, $|P_1|$ divide $|P_2|$.

Considerando agora o homomorfismo $\phi: J_i nS \rightarrow J_i/J_{i+1}$ definido por

$$\phi(r) = r + J_{i+1}, \quad \forall r \in J_i nS,$$

temos que $\ker(\phi) = J_{i+1} nS$; logo, $P_2 \cong \phi(J_i nS)$. Desta forma, P_2 é isomorfo a um subanel de P_3 e, portanto, $|P_2|$ divide $|P_3|$.

Finalmente, para provarmos que $|P_3|$ divide d , observemos que P_3 é fator de uma sequência de composição e, portanto, pelo teorema 2.43, não contém ideal próprio diferente do ideal nulo. Além disso, $P_3^2 \neq \{0\}$. Com efeito, se $P_3^2 = \{0\}$, então, $P_2^2 = \{0\}$, uma vez que, como foi visto, P_2 é isomorfo

a um subanel de P_3 . Nestas condições, $(J_i \cap S)^2 \subseteq J_{i+1} \cap S$; logo

$$(F_{ij})^2 \subseteq (J_i \cap S)^2 \subseteq J_{i+1} \cap S \subseteq F_{i,j+1}$$

e, portanto, $P_1^2 = \{0\}$; uma contradição, pois P_1 é simples, já que é isomorfo a P . Assim, P_3 é um anel finito simples; consequentemente, primitivo (ver [4, pág.39, teor.1]). Além disso, pela construção da sequência (J_i) , é isomorfo a um fator de algum anel de X ; logo, por hipótese, $|P_3|$ divide d .

(iii) Pelo teorema 2.38, R é uma imagem homomorfa de um subanel S de um produto direto $\prod_{i=1}^n R_i$ de um número finito de anéis em X .

Além disso, por hipótese, os fatores nilpotentes de R_i , $1 \leq i \leq n$, tem expoente menor ou igual a e .

Portanto, pelo corolário 2.49 todo fator nilpotente de S tem expoente menor ou igual a e .

Finalmente, como todo fator de R é isomorfo a um fator de S , segue-se a tese. $\square$

OS ANÉIS n -GERADOS E AS IDENTIDADES EM n INDETERMINADAS DE UMA VARIEDADE.

Um anel diz-se n -gerado, para algum inteiro positivo n , se contém um conjunto de geradores com no máximo n elementos.

DEFINIÇÃO 2.50 - Dados um inteiro positivo n e uma variedade de anéis B , denotaremos por $B^{(n)}$ a variedade de anéis determinada pelo conjunto das identidades de B que envolvem no máximo n indeterminadas.

PROPOSIÇÃO 2.51 - Sejam B uma variedade de anéis, W

o conjunto de suas identidades, e n um inteiro positivo. Então, B é uma subvariedade de $B^{(n)}$, e $B^{(n)}$ é a variedade determinada por $W_n = W(\mathbb{Z}[x_1, x_2, \dots, x_n])$.

Demonstração - É imediato que B é uma subvariedade de $B^{(n)}$.

Para a segunda parte, basta observar que os polinômios de W_n são identidades de $B^{(n)}$ e que, além disso, toda identidade de B que envolve no máximo n indeterminadas é uma consequência de W_n . $\square$

LEMA 2.52 - Sejam B uma variedade de anéis, W o conjunto de suas identidades, e n um inteiro positivo. Então, um anel n -gerado R pertence a B se, e somente se, os polinômios de $W_n = W(\mathbb{Z}[x_1, x_2, \dots, x_n])$ são identidades de R .

Demonstração - Se R é um anel em B , é imediato que os polinômios de W_n são identidades de R . Em particular, isto ocorre se R é um anel n -gerado.

Para a recíproca, seja R um anel n -gerado. Então, existe um epimorfismo $\alpha: \mathbb{Z}[x_1, x_2, \dots, x_n] \rightarrow R$. Assim, se os polinômios de W_n são identidades de R , temos que $W_n \subseteq \ker(\alpha)$ e, conseqüentemente,

$$R \cong \frac{\mathbb{Z}[x_1, x_2, \dots, x_n]/W_n}{\ker(\alpha)/W_n};$$

logo, R é isomorfo a um anel quociente do B -anel livre $\mathbb{Z}[x_1, x_2, \dots, x_n]/W_n$ e, portanto, $R \in B$. $\square$

TEOREMA 2.53 - Sejam B uma variedade de anéis, W o conjunto de suas identidades, e n um inteiro positivo. Então, um anel R pertence a $B^{(n)}$ se, e somente se, todo subanel

n -gerado de R pertence a B .

Demonstração - Se R é um anel em $B^{(n)}$, e S é um subanel qualquer de R , então, os polinômios de $W_n = W(\mathbb{Z}[x_1, x_2, \dots, x_n])$ são identidades de S . Em particular, isto ocorre se S é n -gerado e, neste caso, pelo lema anterior, $S \in B$.

Para a recíproca, seja R um anel tal que todo subanel n -gerado de R pertence a B . Então, dado um polinômio $f = f(x_1, x_2, \dots, x_m)$, com $m \leq n$, em W_n , e dados elementos quaisquer $r_1, r_2, \dots, r_m$ em R temos que f é uma identidade do subanel de R gerado pelo conjunto $\{r_1, r_2, \dots, r_m\}$; logo $f(r_1, r_2, \dots, r_m) = 0$ e, portanto, $R \in B^{(n)}$. $\square$

O próximo teorema é um passo importante na demonstração do resultado principal e, como o teorema 2.41, também faz parte do trabalho de R.L. Kruse [6].

TEOREMA 2.54 - *Seja R um anel finito, e seja $B = \text{var}(R)$. Então, para todo inteiro positivo n , o conjunto das identidades de $B^{(n)}$ é finitamente baseado.*

Demonstração - Seja W o conjunto das identidades de R . Então, pelo corolário 2.30, B é a variedade determinada por W , e W é o conjunto de suas identidades.

Além disso, dado um inteiro positivo n , pela proposição 2.51, $B^{(n)}$ é a variedade determinada por $W_n = W(\mathbb{Z}[x_1, x_2, \dots, x_n])$; logo, pela proposição 2.9, toda identidade de $B^{(n)}$ é uma consequência de W_n . Provemos, então, que W_n é finitamente baseado.

De fato, como B é gerada por um anel finito, pelo teorema 2.36, o B -anel livre $\mathbb{Z}[x_1, x_2, \dots, x_n]/W_n$ é finito. Assim, W_n é um ideal de índice finito no anel finitamente gerado $\mathbb{Z}[x_1, x_2, \dots, x_n]$; logo, pelo lema 1.6, W_n é finitamente gerado como anel.

Portanto, se $\{f_1, f_2, \dots, f_m\}$ é um conjunto de geradores de W_n , temos que todo polinômio de W_n é uma consequência de $\{f_1, f_2, \dots, f_m\}$, donde resulta que W_n é finitamente baseado. $\square$

CAPÍTULO 3

ANÉIS CRÍTICOS E VARIEDADES DE CROSS

Este capítulo será baseado no trabalho de R.L.Kruse [6]. Introduziremos os conceitos de anel crítico e de variedade de Cross, examinando algumas de suas propriedades fundamentais.

Com isto, já daremos alguns passos para a demonstração do resultado principal.

ANÉIS CRÍTICOS

DEFINIÇÃO 3.1 - Um anel diz-se *crítico* se é finito e não pertence a variedade gerada pelos seus fatores próprios.

EXEMPLO 3.2 - Sejam p um inteiro primo, e k um inteiro positivo. Sejam, ainda, X a classe dos fatores próprios de $\mathbb{Z}_{p^k}$, e $B = \text{var}(X)$. Nestas condições, pelo teorema 2.38, temos que todo anel finito de B pertence a $\text{qsc}X$. Assim, se R é um anel finito em B , $\text{car}(R) < p^k$; logo $\mathbb{Z}_{p^k} \notin B$ e, portanto, é um anel crítico.

A seguir, apresentaremos algumas propriedades dos anéis críticos.

Para a primeira delas, lembremos que um anel diz-se *subdiretamente irredutível* se a intersecção de seus ideais não nulos é diferente de zero.

PROPOSIÇÃO 3.3 - Um anel crítico é subdiretamente irreduzível.

Demonstração - Seja R um anel crítico, e suponhamos que R não é subdiretamente irreduzível. Então, se $\{I_\lambda : \lambda \in \Lambda\}$ é a família dos ideais não nulos de R , temos que $\cap \{I_\lambda : \lambda \in \Lambda\} = \{0\}$; conseqüentemente, o homomorfismo $\phi: R \rightarrow \prod R/I_\lambda$ definido de forma tal que

$$\phi(r) = \phi_r, \quad \forall r \in R, \quad \text{onde} \quad \phi_r(\lambda) = r + I_\lambda, \quad \forall \lambda \in \Lambda$$

é um monomorfismo.

Temos, então, que R é isomorfo a um subanel de $\prod R/I_\lambda$ e, portanto, pertence à variedade gerada pelos seus fatores próprios; uma contradição, pois R é crítico. $\square$

Mostramos a seguir que nem todo anel subdiretamente irreduzível é crítico.

EXEMPLO 3.4 - Sejam K um corpo finito e A uma álgebra sobre K , com base $\{a, b, c\}$ tal que $a^2 = b^2 = c$, e todos os outros produtos dos elementos da base nulos. Nestas condições, o K -subespaço gerado por c

$$Kc = \{kc \in A : k \in K\}$$

é um ideal não nulo de A , e provemos que está contido em todo ideal não nulo de A . De fato, seja $I \neq \{0\}$ um ideal de A , e seja $r = k_1 a + k_2 b + k_3 c \neq 0$ um elemento em I . Se $k_1 \neq 0$, então, para todo $k \in K$, $kk_1^{-1} ar = kc$; logo, $kc \in I$ e, portanto, $Kc \subseteq I$. Por um argumento análogo, podemos provar que isto também ocorre se $k_2 \neq 0$ ou $k_3 \neq 0$.

Assim, se X é o conjunto dos ideais não nulos de A ,

temos que $Kc \subseteq \cap \{I: I \in X\}$ e, portanto, A é um anel subdiretamente irredutível.

Por outro lado, sejam

$$S_1 = \{k_1 a + k_2 c \in A : k_1, k_2 \in K\} \text{ e } S_2 = \{\ell_1 b + \ell_2 c : \ell_1, \ell_2 \in K\}$$

Então, S_1 e S_2 são ideais próprios e, portanto, fatores próprios de A . Além disso, a função $\phi: \prod_{i=1}^2 S_i \rightarrow A$ definida por

$$\phi(k_1 a + k_2 c, \ell_1 b + \ell_2 c) = k_1 a + k_2 c + \ell_1 b + \ell_2 c, \quad \forall k_1, k_2, \ell_1, \ell_2 \in K,$$

é um epimorfismo; logo, $A \in \text{var} \{S_1, S_2\}$ e, conseqüentemente, não é um anel crítico.

Para o que segue, dado um inteiro primo p , diremos que um anel R é um p -anel se o grupo aditivo de R é um p -grupo.

PROPOSIÇÃO 3.5 - *Todo anel crítico é um p -anel para algum primo p .*

Demonstração - Seja R um anel crítico. Se $|R|$ é uma potência de algum primo p , então, é claro que R é um p -anel. Caso contrário, seja $|R| = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$, com $k > 1$, a decomposição de $|R|$ em fatores primos. Então, R^+ é a soma direta de seus p_i -subgrupos de Sylow, para $i=1, 2, \dots, k$.

Por outro lado, se R_i^+ é o p_i -subgrupo de Sylow de R^+ , $1 \leq i \leq k$, provemos que R_i^+ é um ideal de R . De fato, dados $s \in R_i^+$ e $r \in R$, temos que

$$p_i^{n_i}(rs) = r(p_i^{n_i}s) = 0;$$

logo, a ordem de rs como elemento de R^+ , é uma potência de p_i e, conseqüentemente, $rs \in R_i^+$. Analogamente, $sr \in R_i^+$, para quaisquer $s \in R_i^+$ e $r \in R$.

Assim, $R = \bigoplus_{i=1}^k R_i^+$, com $k > 1$, contrariando a hipótese que R é crítico. $\square$

No exemplo 3.4, se $\text{car}(K) = p > 0$, temos que A é um p -anel não crítico.

Ainda ilustraremos este fato com outro exemplo, que será consequência da seguinte:

PROPOSIÇÃO 3.6 - *Todo anel crítico semi-simples é simples.*

Demonstração - Seja R um anel crítico semi-simples. Então, pelo teorema de Wedderburn-Artin (ver [4, pág. 40]), temos que R é da forma

$$R = \bigoplus_{i=1}^n R_i,$$

onde cada R_i , $1 \leq i \leq n$, é um ideal de R isomorfo a um anel simples; logo, como R é crítico, segue-se $n=1$ e, conseqüentemente, R é simples. $\square$

EXEMPLO 3.7 - Seja K um corpo finito de característica $p > 0$, e seja G um grupo finito tal que p não divide $|G|$.

Lembremos que o anel de grupo KG é o anel das funções $\alpha: G \rightarrow K$ com a adição e a multiplicação de dois elementos $\alpha, \beta \in KG$ definidas por:

$$(\alpha + \beta)(g) = \alpha(g) + \beta(g), \quad \forall g \in G,$$

$$(\alpha\beta)(g) = \sum_{uv=g} \alpha(u)\beta(v), \quad \forall g \in G.$$

Nas condições iniciais $|KG| = |K|^{|G|}$ e portanto, KG é um p -anel. Entretanto, se $|G| > 1$, KG não é crítico.

De fato, como p não divide $|G|$, pelo teorema de Maschke (ver [3, pág.26, teor.1.4.1]), KG é um anel semi-simples; logo, pela proposição anterior, se fosse crítico deveria ser simples. Provemos, então, que KG não é um anel simples.

Para isto, seja $\phi: KG \rightarrow K$ a função definida por

$$\phi(\alpha) = \sum_{g \in G} \alpha(g), \quad \forall \alpha \in KG$$

É fácil ver que ϕ é um epimorfismo e, como $|G| > 1$, não é monomorfismo; logo, $\text{Ker}(\phi)$ é um ideal não nulo de KG e, consequentemente, KG não é um anel simples.

Em continuação damos uma condição suficiente para um anel ser crítico.

PROPOSIÇÃO 3.8 - *Todo anel finito simples é crítico.*

Demonstração - Seja R um anel finito simples, e seja B a variedade gerada pelos seus fatores próprios. Então, conforme a demonstração da parte (ii) do teorema 2.41, a ordem dos fatores primitivos de todo anel finito de B é estritamente menor que $|R|$; logo, como R é um anel finito simples e, portanto, primitivo (ver[4, pág.39, teor.1]), temos que $R \notin B$; consequentemente, R é crítico. $\square$

EXEMPLO 3.9 - Seja n um inteiro positivo, e seja D um anel com divisão finito. Então, o anel $M_n(D)$ das matrizes $n \times n$ sobre D é um anel finito simples; logo, pela proposição anterior, é crítico.

Observamos que nem todo anel crítico é simples, como mostra o seguinte:

EXEMPLO 3.10 - Sejam p um inteiro primo e k um inteiro maior ou igual a 2. Então, conforme foi visto no exemplo 3.2, o anel $\mathbb{Z}_{p^k}$ é crítico.

Por outro lado, $2 \cdot \mathbb{Z}_{p^k}$ é um ideal próprio não nulo de $\mathbb{Z}_{p^k}$; logo, $\mathbb{Z}_{p^k}$ não é um anel simples.

Continuando com propriedades dos anéis críticos, daremos a seguir, aquelas que desempenharão um papel importante na demonstração do resultado principal.

TEOREMA 3.11 - *Seja R um anel finito que contém ideais $I_1, I_2, \dots, I_m$ e um subanel S tais que:*

- (i) $R = S + I_1 + I_2 + \dots + I_m$;
- (ii) nenhum subconjunto próprio de $\{I_1, I_2, \dots, I_m\}$ juntamente com S gera R ;
- (iii) $I_{\pi(1)} I_{\pi(2)} \dots I_{\pi(m)} = \{0\}$, para toda permutação π de $\{1, 2, \dots, m\}$.

Nestas condições, R não é crítico.

Para a demonstração consideremos o seguinte:

LEMA 3.12 - *Seja F um anel livre gerado por um conjunto*

$$\{v_{ij} : 1 \leq i \leq k_j ; 0 \leq j \leq m\}$$

e, para cada $j=1,2,\dots,m$, indiquemos por δ_j o endomorfismo de F definido de forma tal que:

$$\delta_j(v_{ij}) = 0, \quad 1 \leq i \leq k_j$$

$$\delta_j(v_{i\ell}) = v_{i\ell}, \quad \ell \neq j ; 1 \leq \ell \leq m ; 1 \leq i \leq k_\ell.$$

Seja, ainda,

$$K = \cap \{Ker(\delta_j) : 1 \leq j \leq m\}$$

Nestas condições, todo elemento $u \in F$ pode ser escrito na forma $u = v + z_1 + z_2 + \dots + z_t$, para algum inteiro $t \geq 0$, onde $v \in K$ e cada elemento z_i , $1 \leq i \leq t$, é da forma $z_i = \pm \beta_i(u)$, onde a função β_i é uma composição de alguns dos δ_j , $1 \leq j \leq m$.

Demonstração - Para cada subconjunto $S \neq \emptyset$ de $\{1,2,\dots,m\}$, definimos $sn(S)$ igual a $+1$ ou -1 conforme o número de elementos em S seja ímpar ou par e β_S igual a função composta de δ_j , para $j \in S$. Observamos que pela definição dos δ_j , $1 \leq j \leq m$, β_S não depende da ordem em que compomos δ_j , para $j \in S$.

Nestas condições, provemos que, para todo $u \in F$,

$$u = v + \sum_S (sn(S)) \beta_S(u) \quad (*),$$

onde a somatória estende-se por todos os subconjuntos $S \neq \emptyset$ de $\{1,2,\dots,m\}$, e v é a soma de todos os monômios de u que envolvem pelo menos um gerador v_{ij} , para todo $j=1,2,\dots,m$.

De fato, seja w um monômio de u , e seja T o subconjunto de $\{1, 2, \dots, m\}$ que contém os segundos índices j dos geradores v_{1j} que aparecem em w . Se $T = \{1, 2, \dots, m\}$, então, w ocorre como termo de v e $\beta_S(w) = 0$, para todo subconjunto $S \neq \emptyset$ de $\{1, 2, \dots, m\}$; logo, w aparece exatamente uma vez no lado direito da expressão (*). Se $T \neq \{1, 2, \dots, m\}$, então, w não ocorre como termo de v e, além disso, w ocorre na expressão $\beta_S(u)$ se, e somente se, S está contido no complementar T^C de T em $\{1, 2, \dots, m\}$. Assim, obtemos que o coeficiente de w no lado direito da expressão (*) é

$$\sum_{\emptyset \neq S \subseteq T^C} s n l S = \binom{n}{1} - \binom{n}{2} + \dots + (-1)^{n-1} \binom{n}{n},$$

onde n é o número de elementos em T^C . Como

$$0 = (1-1)^n = 1 - \left[\binom{n}{1} - \binom{n}{2} + \dots + (-1)^{n-1} \binom{n}{n} \right],$$

segue-se que

$$1 = \binom{n}{1} - \binom{n}{2} + \dots + (-1)^{n-1} \binom{n}{n};$$

logo,

$$\sum_{\emptyset \neq S \subseteq T^C} s n l S = 1$$

e, portanto, a expressão (*) é verificada.

Assim, desde que claramente $v \in K$, segue-se a tese. $\square$

Demonstração do teorema 3.11 - Seja

$$\{u_{i_0} e_S : 1 \leq i \leq k_0\}$$

um conjunto de geradores de S e, para cada $j=1,2,\dots,m$, seja

$$\{u_{ij} \in I_j : 1 \leq i \leq k_j\}$$

um conjunto de geradores de I_j . Seja, ainda, F um anel livre gerado por um conjunto

$$\{v_{ij} : 1 \leq i \leq k_j ; 0 \leq j \leq m\}.$$

Para cada $j=1,2,\dots,m$, indiquemos por δ_j o endomorfismo de F definido como no lema anterior e consideremos

$$K = \cap \{\text{Ker}(\delta_j) : 1 \leq j \leq m\}.$$

Usando o lema, temos que todo elemento $u \in F$ pode ser escrito como $u = v + z_1 + z_2 + \dots + z_t$, para algum inteiro $t \geq 0$, onde $v \in K$ e cada elemento z_i , $1 \leq i \leq t$, é da forma $z_i = \beta_i(u)$, onde a função β_i é uma composição de alguns dos δ_j , $1 \leq j \leq m$.

Finalmente, seja $\alpha: F \rightarrow R$ o homomorfismo definido de forma tal que

$$\alpha(v_{ij}) = u_{ij}, \quad 1 \leq i \leq k_j ; 0 \leq j \leq m.$$

Então, a definição dos β_i , $1 \leq i \leq t$, e a hipótese (ii) implicam que $\alpha(\beta_i(F))$ é um subanel próprio de R .

Consideremos agora o anel

$$A = \prod_{i=1}^t \alpha(\beta_i(F)),$$

e mostremos que existe um epimorfismo de um subanel de A em R .

Seja $\phi: F \rightarrow A$ o homomorfismo definido de forma tal que

$$\phi(u) = \phi_u, \quad \forall u \in F, \text{ onde } \phi_u(i) = \alpha(\beta_i(u)), \quad \forall i, 1 \leq i \leq t.$$

Então, $\text{Ker}(\phi) \subseteq \text{Ker}(\alpha)$.

De fato, dado $u \in \text{Ker}(\phi)$, pelo lema anterior,

$$u = v + z_1 + z_2 + \dots + z_t, \quad \text{onde } z_i = \beta_i(u), \quad 1 \leq i \leq t, \quad \text{e } v \in K.$$

Além disso, como $\phi(u) = 0$, para todo i , $1 \leq i \leq t$, temos que $\alpha(\beta_i(u)) = 0$ e, portanto $\beta_i(u) \in \text{Ker}(\alpha)$.

Por outro lado, como $K = \sum \{\text{Ker}(\delta_j) : 1 \leq j \leq m\}$, todo elemento de K é uma soma de monômios, cada um dos quais envolve pelo menos um gerador v_{ij} , para todo j , $1 \leq j \leq m$.

Assim, desde que $I_1, I_2, \dots, I_m$ são ideais, a hipótese (iii) implica que $K \subseteq \text{Ker}(\alpha)$, portanto, $v \in \text{Ker}(\alpha)$ e, assim, $\text{Ker}(\phi) \subseteq \text{Ker}(\alpha)$.

Disto segue-se que existe um epimorfismo $\rho: \phi(F) \rightarrow R$ tal que $\rho \circ \phi = \alpha$. Para isto basta definirmos

$$\rho(\phi(u)) = \alpha(u), \quad \forall u \in F.$$

Desta forma, R pertence à variedade gerada pelos seus fatores próprios e, portanto, não é crítico. $\square$

COROLÁRIO 3.13 - *Seja R um anel crítico, e seja $e = \exp(J(R))$. Então, o número de componentes simples de $R/J(R)$ é menor que $2e$.*

Demonstração - Suponhamos que $R/J(R)$ tenha m com-

ponentes simples, com $m > 1$, e sejam I_j , $1 \leq j \leq m$, os ideais de R tais que $J(R) \subseteq I_j$ e $I_j/J(R)$ são as componentes simples de $R/J(R)$.

Tomando $S=J(R)$, temos que as hipóteses (i) e (ii) do teorema anterior estão satisfeitas. De fato, dado $r \in R$, existem elementos $r_j \in I_j$, $1 \leq j \leq m$, tais que

$$r + J(R) = r_1 + J(R) + r_2 + J(R) + \dots + r_m + J(R);$$

logo, $r - (r_1 + r_2 + \dots + r_m) \in J(R)$ e, portanto, existe $s \in J(R)$ tal que:

$$r = s + r_1 + r_2 + \dots + r_m$$

Assim, $R = J(R) + I_1 + I_2 + \dots + I_m$, o que verifica (i). Suponhamos agora - reordenando os ideais I_j , $1 \leq j \leq m$, se necessário - que o conjunto $\{I_1, I_2, \dots, I_k\}$, com $k < n$, juntamente com $J(R)$ gera R , e seja $z_{k+1} \in I_{k+1}$ tal que $z_{k+1} \notin J(R)$. Então, existem $w \in J(R)$ e $z_i \in I_i$, $1 \leq i \leq k$, tais que:

$$z_{k+1} = w + z_1 + z_2 + \dots + z_k;$$

logo,

$$z_{k+1} + J(R) = z_1 + J(R) + z_2 + J(R) + \dots + z_k + J(R)$$

e, como $R/J(R)$ é a soma direta dos ideais $I_j/J(R)$, $1 \leq j \leq m$, segue-se que $z_i \in J(R)$, para todo i , $1 \leq i \leq k+1$; uma contradição com o fato de z_{k+1} não pertencer a $J(R)$. Portanto, nenhum subconjunto próprio de $\{I_1, I_2, \dots, I_m\}$ juntamente com $J(R)$ gera R , o que verifica (ii).

Além disso, se $m \geq 2$ e, então, $I_{\Pi(1)} I_{\Pi(2)} \dots I_{\Pi(m)} = \{0\}$, para toda permutação Π de $\{1, 2, \dots, m\}$. Com efeito, co

mo $R/J(R)$ é a soma direta dos ideais $I_j/J(R)$, $1 \leq j \leq m$, temos que $I_k I_\ell \subseteq J(R)$, para $k \neq \ell$ e $1 \leq k, \ell \leq m$; logo indicando por $[m/2]$ o maior inteiro que é menor ou igual a $m/2$, segue-se que

$$I_{\Pi(1)} I_{\Pi(2)} \cdots I_{\Pi(m)} \subseteq (J(R))^{[m/2]} = \{0\}$$

e, portanto, também a hipótese (iii) estaria verificada.

Assim, como R é crítico, devemos ter $m < 2e$. $\square$

A seguir damos algumas propriedades dos anéis nilpotentes, que serão úteis para estabelecermos mais alguns resultados sobre os anéis críticos.

LEMA 3.14 - *Seja R um anel nilpotente, e seja S um subanel de R tal que $R = S + R^2$. Então, $R = S$.*

Demonstração - Como R é nilpotente, existe um inteiro positivo k tal que $R^k = S^k$, e seja n o menor inteiro que satisfaz esta propriedade. Se $n > 1$, então,

$$R^{n-1} = (S + R^2)^{n-1} \subseteq S^{n-1} + R^n = S^{n-1}$$

o que contraria a definição de n ; logo, devemos ter $n=1$. $\square$

PROPOSIÇÃO 3.15 - *Seja R um anel nilpotente, e seja J um ideal maximal de R . Então, $R^2 \subseteq J$.*

Demonstração - Suponhamos que J não contém R^2 . Então como J é maximal, segue-se $R = J + R^2$; logo, pelo lema anterior, temos $R=J$; uma contradição, pois J é maximal. $\square$

PROPOSIÇÃO 3.16 - *Seja R um p-anel nilpotente, pa*

ra algum primo p , e seja J um ideal maximal de R . Então, $pR \subseteq J$.

Demonstração - Pela proposição anterior $R^2 \subseteq J$. Então, o anel $A=R/J$ tem todos os produtos iguais a zero.

Assim, todo subgrupo de A^+ é um ideal de A ; logo, é da forma I/J , onde I é um ideal de R que contém J .

Portanto, como J é maximal, segue-se que A^+ não contém subgrupo próprio diferente do subgrupo nulo; consequentemente, $|A^+|$ é um inteiro primo, e, como R é um p -anel, temos que $|A^+|=p$, donde resulta a tese. $\square$

PROPOSIÇÃO 3.17 - *Seja R um anel nilpotente, e seja S um subanel próprio de R . Então, existe um ideal próprio de R que contém S .*

Demonstração - Seja I o ideal de R gerado por S . Se $R=I$, então, $R=S+R^2$, logo, pelo lema 3.14, temos $R=S$; uma contradição, pois S é próprio. $\square$

TEOREMA 3.18 (Burnside) - *Seja R um p -anel finito nilpotente, para algum primo p , e seja $T=pR+R^2$. Então, $|R/T|=p^n$, para algum inteiro $n \geq 1$, e todo conjunto de geradores de R contém um conjunto com n elementos que também gera R .*

Demonstração - Provemos inicialmente que $|R/T|=p^n$, para algum inteiro $n \geq 1$. De fato, se $R=pR+R^2$, pelo lema 3.14, temos $R=pR$; uma contradição, pois sendo $\text{car}(R)=p^k$, onde k é um inteiro positivo maior ou igual a 1, então, existe $r \in R$ tal que a ordem de r como elemento de R^+ é p^k e, por outro lado, todo elemento de $(pR)^+$ tem ordem menor ou igual a p^{k-1} .

Para a segunda parte consideremos $A=R/T$ como uma álgebra sobre o corpo de p elementos $GF(p)$, e provemos que a dimensão de A sobre $GF(p)$ é igual a n . Com efeito, A^+ é uma soma direta de p -subgrupos cíclicos, cujos geradores formam uma base de A sobre $GF(p)$, e como todo elemento não nulo de A^+ tem ordem p , segue-se que o número de tais geradores deve ser n .

Seja agora, G um conjunto de geradores de R , e seja ϕ o homomorfismo canônico de R em A . Então, $\phi(G)$ é um conjunto de geradores de A , e sejam $r_1, r_2, \dots, r_n$ elementos em G tais que $\{\phi(r_1), \phi(r_2), \dots, \phi(r_n)\}$ é uma base de A .

Suponhamos que o conjunto $\{r_1, r_2, \dots, r_n\}$ gera um subanel próprio de R . Como R é finito, pela proposição 3.17, temos que existe um ideal maximal J de R que contém este subanel. Além disso, pelas proposições 3.15 e 3.16, temos também que $T \subseteq J$.

Assim, $\phi(r_1), \phi(r_2), \dots, \phi(r_n)$ são elementos em J/T ; logo, $J/T=A$ e, conseqüentemente, $R=J$; uma contradição, pois J é maximal. $\square$

PROPOSIÇÃO 3.19 - *Seja R um anel crítico que contém um ideal nilpotente N , um subanel S tal que $R=S+N$, e subanéis $N_1, N_2, \dots, N_m$ de N tais que:*

$$(i) \quad N_j S + S N_j \subseteq N_j, \quad \text{para } 1 \leq j \leq m;$$

$$(ii) \quad R = S + N_1 + N_2 + \dots + N_m;$$

(iii) *nenhum subconjunto próprio de $\{N_1, N_2, \dots, N_m\}$ juntamente com S gera R .*

Então, $m < \exp N$

Demonstração - Para cada $j=1,2,\dots,m$, seja $I_j=N_j+N_j^2$. Então, da hipótese (i), e como $R=S+N$, temos que $I_j, 1 \leq j \leq m$, são ideais de R . Provemos que tais ideais e o subanel S satisfazem as hipóteses (i) e (ii) do teorema 3.11.

De fato,

$$S+I_1+\dots+I_m=S+N_1+N_1^2+\dots+N_m+N_m^2=S+N_1+\dots+N_m+N^2 \supseteq R+N^2=R,$$

o que verifica (i).

Suponhamos agora - reordenando os ideais $I_j, 1 \leq j \leq m$, se necessário - que $R=S+I_1+\dots+I_n$, com $n \leq m$, e seja $T=S+N_1+\dots+N_n$. Então, $R=T+N^2$ e, portanto, para todo $u \in N$, existem $t \in T$ e $v \in N^2$ tais que $u = t+v$. Assim, observando que $t \in T \cap N$, segue-se $N = (T \cap N) + N^2$, donde, pelo lema 3.14, vem que $N = T \cap N$; logo, $N \subseteq T$ e, como $R=T+N^2$, temos $R=T$, o que contradiz a hipótese (iii).

Desta forma, nenhum subconjunto próprio de $\{I_1, I_2, \dots, I_m\}$ juntamente com S gera R , o que verifica (ii) do teorema 3.11.

Além disso, se $m \geq \exp N$, para toda permutação Π de $\{1,2,\dots,m\}$ temos que:

$$I_{\Pi(1)} I_{\Pi(2)} \dots I_{\Pi(m)} = (N_{\Pi(1)} + N^2) (N_{\Pi(2)} + N^2) \dots (N_{\Pi(m)} + N^2) \subseteq N^m \subseteq N^{\exp(N)} = \{0\}$$

e, portanto, também a hipótese (iii) do teorema 3.11 estaria verificada.

Assim, como R é crítico, devemos ter $m < \exp N$. $\square$

Para estabelecermos mais uma propriedade dos anéis críticos, vamos lembrar alguns conceitos e resultados de estrutura de álgebras.

Seja A uma álgebra sobre um corpo K . Então, o radi

cal de Jacobson de A é o radical de Jacobson de A como anel. De acordo com isto, também vamos denotá-lo por $J(A)$.

Como para anéis, dizemos que A é uma *álgebra semi-simples* se $J(A) = \{0\}$, e dizemos que A é uma *álgebra simples* se:

$$(i) A^2 \neq \{0\}$$

(ii) A não contém ideal próprio.

Sendo que aqui, o termo ideal é empregado para subconjuntos que são ideais de A como anel e subálgebras.

Dada uma álgebra A de dimensão finita sobre um corpo K , dizemos que A é uma *álgebra separável* se, para toda extensão E do corpo K , $E \otimes_K A$ é uma álgebra semi-simples sobre E .

Uma condição necessária e suficiente, para que uma álgebra seja separável é dada pelo seguinte:

TEOREMA 3.20 - *Seja A uma álgebra de dimensão finita sobre um corpo K . Então, A é uma álgebra separável se, e somente se, A é uma álgebra semi-simples tal que o centro de cada uma de suas componentes simples é uma extensão separável do corpo K .*

Uma demonstração deste resultado pode ser encontrada em [1, pág.44, teor.21].

Observamos que, se A é uma álgebra finita, semi-simples, sobre $GF(p)$, para algum primo p , então, A é uma álgebra separável. De fato, nestas condições, o centro de cada uma das componentes simples de A é uma extensão finita do corpo finito $GF(p)$; logo é uma extensão separável de $GF(p)$ e,

portanto, pelo teorema anterior, A é uma álgebra separável.

Em continuação enunciaremos um resultado, também relacionado a álgebras separáveis, conhecido como Teorema Principal de Wedderburn, e cuja demonstração pode ser encontrada em [1, pág 47, teor.23].

TEOREMA 3.21 - *Seja A uma álgebra de dimensão finita sobre um corpo K . Se $A/J(A)$ é separável, então, A contém uma subálgebra S tal que*

$$A = S + J(A) \quad e \quad S \cong A/J(A)$$

Finalmente, estamos em condições de provar a seguinte propriedade dos anéis críticos:

PROPOSIÇÃO 3.22 - *Sejam R um p -anel crítico, para algum primo p , $e = \exp(J(R))$, e $p^m = |R/J(R)|$. Então, $J(R)$ contém um conjunto de geradores com cardinalidade menor que $(4e-3)m+e$.*

Demonstração - Sejam $T = pJ(R) + J(R)^2$, e $p^n = |J(R)/T|$. Então, conforme a prova do teorema 3.18, o número mínimo de elementos que geram $J(R)$ é igual a n .

Certamente, $T+pR$ é um ideal de R , e podemos considerar $R/(T+pR)$ como uma álgebra sobre $GF(p)$. Feito isto, temos dois casos possíveis:

$$(1^\circ) \quad \frac{R}{T+pR} = J\left(\frac{R}{T+pR}\right)$$

ou

$$(2^\circ) \quad \frac{R/(T+pR)}{J(R)/(T+pR)} \text{ é uma álgebra separável, pela}$$

observação posterior ao teorema 3.20.

Em ambos os casos existe um subanel $\bar{S}$ de $R/(T+pR)$ tal que

$$\frac{R}{T+pR} = \bar{S} + J\left(\frac{R}{T+pR}\right) \quad \text{e} \quad \bar{S} \cong \frac{R/(T+pR)}{J(R/(T+pR))}$$

De fato, no (1º) basta considerar $\bar{S} = \{0\}$, e no (2º) a existência de $\bar{S}$ é assegurada pelo teorema 3.21.

Observemos que pR é um ideal do p-anel finito R ; logo, pR é um ideal nilpotente e, portanto, $pR \subseteq J(R)$ (ver [4, pág.9, corol.do teor.2]). Como, claramente, $T \subseteq J(R)$, segue-se que $T+pR \subseteq J(R)$ e, assim,

$$J\left(\frac{R}{T+pR}\right) = \frac{J(R)}{T+pR}$$

Seja S o subanel de R tal que $S \supseteq T+pR$ e $\bar{S} = S/(T+pR)$.

Então,

$$\frac{R}{T+pR} = \frac{S}{T+pR} + \frac{J(R)}{T+pR}$$

e, portanto, $R = S + J(R)$. Além disso, temos

$$\frac{S}{T+pR} \cong \frac{R/(T+pR)}{J(R)/(T+pR)} \cong \frac{R}{J(R)},$$

o que implica $|S/(T+pR)| = p^m$.

Por outro lado, também temos

$$\frac{S}{T+pR} \cong \frac{R/(T+pR)}{J(R)/(T+pR)} = \frac{S/(T+pR) + J(R)/(T+pR)}{J(R)/(T+pR)} \cong \frac{S/(T+pR)}{S/(T+pR) \cap J(R)/(T+pR)}$$

donde resulta que $J(R) \cap S = T + pR$.

Para cada $u \in J(R)$, $u \notin T$, seja

$$J(u) = \{nu + s_1u + s_2u + s_3us_4\} + T,$$

onde n percorre o conjunto dos inteiros, e s_1, s_2, s_3, s_4 , percorrem o subanel S . Claramente, $J(u)$ é um subanel de $J(R)$, e $J(u)S + SJ(u) \subseteq J(u)$.

Além disso, pue T e, para quaisquer elementos s_1, s_2 em S , se $s_1 - s_2 \in T + pR$, então, $s_1u - s_2u \in T$. De fato, se $s_1 - s_2 \in T + pR$, então, $s_1 - s_2 = t + pr$, para algum $t \in T$ e algum $r \in R$. Como T é um ideal de $J(R)$, e $pR \subseteq J(R)$, segue-se que

$$s_1u - s_2u = tu + (pr)u \in T + J(R)^2 = T$$

Analogamente, para quaisquer elementos s_1, s_2, s_3 em S , podemos provar que, se $s_1 - s_2 \in T + pR$, então, $us_1 - us_2$, $s_1us_3 - s_2us_3$, e $s_3us_1 - s_3us_2$ são elementos em T .

Portanto, como $|S/(T+pR)| = p^m$, temos que

$$\left| \frac{J(u)}{T} \right| \leq p^m p^m p^m p^m = p^{4m+1}$$

Sejam agora $J_1, J_2, \dots, J_\ell$ subanéis selecionados entre os subanéis $J(u)$ de forma tal que $R = S + J_1 + J_2 + \dots + J_\ell$ e nenhum subconjunto próprio de $\{J_1, J_2, \dots, J_\ell\}$ juntamente com S gera R . Então, valem as hipóteses da proposição 3.19 e consequentemente, $\ell < e$.

Desde que, $R = S + J_1 + J_2 + \dots + J_\ell$ e $J(R) \cap S = T + pR$, temos

$$J(R) = J(R) \cap (S + J_1 + \dots + J_\ell) = (J_1 + \dots + J_\ell) + (J(R) \cap S) = J_1 + \dots + J_\ell + T + pR;$$

logo,

$$p^n = \left| \frac{J(R)}{T} \right| \leq \left| \frac{J_1}{T} \right| \cdot \left| \frac{J_2}{T} \right| \cdots \left| \frac{J_\ell}{T} \right| \left| \frac{pR}{T} \right|$$

e como valem as desigualdades: $m < e$, $|J_i/T| \leq p^{4m+1}$, $1 \leq i \leq \ell$, e $|pR/T| \leq |pR/pJ(R)| \leq |R/J(R)| = p^m$, sendo esta última desigualdade válida para todo grupo abeliano finito, segue-se que:

$$p^n \leq p^{(4m+1)(\ell-1)} p^m$$

e, conseqüentemente

$$n \leq (4m+1)(\ell-1) + r < (4e-3)m + e. \quad \square$$

Em continuação veremos alguns resultados que ilustram o papel dos anéis críticos na construção de variedades.

PROPOSIÇÃO 3.23 - *Se uma variedade B é gerada pelos seus anéis finitos, então, B é gerada pelos seus anéis críticos.*

Demonstração - Seja B' a subvariedade de B gerada pelos anéis críticos de B . Se B' é uma subvariedade própria, então, desde que B é gerada pelos seus anéis finitos, existe um anel finito em B , que não pertence a B' . Seja, então, R um anel finito de ordem mínima tal que $R \in B$ e $R \notin B'$.

Assim, todo fator próprio de R , pertence a B' e, portanto, R é um anel crítico, contrário a definição de B' ; logo, deve ocorrer $B=B'$. $\square$

COROLÁRIO 3.24 - *Seja B' uma subvariedade própria de uma variedade localmente finita B . Então, existe um anel crítico em B que não pertence a B' .*

Demonstração - Como B é localmente finita, todo anel finitamente gerado de B é finito. Assim, pelo teorema 2.23, temos que B é gerada pelos seus anéis finitos; logo, pela proposição anterior, B é gerada pelos seus anéis críticos o que implica a tese. $\square$

PROPOSIÇÃO 3.25 - *Todo anel finito pertence à variedade gerada pelos seus fatores críticos.*

Demonstração - O resultado é verdadeiro para todo anel de ordem prima p , desde que um tal anel é certamente crítico. Procederemos por indução sobre a ordem do anel.

Seja, então, R um anel finito. Se R é crítico o resultado é verdadeiro. Caso contrário, R pertence à variedade gerada pelos seus fatores próprios, os quais, pela hipótese de indução, pertencem à variedade gerada pelos seus fatores críticos.

Como todo fator crítico de um fator de R é isomorfo a um fator crítico de R , segue-se que R pertence à variedade gerada pelos seus fatores críticos. $\square$

VARIEDADES DE CROSS

DEFINIÇÃO 3.26 - Uma variedade de anéis B é chamada uma *variedade de Cross* se:

- (i) B é localmente finita;

(ii) o conjunto das identidades de B é finitamente baseado;

(iii) B tem somente um número finito de anéis críticos não isomorfos dois a dois.

TEOREMA 3.27 - *Toda variedade de Cross é uma variedade gerada por um anel finito.*

Demonstração - Seja B uma variedade de Cross. Então, como B é localmente finita, pelo teorema 2.33, segue-se que B é gerada pelos seus anéis finitos; logo, pela proposição 3.23, B é gerada pelos seus anéis críticos.

Portanto, sendo A o produto direto de representantes de cada uma das classes de isomorfismo dos anéis críticos de B , temos que $B = \text{var}(A)$. Então, como por (iii) da definição 3.26, A é um anel finito, segue-se que B é gerada por um anel finito. $\square$

Vale também a recíproca do teorema anterior, a qual demonstraremos no capítulo seguinte, quando, então, provarmos o resultado principal.

O próximo resultado e o seu corolário desempenharão também um papel muito importante na demonstração do resultado principal.

PROPOSIÇÃO 3.28 - *Toda subvariedade de uma variedade de Cross é uma variedade de Cross.*

Demonstração - Seja B uma variedade de Cross e B' uma subvariedade própria de B . Claramente, B' satisfaz (i) e (iii) da definição 3.26, assim é necessário apenas verificar (ii).

Para isto, seja

$$B_k = B' \subset B_{k-1} \subset \dots \subset B_0 = B$$

uma sequência estritamente decrescente de subvariedades de B . Pelo corolário 3.24, para cada i , $0 \leq i \leq k-1$, existe um anel crítico em B_i que não pertence a B_{i+1} . Assim, por (iii) da definição 3.26, o comprimento k da sequência é limitado e, então, podemos assumir que a sequência não pode ser refinada.

Para cada i , $0 \leq i \leq k$, seja W_i o conjunto das identidades de B_i , e completamos a demonstração por indução sobre k . Se $k=1$, existe um polinômio f em W_1 que não pertence a W_0 , e seja B'' a variedade de anéis determinada por $\{f\} \cup W_0$. Então, como por hipótese, W_0 é finitamente baseado, temos que o conjunto das identidades de B'' é finitamente baseado. Além disso, temos que

$$B_1 = B' \subseteq B'' \subset B_0 = B.$$

Mas a sequência não pode ser refinada; logo, $B' = B''$, e para $k=1$, a prova está completa. Se $k > 1$, basta observar que, pela hipótese de indução, W_{k-1} é finitamente baseado, e repetir o raciocínio anterior para obter que W_k é finitamente baseado. $\square$

COROLÁRIO 3.29 - Se um anel pertence a uma variedade de Cross, então, o conjunto de suas identidades é finitamente baseado.

Demonstração - Sejam B uma variedade de Cross, e R

um anel em B . Então, pela proposição anterior $\text{var}(R)$ é uma variedade de Cross.

Assim, o conjunto das identidades de $\text{var}(R)$ é finitamente baseado. Mas este conjunto, pelo corolário 2.30, é o conjunto das identidades de R . $\square$

CAPÍTULO 4

IDENTIDADES POLINOMIAIS DE CERTOS ANÉIS

Como o capítulo anterior, este também será baseado no trabalho de R.L.Kruse [6] . Provaremos o resultado principal deste nosso trabalho, isto é, que o conjunto das identidades polinomiais de todo anel finito é finitamente baseado, e o estenderemos para o caso de anéis que contem um ideal nilpotente de índice finito.

Apresentaremos, ainda, uma tentativa no sentido de estender um pouco mais este último resultado, e também daremos um exemplo de variedade de Cross, que seguira como consequência de resultados utilizados na prova do resultado principal.

O RESULTADO PRINCIPAL

Dedicaremos esta seção à prova da recíproca do teorema 3.27, que enunciamos como

TEOREMA 4.1 - *Toda variedade gerada por um anel finito é uma variedade de Cross.*

Claramente, o resultado principal é consequência imediata deste teorema e do corolário 3.29.

Apresentaremos a demonstração do teorema 4.1 em

rios passos. Dado um anel finito R , definimos $B = \text{var}(R)$. Em seguida provaremos que, para algum inteiro positivo n , a variedade $B^{(n)}$ determinada pelo conjunto das identidades de B , que envolvem no máximo n indeterminadas, é uma variedade de Cross. Desde que B é uma subvariedade de $B^{(n)}$, o teorema 4.1 seguirá, então, da proposição 3.28.

Já provamos no teorema 2.54, que o conjunto das identidades de $B^{(n)}$ é finitamente baseado; logo, $B^{(n)}$ satisfaz a condição (ii) da definição 3.26. Para verificarmos as condições (i) e (iii), definiremos uma certa classe de anéis, e estabeleceremos três lemas principais, que chamaremos A, B, e C. Tais lemas afirmarão, respectivamente, que $B^{(n)}$ está contida na classe, que a classe satisfaz a condição (i) da definição 3.26, e que a classe satisfaz a condição (iii) da mesma definição.

Assim, após a demonstração destes lemas, a prova do teorema 4.1 estará completa, e com ela a prova do resultado principal.

DEFINIÇÃO 4.2 - Dados inteiros positivos c , d , e e , denotaremos por $C(c,d,e)$ a classe de todos os anéis R tais que:

- (i) $\text{car}(R)$ divide c ;
- (ii) os fatores primitivos de R são anéis finitos cujas ordens dividem d ;
- (iii) os fatores nilpotentes de R tem expoente menor ou igual a e .

Uma propriedade de verificação simples de toda classe da forma $C(c,d,e)$ é dada pela seguinte:

PROPOSIÇÃO 4.3 - $sc(c,d,e) \subseteq C(c,d,e)$, e $qC(c,d,e) \subseteq C(c,d,e)$

A seguir vamos considerar alguns resultados que serão utilizados para estabelecermos o lema A.

LEMA 4.4 - *Todo anel finito pertence a alguma classe da forma $C(c,d,e)$.*

Demonstração - Seja R um anel finito de ordem n. Então, $nr=0$, para todo $r \in R$; logo $\text{car}(R)$ divide n, e tomaremos $c=n$.

Desde que R é finito, temos que os fatores de R são finitos e em número finito. Assim, se $d_1, d_2, \dots, d_m$ são os ordens dos fatores primitivos de R, tomaremos d como sendo o mínimo múltiplo comum entre $d_1, d_2, \dots, d_m$. Finalmente, se $e_1, e_2, \dots, e_k$ são os expoentes dos fatores nilpotentes de R, tomaremos e igual ao máximo entre $e_1, e_2, \dots, e_k$.

Portanto, $R \in C(c,d,e)$. $\square$

Para o que segue lembramos inicialmente os conceitos de produto subcartesiano e produto subdireto de uma família de anéis.

Seja $\{A_\lambda : \lambda \in \Lambda\}$, uma família de anéis, e para cada $\lambda \in \Lambda$, indiquemos por π_λ a projeção do produto cartesiano $\prod A_\lambda$ (produto direto $\prod A_\lambda$) sobre A_λ , isto é,

$$\pi_\lambda(\phi) = \phi(\lambda), \quad \forall \phi \in \prod A_\lambda \quad (\forall \phi \in \prod A_\lambda)$$

Nestas condições, dizemos que um subanel S de $\prod A_\lambda$ ($\prod A_\lambda$) é um produto subcartesiano (produto subdireto) da família $\{A_\lambda : \lambda \in \Lambda\}$ se

$$\pi_{\lambda}(S) = A_{\lambda}, \quad \forall \lambda \in \Lambda$$

Lembramos, também, que um ideal P de um anel R diz-se um *ideal primitivo* se R/P é um anel primitivo. Desde que um anel primitivo é necessariamente não nulo, P é um ideal próprio.

Relacionado a este conceito temos o seguinte teorema, cuja demonstração pode ser encontrada em [4, pág. 4, teor.1]

TEOREMA 4.5 - *O radical de um anel é a intersecção de seus ideais primitivos.*

Assim, se R é um anel semi-simples, e $\{P_{\lambda} : \lambda \in \Lambda\}$ é a família de seus ideais primitivos, então, $\cap \{P_{\lambda} : \lambda \in \Lambda\} = \{0\}$.

Com isto é fácil mostrar o seguinte:

TEOREMA 4.6 - *Todo anel semi-simples é um produto subcartesiano de alguns de seus fatores primitivos.*

Em continuação enunciamos um resultado sobre anéis primitivos com identidade polinomial, que será muito útil na demonstração do lema seguinte.

TEOREMA 4.7 - *Seja R um anel primitivo com uma identidade polinomial de grau d . Então, o centro de R é um corpo e a dimensão de R como uma álgebra sobre o seu centro é menor ou igual a $[d/2]^2$*

Uma demonstração deste resultado pode ser encontrada em [4, pág. 226, teor. 1].

LEMA 4.8 - *Dados inteiros positivos d e e , existe um*

polinômio $f_d(x)$ numa indeterminada x tal que $(f_d(x))^e$ é uma identidade de todo anel cujo radical de Jacobson é nilpotente de expoente menor ou igual a e , e cujos fatores primitivos são anéis finitos de ordens divisores de d . Ainda mais, existe um inteiro positivo a , que depende apenas de d e e tal que, se $(f_d(x))^e$ é uma identidade de um anel R , então, todo fator primitivo de R é um anel finito de ordem divisor de a .

Demonstração - Seja $d = p_1^{n_1} p_2^{n_2} \dots p_t^{n_t}$ a decomposição de d em fatores primos. Para cada i , $1 \leq i \leq t$, existe um inteiro positivo k_i dependendo apenas de $p_i^{n_i}$, tal que $GF(p_i^{k_i})$, o corpo de $p_i^{k_i}$ elementos, contém todas as raízes de todo polinômio de grau no máximo $\sqrt{n_i}$ e coeficientes em qualquer dos corpos finitos $GF(p_i^j)$, $1 \leq j \leq n_i$. Indicando por m_i o maior inteiro que é menor ou igual a $\sqrt{n_i}$, definimos

$$f_d(x) = (x^{p_1^{k_1}} - x)^{m_1} (x^{p_2^{k_2}} - x)^{m_2} \dots (x^{p_t^{k_t}} - x)^{m_t}$$

Inicialmente, provaremos a primeira parte do lema. Seja R um anel cujo radical de Jacobson é nilpotente de expoente menor ou igual a e , e cujos fatores primitivos são anéis finitos de ordens divisores de d . Nestas condições, para provarmos que $(f_d(x))^e$ é uma identidade de R é suficiente mostrarmos que $f_d(x)$ é uma identidade de $R/J(R)$, uma vez que, para todo $r \in R$, se $f_d(r+J(R)) = 0$, então, $f_d(r) \in J(R)$ e, portanto, $(f_d(r))^e = 0$.

Por outro lado, usando o teorema 4.6, temos que $R/J(R)$ é um produto subcartesiano de fatores primitivos de R , os quais, por hipótese, são anéis finitos cujas ordens dividem d .

Assim, é suficiente mostrarmos que, se S é um anel fi

nito primitivo, cuja ordem divide d , então $f_d(x)$ é uma identidade de S .

Desde que S é finito primitivo, temos que S é simples (ver [4, pág. 39, teor.1]). Então, como $|S|$ divide d , segue-se que $|S|$ é uma potência de um primo $p=p_i$, para algum i , com $1 \leq i \leq t$, uma vez que, conforme já foi visto na demonstração da proposição 3.5, todo q -subgrupo de Sylow, para algum primo q , do grupo aditivo de um anel é um ideal do anel. Fazendo, $k_i = k$, $n_i = n$, e $m_i = m$, mostraremos que $(x^{p^k} - x)^m$ é uma identidade de S .

Podemos considerar S o anel das matrizes $r \times r$ sobre o corpo finito $GF(p^j)$, com $1 \leq r \leq m$ e $1 \leq j \leq n$. De fato, como S é finito simples temos que S é isomorfo a um anel de matrizes $r \times r$ sobre um anel com divisão D (ver [4, pág.39, teor. 1]), sendo, neste caso, D um corpo pois é finito (ver [4, pág.183, teor.1]). Assim, se $|S| = p^l$, com $1 \leq l \leq n$, temos que $|D|^{r^2} = p^l$ e, portanto, $|D| = p^j$, para algum inteiro positivo j . Nestas condições, $p^j r^2 = p^l$, o que implica

$$1 \leq r^2 \leq j r^2 = l \leq n \quad \text{e} \quad 1 \leq j \leq j r^2 = l \leq n ;$$

consequentemente,

$$1 \leq r \leq m \quad \text{e} \quad 1 \leq j \leq n.$$

Seja A uma matriz em S , e seja f_A o polinômio característico de A . Então, f_A é um polinômio de grau no máximo m , e coeficientes no corpo $GF(p^j)$, com $1 \leq j \leq n$; logo $GF(p^k)$ contém todas as razões de f_A . Assim, como podemos considerar A uma matriz sobre $GF(p^k)$, temos que existe a forma canônica de Jordan de A sobre $GF(p^k)$, que indicaremos por A' .

A seguir provaremos que $(A'^{p^k} - A')^m = 0$, o que implicará

$$(A^{p^k} - A)^m = 0.$$

Podemos escrever $A' = B + C$, onde B é uma matriz diagonal sobre $GF(p^k)$, C é uma matriz nilpotente, com $C^r = 0$, e $BC = CB$.

Inicialmente, observamos que podemos aplicar o teorema binomial para desenvolver $(B+C)^{p^k}$, e obter:

$$(B+C)^{p^k} = B^{p^k} + C^{p^k}$$

Por outro lado, $x^{p^k} - x$ é uma identidade de $GF(p^k)$, pois $GF(p^k) \setminus \{0\}$ é um grupo multiplicativo de ordem $p^k - 1$; consequentemente, como B é uma matriz diagonal sobre $GF(p^k)$ segue-se

$$B^{p^k} = B$$

Além disso, como

$$r \leq m, \quad r \leq |S| = p^l \leq p^n \leq p^k, \quad \text{e} \quad C^r = 0$$

resulta

$$C^{p^k} = 0 \quad \text{e} \quad C^m = 0$$

Assim,

$$\begin{aligned} (A^{p^k} - A')^m &= ((B+C)^{p^k} - (B+C))^m = (B^{p^k} + C^{p^k} - (B+C))^m = \\ &= (B+0 - (B+C))^m = (-1)^m C^m = 0 \end{aligned}$$

Portanto, $(x^{p^k} - x)^m$ é uma identidade de S , o que completa a prova da primeira parte do lema.

Para a demonstração da segunda parte, seja R um anel tal que $(f_d(x))^e$ é uma identidade de R , e seja p um fator primo

tivo de R . Claramente, $(f_d(x))^e$ é uma identidade de P ; logo, pelo teorema 4.7, e indicando por $Z(P)$ o centro de P , temos que $Z(P)$ é um corpo e P é uma álgebra de dimensão limitada por um inteiro positivo b que depende apenas de grau de $(f_d(x))^e$ portanto, apenas d , e e e . Além disso, como $(f_d(x))^e$ é uma identidade de $Z(P)$, temos que $Z(P)$ é finito, e suponhamos que $|Z(P)| = q^c$, para algum primo q , é um inteiro positivo c .

Por outro lado, $Z(P) \setminus \{0\}$ é um grupo multiplicativo cíclico, e seja r um gerador deste grupo. Então, existe i , $1 \leq i \leq t$, tal que

$$r^{p_i^{k_i}} - r = 0; \text{ logo, } r^{p_i^{k_i} - 1} = 1$$

e, portanto, q^{c-1} divide $p_i^{k_i} - 1$. Com isto, $q^c \leq p_i^{k_i}$; consequentemente, q^c divide $p_i^{k_i}!$

Assim, a segunda parte do lema fica provada se tomarmos $a = (p_1^{k_1!} p_2^{k_2!} \dots p_t^{k_t!})^b$. $\square$

LEMA 4.9 - Sejam e um inteiro positivo, R um anel finito cujos fatores nilpotentes tem expoente menor ou igual a e , e $B = \text{var}(R)$. Então, os fatores nilpotentes de todo anel em $B^{(e)}$ tem expoente menor ou igual a e .

Demonstração - Suponhamos por absurdo que existe um anel em $B^{(e)}$, que admite um fator nilpotente N tal que $N^e \neq \{0\}$. Então, existem elementos $n_1, n_2, \dots, n_e$ em N tais que $n_1 n_2 \dots n_e \neq 0$, e seja S o subanel de N gerado por

$\{n_1, n_2, \dots, n_e\}$. Nestas condições, S é um subanel e -gerado de N , e como $N \in B^{(e)}$, o teorema 2.53 implica que $S \in B$.

Por outro lado, desde que B é gerada por um anel finito, pelo teorema 2.40, B é localmente finita; logo, S é um anel finito nilpotente em B e, então, pela parte (iii) do teorema 2.41, o expoente de S deve ser menor ou igual a e , o que contradiz $n_1 n_2 \dots n_e \neq 0$. $\square$

LEMA A - Sejam R um anel finito, c, d, e e inteiros positivos tais que $R \in C(c, d, e)$, e $B = \text{var}(R)$. Então, existe um inteiro positivo a , que depende apenas de d, e e tal que

$$B^{(e)} \subseteq C(c, a, e)$$

Demonstração - Como $R \in C(c, d, e)$, o polinômio cx é uma identidade de todo anel em B . Portanto, pelo corolário 2.30, cx é uma identidade de B e, portanto, de $B^{(e)}$; logo, a característica de todo anel em $B^{(e)}$ divide c .

Pela primeira parte do lema 4.8, existe um polinômio $f_d(x)$ em uma indeterminada x , tal que $(f_d(x))^e$ é uma identidade de R ; logo, por um raciocínio análogo ao anterior $(f_d(x))^e$ é uma identidade de $B^{(e)}$. Assim, pela segunda parte do mesmo lema, existe um inteiro positivo a , que depende apenas de d, e , tal que os fatores primitivos de todo anel em $B^{(e)}$ são anéis finitos cujas ordens dividem a .

Finalmente, pelo lema anterior, os fatores nilpotentes de todo anel em $B^{(e)}$ tem expoente menor ou igual a e .

Portanto, $B^{(e)} \subseteq C(c, a, e)$. $\square$

Para estabelecermos o lema B, introduzimos a seguir - alguns resultados que serão utilizados na sua demonstração.

Inicialmente lembremos que dado um anel R , então, um elemento $r \in R$, diz-se *quase-regular à direita*, se existe $r' \in R$ tal que $r+r'-rr' = 0$

De acordo com isto, um ideal I de R diz-se *quase-regular* se todo elemento em I é quase-regular à direita.

Relacionado a este conceito temos o seguinte teorema, cuja demonstração pode ser encontrada em [4, pág.9, teor.1(2)]

TEOREMA 4.10 - *O radical de Jacobson de um anel R é um ideal quase-regular que contém todo ideal quase-regular de R .*

Usando este resultado vamos provar o seguinte:

LEMA 4.11 - *Seja R um anel radical e M um R -módulo finitamente gerado. Então, $M=0$.*

Demonstração - Seja $\{m_1, m_2, \dots, m_k\}$ um conjunto de geradores de M . Provaremos, por indução sobre k , que $m_i=0$, para todo i , $1 \leq i \leq k$.

Se $k=1$, então existe $r \in R$ tal que $m_1=m_1r$. Como R é radical, pelo teorema anterior, existe $r' \in R$ tal que

$$r+r' - rr' = 0;$$

logo,

$$0 = m_1r - m_1 = m_1rr' - m_1r' = m_1(rr' - r') = m_1r$$

e, portanto,

$$m_1 = m_1r = 0$$

Se $k > 1$, basta observar que, pela hipótese de indução, o submódulo de M gerado por $\{m_1, m_2, \dots, m_{k-1}\}$ é o submódulo nulo, e repetir o raciocínio anterior para obter $m_k = 0$. $\square$

LEMA 4.12 - Sejam c, t, e e inteiros positivos, e seja R um anel nilpotente de expoente menor ou igual a e , cuja característica divide c , e que contém um conjunto de geradores com t elementos. Então, R é finito de ordem limitada por um inteiro que depende apenas de c, t, e .

Demonstração - Seja $G = \{r_1, r_2, \dots, r_t\}$ um conjunto de geradores de R . Então, R^+ é gerado pela união dos conjuntos

$$G_j = \{r_{i_1} r_{i_2} \dots r_{i_j} : 1 \leq i_1, i_2, \dots, i_j \leq t\}, \quad 1 \leq j \leq e-1$$

Como para cada $j, 1 \leq j \leq e-1$, o número de elementos em G_j é menor ou igual a t^j , temos que R^+ é gerado por um conjunto finito com n elementos tal que

$$n \leq t + t^2 + \dots + t^{e-1}$$

Finalmente, como $\text{car}(R)$ divide c , resulta que

$$|R| \leq c^n \leq c^{t+t^2+\dots+t^{e-1}}. \quad \square$$

LEMA B - Todo anel finitamente gerado em uma classe da forma $C(c, d, e)$ é finito.

Demonstração - Seja R um anel finitamente gerado em $C(c, d, e)$, e provemos inicialmente que $R/J(R)$ é finito.

De fato, pelo teorema 4.5, $J(R)$ é a intersecção dos ideais primitivos de R ; logo, como $REC(c,d,e)$, o índice de tais ideais em R é menor ou igual a d e portanto, pelo lema 1.5, R contém apenas um número finito de ideais primitivos.

Sejam $P_1, P_2, \dots, P_n$, os ideais primitivos de R , e seja $\phi: R \rightarrow \prod_{i=1}^n R/P_i$ o homomorfismo definido de forma tal que

$$\phi(r) = \phi_r, \forall r \in R, \text{ onde } \phi_r(i) = r + P_i, \forall i, 1 \leq i \leq n.$$

Então, como

$$\text{Ker}(\phi) = \cap \{P_i : 1 \leq i \leq n\} = J(R),$$

segue-se que $R/J(R) \cong \phi(R)$; logo, $R/J(R)$ é finito.

Provemos agora que $J(R)$ é finito. Com efeito, pelo lema 1.6, $J(R)$ é finitamente gerado como anel. Além disso, como $REC(c,d,e)$, temos que $(J(R))^e = (J(R))^{e+1}$, pois caso contrário $J(R)/(J(R))^{e+1}$ seria um fator nilpotente de R de expoente $e+1$. Assim, se $\{s_1, s_2, \dots, s_n\}$ é um conjunto de geradores de $J(R)$, então, $(J(R))^e$ é gerado como $J(R)$ -módulo pelo conjunto $\{s_{i_1} s_{i_2} \dots s_{i_e} : 1 \leq i_1, i_2, \dots, i_e \leq n\}$; logo, pelo lema 4.11, $(J(R))^e = \{0\}$.

Temos, então, que $J(R)$ é um anel finitamente gerado, nilpotente e, além disso, como $REC(c,d,e)$, $\text{car}(J(R))$ divide c ; consequentemente, pelo lema 4.12, $J(R)$ é finito.

Desta forma $R/J(R)$ e $J(R)$ são finitos; logo R é finito, donde segue-se a tese. $\square$

LEMA C - Toda classe da forma $C(c,d,e)$ contém apenas

um número finito de anéis críticos não isomorfos dois a dois.

Demonstração - Mostraremos que a ordem de um anel crítico em $C(c,d,e)$ é limitada por um inteiro que depende apenas de c, d, e e e . Com isto o lema estará provado, uma vez que existe apenas um número finito de anéis, não isomorfos dois a dois, de uma dada ordem finita.

Seja R um anel crítico em $C(c,d,e)$. Pelo corolário 3.13, o número de componentes simples de $R/J(R)$ é menor que $2 \exp(J(R))$; logo, menor que $2e$. Além disso, uma componente simples de $R/J(R)$ é um fator primitivo de R ; consequentemente, é finita de ordem menor ou igual a d . Assim,

$$\left| \frac{R}{J(R)} \right| \leq d^{2e-1}$$

Por outro lado, se $|R/J(R)| = p^m$, para algum primo p , então, pela proposição 3.22, $J(R)$ contém um conjunto de geradores com cardinalidade menor que $(4e-3)m+e$. Como, $p^m \leq d^{2e-1}$, temos que $J(R)$ é gerado por um conjunto cuja cardinalidade é limitada por um inteiro que depende apenas de d, e e e . Além disso, como $\exp(J(R)) \leq e$, e $\text{car}(J(R))$ divide c , pelo lema 4.12 temos que $J(R)$ é finito de ordem limitada por um inteiro que depende apenas de c, d, e e e .

Assim, $|R/J(R)|$ e $|J(R)|$ são limitadas por um inteiro que depende apenas de c, d, e e e ; consequentemente, o mesmo ocorre para $|R|$. $\square$

UM EXEMPLO DE VARIEDADE DE CROSS

Nesta seção provaremos que toda classe na forma $C(c,d,e)$ é uma variedade de Cross.

Para isto consideremos inicialmente o seguinte:

LEMA 4.13 - *Seja R um anel finito, e sejam c, d, e e inteiros positivos tais que $REC(c,d,e)$. Então, $var(R) \subseteq C(c,d,e)$.*

Demonstração - Pelo lema A, existe um inteiro positivo a tal que $var(R) \subseteq C(c,a,e)$. Então dado um anel S na $var(R)$ todo fator primitivo P de S é um anel finito primitivo na $var(R)$.

Assim, pela parte (ii) do teorema 2.41, temos que $|P|$ divide d ; logo, se $C(c,d,e)$ e, conseqüentemente, $var(R) \subseteq C(c,d,e)$. $\square$

TEOREMA 4.14 - *Toda classe da forma $C(c,d,e)$ é uma variedade de Cross.*

Demonstração - Seja B a variedade gerada por representantes de cada uma das classes de isomorfismo dos anéis críticos de $C(c,d,e)$. Então, pelo lema C, B é gerada por uma classe finita de anéis finitos de $C(c,d,e)$. Além disso, se A é o produto direto destes anéis, pelo teorema 2.41, temos que $A \in C(c,d,e)$; logo, pelo lema anterior, $var(A) \subseteq C(c,d,e)$.

Mostraremos agora que $C(c,d,e) \subseteq var(A)$. Para isto, seja $REC(c,d,e)$, e provemos que $var(R) \subseteq var(A)$.

Pelo corolário 2.30, se W é conjunto das identidades de R , então, $\tilde{W}$ também é o conjunto das identidades da $var(R)$, e consideremos $\tilde{W} = \mathbb{Z}[X] \setminus W$. Se $\tilde{W} = \emptyset$, então, $R = \{0\}$, e claramente $var(R) \subseteq var(A)$. Caso contrário, para cada $f = f(x_1, x_2, \dots, x_n) \in \tilde{W}$

existem elementos $r_1^f, r_2^f, \dots, r_n^f$ em R tais que $f(r_1^f, r_2^f, \dots, r_n^f) \neq 0$.

Seja S_f o subanel de R gerado pelos elementos $r_1^f, r_2^f, \dots, r_n^f$, e seja $S = c \cap S_f$. Então, é claro que $S \in \text{var}(R)$ e, portanto, os polinômios de W são identidades de S . Além disso, se $f \in \tilde{W}$, então, f não é uma identidade de S_f e, portanto, pela proposição 2.19, também não é uma identidade de S . Assim, o conjunto das identidades de S é W ; logo, pelo corolário 2.28, $\text{var}(R) = \text{var}(S)$. Então, se provarmos que todo subanel finitamente gerado de R pertence a $\text{var}(A)$, resultará que $\text{var}(R) \subseteq \text{var}(A)$.

Seja T um subanel finitamente gerado de R ; a proposição 4.3, implica que $T \in C(c, d, e)$ e, portanto, pelo lema B, T é um anel finito. Assim, da proposição 3.25, resulta que T pertence à variedade gerada pelos seus fatores críticos, os quais, pela proposição 4.3, são anéis em $C(c, d, e)$; logo, são anéis críticos de $C(c, d, e)$ e, conseqüentemente, $T \in \text{var}(A)$.

Desta forma, $C(c, d, e) = \text{var}(A)$ e, portanto, pelo teorema 4.1, $C(c, d, e)$ é uma variedade de Cross. $\square$

UMA EXTENSÃO DO RESULTADO PRINCIPAL

Se P_1 e P_2 são propriedades referentes a anéis, então, um anel R diz-se P_1 -por- P_2 se contém um ideal I com a propriedade P_1 tal que R/I tem a propriedade P_2 .

Nesta seção provaremos o teorema 2, o qual, na terminologia anterior, afirma que o conjunto das identidades de todo anel nilpotente-por-finito é finitamente baseado.

Iniciamos a demonstração com alguns resultados auxiliares.

LEMA 4.15 - *Seja R um anel nilpotente-por-finito finitamente gerado. Então, R^+ é finitamente gerado.*

Demonstração - Seja N um ideal nilpotente de R tal que R/N é finito. Então, pelo lema 1.6, N é finitamente gerado como anel.

Além disso, desde que N é nilpotente, segue-se, conforme a prova do lema 4.12, que N^+ é finitamente gerado.

Portanto, como R/N é finito, temos que R^+ é finitamente gerado. $\square$

Um anel R diz-se *residualmente finito* se, para todo $r \in R$, $r \neq 0$, existe um ideal $I(r)$ tal que $r \notin I(r)$ e $R/I(r)$ é finito.

PROPOSIÇÃO 4.16 - *Um anel é residualmente finito se, e somente se, é isomorfo a um produto subcartesiano de anéis finitos.*

Demonstração - Seja R um anel residualmente finito e, para cada $r \in R$, $r \neq 0$, seja $I(r)$ um ideal tal que $r \notin I(r)$ e $R/I(r)$ é finito. Seja, ainda, $\phi: R \rightarrow \prod R/I(r)$ o homomorfismo definido de forma tal que

$$\phi(r) = \phi_r, \quad \forall r \in R, \quad \text{onde} \quad \phi_r(u) = u + I(r), \quad \forall u \in R.$$

Nestas condições,

$$\text{Ker}(\phi) = \cap \{I(r) : r \in R\} = \{0\};$$

logo, ϕ é um monomorfismo e, portanto, $R \cong \phi(R)$. Além disto, se π_r é a projeção de $\prod R/I(r)$ sobre $R/I(r)$, então para todo

$u \in R$, $u + I(r) = \pi_r(\phi(u))$ logo, $\pi_r(\phi(R)) = R/I(r)$ e, consequentemente, $\phi(R)$ é um produto subcartesiano da família de anéis finitos $\{R/I(r) : r \in R\}$.

Para a recíproca, seja R um anel isomorfo a um produto subcartesiano S de uma família de anéis finitos $\{S_\lambda : \lambda \in \Lambda\}$. Então, dado $\psi \in S$, $\psi \neq 0$, existe $\lambda \in \Lambda$ tal que $\psi(\lambda) \neq 0$. Assim, se π_λ é a projeção de $c\pi S_\lambda$ sobre S_λ , temos que $\psi \notin \text{Ker}(\pi_\lambda)$. Além disso, como $\pi_\lambda(S) = S_\lambda$, segue-se que $S/\text{Ker}(\pi_\lambda) \cong S_\lambda$; logo, $S/\text{Ker}(\pi_\lambda)$ é finito e, portanto, S é residualmente finito, donde resulta que R é residualmente finito. $\square$

PROPOSIÇÃO 4.17 - *Seja R um anel nilpotente-por-finito finitamente gerado. Então, R é residualmente finito.*

Demonstração - Pelo lema 4.15, R^+ é finitamente gerado; logo,

$$R^+ = S_1 \oplus \dots \oplus S_k \oplus T_1 \oplus \dots \oplus T_\ell, (*)$$

onde para cada i , $1 \leq i \leq k$, S_i é um subgrupo cíclico finito e, para cada j , $1 \leq j \leq \ell$, T_j é um subgrupo cíclico infinito.

Com isto, é fácil verificar que, para cada inteiro positivo m , temos

$$\left(\frac{R}{mR}\right)^+ \cong \frac{S_1}{mS_1} \times \dots \times \frac{S_k}{mS_k} \times \frac{T_1}{mT_1} \times \dots \times \frac{T_\ell}{mT_\ell},$$

donde segue que R/mR é finito.

Por outro lado,

$$n\{mR : m = 1, 2, \dots\} = \{0\}.$$

De fato, se n é o mínimo múltiplo comum entre as ordens dos subgrupos S_i , $1 \leq i \leq k$, então,

$$(nR)^+ = nT_1 \oplus \dots \oplus nT_\ell$$

Assim, se $r \neq 0$ é um elemento pertencente a $\hat{n}\{mR: m=1,2,\dots\}$, e se $t_1, t_2, \dots, t_\ell$ são os geradores dos grupos cíclicos T_j , $1 \leq j \leq \ell$, então, existem inteiros positivos $n_1, n_2, \dots, n_\ell$ tais que

$$r = n n_1 t_1 + \dots + n n_\ell t_\ell,$$

e seja c um inteiro positivo tal que c não divide $n n_j$, para algum j , $1 \leq j \leq \ell$.

Desde que $r \in (cR)^+$, existem inteiros positivos $m_1, m_2, \dots, m_\ell$, tais que

$$r = c m_1 t_1 + \dots + c m_\ell t_\ell ;$$

logo como a soma em (*) é direta, temos que $n n_j t_j = c m_j t_j$, donde segue $n n_j = c m_j$, pois a ordem de t_j como elemento de T_j é infinita. Assim, c divide $n n_j$; uma contradição.

Portanto, o homomorfismo $\phi: R \rightarrow c\pi R/mR$ definido de forma tal que

$\phi(r) = \phi_r$, $\forall r \in R$, onde $\phi_r(m) = r + mR$, $\forall m$, $m=1,2,\dots$, é um monomorfismo e, conseqüentemente, temos que $R \cong \phi(R)$. Além disto, para todo $m=1,2,\dots$, se π_m é a projeção de $c\pi R/mR$ sobre R/mR , então, $\pi_m(\phi(R)) = R/mR$.

Disto segue que R é isomorfo a um produto subcartesiano de anéis finitos; logo, pela proposição anterior é re-

sidualmente finito. $\square$

Para os próximos resultados, seja $p=p(x_1, x_2, \dots, x_n)$ um polinômio nas indeterminadas $x_1, x_2, \dots, x_n$. Definamos, para cada inteiro positivo e , um polinômio p_e nas indeterminadas $x_1, x_2, \dots, x_{en}, x_{en+1}, \dots, x_{en+e-1}$ por

$$p_e = p(x_1, \dots, x_n) x_{en+1} p(x_{n+1}, \dots, x_{2n}) x_{en+2} \dots x_{en+e-1} p(x_{(e-1)n+1}, \dots, x_{en})$$

e indiquemos por B_e a variedade de anéis determinada por $\{p_e\}$

PROPOSIÇÃO 4.18 - Se B_1 é gerada por um anel finito, então, para todo inteiro positivo e , existe um inteiro positivo n , que depende unicamente do polinômio p_e , tal que toda subvariedade B' de B_e é gerada pelo seu B' -anel livre $F_n(B')$.

Demonstração - Seja m um inteiro positivo, e consideremos o B_e -anel livre $F=F_m(B_e)$. Seja, ainda, $I=p(F)$, isto é, I é o ideal de F gerado pelo conjunto $\{\alpha(p): \alpha \in \text{Hom}(\mathbb{Z}[X], F)\}$. Então, F/I é um anel finitamente gerado de B_1 e, portanto, pelo teorema 2.40, temos que F/I é finito. Além disso, pela definição de p_e , I é um ideal nilpotente; logo, F é um anel nilpotente-por-finito.

Pelo corolário 2.34, B_e é gerada pelos seus B_e -anéis livres da forma $F_m(B_e)$, para $m=1, 2, \dots$. Portanto, da demonstração da proposição 4.17, vem que B_e é gerada pelos seus anéis finitos. Assim, da proposição 3.23, segue-se que B_e é gerada pelos seus anéis críticos.

Além disto, toda subvariedade de B_e é gerada por uma subclasse desses anéis críticos. De fato, seja B' uma subva-

riedade de B_e , e seja W' o conjunto de suas identidades. Pelo corolário 2.34, B' é gerada pelos seus B' -anéis livres da forma $L/W'(L)$ onde L é um anel livre de posto finito. Como $p_e(L) \subseteq W'(L)$, segue-se que

$$\frac{L}{W'(L)} \cong \frac{L/p_e(L)}{W'(L)/p_e(L)} ;$$

logo, $L/W'(L)$ é uma imagem homomorfa do B_e -anel livre $L/p_e(L) = F_k(B_e)$, onde $k=|L|$. Portanto, desde que $F_k(B_e)$ é nilpotente-por-finito, é simples verificar que $L/W'(L)$ também é nilpotente-por-finito. Assim, B' também é gerada pelos seus anéis críticos, os quais, é claro, formam uma subclasse dos anéis críticos de B_e .

De acordo com isto, resulta que se limitarmos o número de geradores de todo anel crítico de B_e por um inteiro positivo n , que dependa apenas de p_e , teremos completado a demonstração.

Existem inteiros positivos c, d , e b , tais que $B_1 \subseteq C(c, d, b)$, pois B_1 é gerada por um anel finito, e sejam R um anel crítico de B_e , e $I=p(R)$. Então, I é nilpotente de expoente menor ou igual a $2e-1$ e, portanto, $I \subseteq J(R)$ (ver [4, pág. 9, corol. do teor. 2]). Além disso, $J(R)/IEB_1$; logo, $J(R)/IEC(c, d, b)$ e, conseqüentemente, $\exp(J(R)) \leq b(2e-1)$.

Por outro lado, como $R/J(R)$ é isomorfo a um fator de R/I e R/I é um anel em $B_1 \subseteq C(c, d, b)$, segue-se que $R/J(R) \in C(c, d, b)$. Então, a ordem de toda componente simples de $R/J(R)$ é menor ou igual a d e, pelo corolário 3.13, o número de tais componentes é menor ou igual a $2\exp(J(R))$; logo,

$$|R/J(R)| \leq d^{2b(2e-1)},$$

e, portanto, a proposição 3.22, limita o número de geradores de $J(R)$ por um inteiro positivo que depende apenas de c, d, b , e e .

Finalmente, observando que os inteiros c, d, b , e e dependem apenas do polinômio p_e , segue-se que $|R|$ é limitada por um inteiro que depende apenas de p_e . $\square$

PROPOSIÇÃO 4.19 - Se B_1 é gerada por um anel finito, então, para todo inteiro positivo e , o conjunto das identidades de toda subvariedade de B_e é finitamente baseado.

Demonstração - Seja B' uma subvariedade de B_e , e denotemos $B_e = U_0$. Então, U_0 é uma subvariedade de B_e tal que $B' \subseteq U_0$, e o conjunto das identidades de U_0 é finitamente baseado.

Suponhamos que, para $i \geq 0$, seja definida uma subvariedade U_i de B_e que $B' \subseteq U_i$, e o conjunto das identidades de U_i é finitamente baseado. Se $U_i \neq B'$, definimos a subvariedade U_{i+1} de B_e determinada pelos polinômios que determinam U_i junto com um polinômio que é uma identidade de B' mas não é uma identidade de U_i . Assim, se provarmos que B_e satisfaz a condição de cadeia descendente para subvariedades, teremos que existe um inteiro positivo m tal que $U_m = B'$, e disto resultará a tese.

Seja L um anel livre de posto n , onde n é o inteiro positivo obtido na proposição anterior, e consideremos o B_e -anel livre $F = L/p_e(L)$. Seja, ainda,

$$B_e \supseteq U_1 \supseteq \dots \supseteq U_k \supseteq \dots$$

uma cadeia descendente de subvariedades de B_e . Então para cada $i=1, 2, \dots$, indicando por W_i o conjunto das identidades de U_i , temos que $W_i(F) = W_i(L)/p_e(L)$ e, portanto, $F/W_i(F)$ gera U_i , uma vez que $F/W_i(F) = L/W_i(L)$, e pela proposição anterior.

or, $L/W_i(L)$ gera U_i .

Por outro lado,

$$W_1(F) \subseteq W_2(F) \subseteq \dots \subseteq W_k(F) \subseteq \dots$$

é uma cadeia ascendente de ideais de F , e como na prova de proposição anterior, F é um anel nilpotente-por-finito. Então, desde que F é finitamente gerado, temos, pelo lema 4.15, que F^+ é finitamente gerado e, portanto, satisfaz a condição de cadeia ascendente para subgrupos. Assim, existe um inteiro positivo ℓ tal que, $W_\ell(F) = W_{\ell+1}(F) = W_{\ell+2}(F) = \dots$; logo, $F/W_\ell(F) = F/W_{\ell+1}(F) = F/W_{\ell+2}(F) = \dots$ e consequentemente, $B_\ell = B_{\ell+1} = B_{\ell+2} = \dots$. $\square$

Finalmente, segue-se:

Demonstração do teorema 2 - Sejam R um anel, e N um ideal nilpotente de R tal que R/N é finito. Então, se W é o conjunto das identidades de R/N , pelo teorema 4.1, temos que existe um conjunto finito de polinômios W' contido em W tal que todo polinômio de W é uma consequência de W' . Mostraremos que na verdade, existe um polinômio p em W tal que todo polinômio de W é uma consequência de $\{p\}$.

Para verificarmos isto, basta reescrevermos os polinômios de W' de forma tal que as indeterminadas que comparecem em um deles não figuram nos demais, e tomarmos p igual a soma dos polinômios assim obtidos.

Feito isto, usando a notação da proposição anterior, temos que, se $e = \exp(N)$, então, p_e é uma identidade de R , e

$$B_1 = \text{var}(R/N) \subseteq \text{var}(R) \subseteq B_e.$$

Portanto, a tese segue da proposição anterior. $\square$

COROLÁRIO 4.20 - *Sejam U_1 uma variedade nilpotente, e U_2 uma variedade gerada por um anel finito. Então, o conjunto das identidades da variedade U gerada por $U_1 \cup U_2$ é finitamente baseado.*

Demonstração - Sejam W_1 e W_2 os conjuntos das identidades de U_1 e U_2 , respectivamente. Então, $W = W_1 \cap W_2$ é o conjunto das identidades de U .

Por outro lado, se $F = F_\infty(U_1)$ e R é um anel finito tal que $U_2 = \text{var}(R)$, então, pelo corolário 2.35, $U_1 = \text{var}(F)$ e, pelo corolário 2.30, W_1 e W_2 são os conjuntos das identidades de F e R , respectivamente.

Assim, da proposição 2.19, vem que W é conjunto das identidades do produto direto $F \times R$, o qual é um anel nilpotente-por-finito; logo, pelo teorema 2, W é finitamente baseado. $\square$

Uma consequência imediata do teorema 2 é o seguinte:

COROLÁRIO 4.21 - *O conjunto das identidades de todo anel nilpotente é finitamente baseado.*

Entretanto, com o objetivo de darmos uma prova mais construtiva, apresentaremos uma nova demonstração deste resultado independente do teorema 2.

Para isto introduzimos:

DEFINIÇÃO 4.22 - Dizemos que um polinômio f é um *polinômio combinado*, se toda vez que uma indeterminada comparece

em um monômio de f , então, ela comparece em todos os monômios de f .

DEFINIÇÃO 4.23 - Dizemos que um polinômio f é uma *identidade combinada* de um anel R , se f é um polinômio combinado e é uma identidade de R .

PROPOSIÇÃO 4.24 - As identidades de todo anel R são consequência do conjunto das identidades combinadas de R .

Demonstração - Inicialmente, observemos que todo polinômio pode ser escrito como uma soma finita de polinômios combinados. Assim, se f é uma identidade de R , então, $f = f_1 + f_2 + \dots + f_m$, onde $f_1, f_2, \dots, f_m$ são polinômios combinados, e provemos, por indução sobre m , que tais polinômios são identidades de R . Claramente, isto implicará a tese.

Se $m=1$, é imediato que f_1 é uma identidade de R . Se $m>1$, podemos supor que, para cada j , $1 \leq j \leq m-1$, o número de indeterminadas que comparecem em f_j é menor ou igual ao número de indeterminadas que comparecem em f_{j+1} . Então, para cada j , $1 < j \leq m$, temos que existem indeterminadas que comparecem em f_j e não comparecem em f_1 . Assim, fazendo tais indeterminadas iguais a zero, é fácil ver que f_1 é uma identidade de R ; logo,

$$g = f_2 + \dots + f_m = f - f_1$$

também é uma identidade de R e, portanto, pela hipótese de indução, $f_2, f_3, \dots, f_m$ são identidades de R . $\square$

Demonstração do corolário 4.21 - Seja R um anel nilpotente, e seja e um inteiro positivo tal que $e = \exp(R)$. Então, $f = x_1 x_2 \dots x_e$ é uma identidade de R e, além disso, todas as identidades de R , cujos monômios tem grau maior ou igual a e ,

são consequências de $\{f\}$.

Assim, as identidades de R são consequências de $\{f\}$ reunido com o conjunto formado pelas identidades de grau menor ou igual a $e-1$.

Pela proposição anterior, estas são consequências de identidades combinadas de R , as quais, neste caso, envolvem no máximo $e-1$ indeterminadas.

Portanto, as identidades de R são consequências de um ideal I de $F = \mathbb{Z}[x_1, x_2, \dots, x_e]$ tal que $F^e \subseteq I$. Como o anel F/F^e é nilpotente finitamente gerado, segue-se, conforme a prova do lema 4.12, que $(F/F^e)^+$ é finitamente gerado; logo $(I/F^e)^+$ como subgrupo de $(F/F^e)^+$ também é finitamente gerado.

Assim, se $\{f_1 + F^e, f_2 + F^e, \dots, f_n + F^e\}$ é um conjunto de geradores de $(I/F^e)^+$, então, os polinômios de I são consequências de $\{f, f_1, f_2, \dots, f_n\}$. $\square$

Observemos que existem anéis nilpotentes-por-finito que não são nilpotentes, nem finitos, como mostra o seguinte:

EXEMPLO 4.25 - Sejam F um anel finito com unidade, e N um anel nilpotente infinito. Podemos considerar, por exemplo, $F = \mathbb{Z}_2$, e N uma álgebra sobre o corpo dos números reais com base $\{a\}$ tal que $a^2 = 0$. Então, o produto direto $F \times N$ é um anel nilpotente-por-finito, que não é finito, nem nilpotente.

UMA OBSERVAÇÃO FINAL

Encerraremos nosso trabalho observando que, entre as possíveis extensões do teorema 2, poderíamos considerar o caso de um anel R com uma sequência normal

$$R_0 = R \supseteq R_1 \supseteq \dots \supseteq R_n = \{0\}$$

tal que os fatores R_i/R_{i+1} , com $0 \leq i \leq n-1$, são finitos ou nilpotentes.

Entretanto, isto não estenderia o teorema 2, uma vez que um tal anel é nilpotente-por-finito. Para demonstrar este fato começamos provando o seguinte:

LEMA 4.26 - *Seja R um anel primitivo e I um ideal finito, não nulo, de R . Então $R=I$.*

Demonstração - Seja M um R -módulo fiel irredutível. Então, $\Gamma = \text{End}(M_R)$ é um anel com divisão, e M é um espaço vetorial sobre Γ . Assim, pelo teorema da densidade (ver [4, pág. 28 e pág. 31]) temos que R é denso no anel L das transformações lineares do espaço vetorial M sobre Γ em M , isto é, dados $v_1, v_2, \dots, v_n$, vetores linearmente independentes em M sobre Γ , e $w_1, w_2, \dots, w_n$, elementos quaisquer em M , existe $r \in R$ tal que $v_i r = w_i$, para $i=1, 2, \dots, n$. Mas, então, como I é um ideal não nulo, temos também que I é denso em L (ver [4, pág. 33, teor. 4(3)]).

Disto segue que a dimensão de M sobre Γ é finita. De fato, suponhamos que existe um conjunto de vetores $\{u_1, u_2, \dots\}$ linearmente independentes em M sobre Γ e, para cada $k=1, 2, \dots$, seja

$$I_k = \{s \in I : x_i s = 0, \quad 1 \leq i \leq k\}$$

Então, I_k é um ideal à direita de I e, além disso,

$$I_1 \supseteq I_2 \supseteq \dots \supseteq I_k \supseteq \dots \quad (*)$$

Pelo teorema da densidade, para todo $k=1, 2, \dots$, temos

que existe $s_k \in I$ tal que $s_k \in I_k$ e $s_k \notin I_{k+1}$. Portanto, a sequência (*) é estritamente decrescente; uma contradição pois I é finito.

Seja, então, $\{u_1, u_2, \dots, u_m\}$ uma base de M sobre Γ , e seja $r \in R$. Aplicando mais uma vez o teorema da densidade, temos que existe $s \in I$ tal que

$$u_i s = u_i r, \quad \forall i, \quad 1 \leq i \leq m$$

Como M é fiel, segue-se que $r=s$; logo, $r \in I$ e, portanto, $I=R$ $\square$

LEMA 4.26 - Se R é um anel primitivo, então, R não pode ser nilpotente.

Demonstração - Suponhamos, por absurdo, que R é um anel nilpotente, e seja M um R -módulo fiel irredutível. Como $M R^n \neq \{0\}$, devemos ter $\exp(R) = e > 1$, e seja $r \in R$ tal que $r^{e-1} \neq 0$.

Assim, desde que M é irredutível vem que $M r = M$ ou $M r = \{0\}$. Mas, M é fiel e $r \neq 0$; logo, $M r = M$ e, portanto, $M r^{e-1} = 0$, o que é uma contradição pois $r^{e-1} \neq 0$. $\square$

PROPOSIÇÃO 4.27 - Todo anel finito-por-nilpotente é nilpotente-por-finito.

Demonstração - Sejam R um anel e F um ideal finito de R tal que R/F é nilpotente. Se $F=\{0\}$, é imediato que R é um anel nilpotente-por-finito. Faremos a prova por indução sobre $|F|$.

Suponhamos, inicialmente, que $R=J(R)$. Desde que R é finito-por-nilpotente, existe um inteiro positivo e tal que R^e é finito. Então, como qualquer potência de um ideal quase-regular é também um ideal quase regular, segue-se que R^e é um anel radical finito e, portanto, nilpotente. Isto implica que o próprio R é nilpotente e, conseqüentemente, é nilpotente-por-finito.

Suponhamos, agora, que $R \neq J(R)$. Pelo teorema 4.5, R deve conter um ideal primitivo P , e observemos que $F+P \neq P$, pois caso contrário, o anel R/P seria primitivo e nilpotente; uma contradição, como mostra o lema anterior. Temos, então, que $(F+P)/P$ é um ideal finito, não nulo, do anel primitivo R/P ; logo, usando o lema 4.25, vem que $F+P=R$ e, portanto, R/P é finito.

Seja agora, $I=F \cap P$. Então, I é um ideal finito de R e, ainda mais, $|I| < |F|$. De fato, se $|I|=|F|$, então, F é um ideal de P ; logo

$$\frac{R}{P} \cong \frac{R/F}{P/F},$$

o que é uma contradição, pois R/P é primitivo e $(R/F)/(P/F)$ é nilpotente. Além disso, P/I é nilpotente, uma vez que

$$\frac{P}{I} = \frac{P}{P \cap F} \cong \frac{P+F}{F} = \frac{R}{F}$$

Assim, pela hipótese de indução, aplicada ao anel P contendo o ideal finito I tal que P/I é nilpotente, temos que existe um ideal N de P tal que P/N é finito.

Seja, então,

$$J = N + NR + RN + RNR$$

Claramente, J é um ideal de R . Além disso, como N , NR , RN e RNR são ideais nilpotentes de P , segue-se que J é um ideal nilpotente de P e, conseqüentemente, de R .

Finalmente, lembrando que R/P é finito, e observando que P/J é finito, pois

$$\frac{P}{J} \cong \frac{P/N}{J/N},$$

temos que R/J também é finito, uma vez que

$$\frac{R}{P} \cong \frac{R/J}{P/J}$$

Portanto, R é nilpotente-por-finito. $\square$

A recíproca desta proposição é falsa, como mostra o seguinte:

EXEMPLO 4.28 - Seja R uma álgebra sobre um corpo finito K com base $\{v_1, v_2, \dots\}$ tal que

$$v_1 v_j = v_j v_1 = v_j, \text{ para } j = 1, 2, \dots,$$

e todos os outros produtos dos elementos da base nulos. Então, R não é um anel finito-por-nilpotente.

De fato, se J é um ideal de R tal que R/J é nilpotente, então, $v_1 \in J$; logo, também $v_j \in J$, para $j=2, 3, \dots$, e temos $J=R$, donde segue que J não é finito.

Mas, R é nilpotente-por-finito. Com efeito, como espa

ço vetorial, R é a soma direta dos subespaços, Kv_j , para $j=1,2,\dots$. Assim, se considerarmos o subespaço I igual a soma direta dos subespaços Kv_j , para $j=2,3,\dots$, temos que I é um ideal nilpotente de R tal que R/I é finito, uma vez que como espaço vetorial, $R/I \cong Kv_1$.

PROPOSIÇÃO 4.29 - *Seja R um anel com uma sequência normal $(R_i)_{0 \leq i \leq n}$ tal que os fatores R_i/R_{i+1} , com $0 \leq i \leq n-1$, são nilpotentes ou finitos. Então, R é nilpotente-por-finito.*

Demonstração - Faremos a prova por indução sobre n . Se $n=1$, R é nilpotente ou finito, e, claramente, em ambos os casos R é nilpotente-por-finito.

Suponhamos, então, que a proposição vale para todo inteiro n menor ou igual a um certo inteiro $k > 1$, e provemos que também vale para $n=k+1$.

Neste caso, pela hipótese de indução, R_1 é nilpotente-por-finito; logo, R_1 contém um ideal nilpotente N tal que R_1/N é finito. Assim, como na demonstração da proposição anterior, temos que

$$J = N + RN + NR + RNR$$

é um ideal nilpotente de R , e provemos que R/J é finito.

Para isto consideremos a sequência normal

$$R_0 = R \supseteq R_1 \supseteq J \supseteq N \supseteq \{0\}$$

onde, por hipótese, R/R_1 é finito ou nilpotente.

Se R/R_1 é finito, então, $(R/J)/(R_1/J)$ também é finito, pois é isomorfo a R/R_1 . Além disto, como

$$\frac{R_1}{J} \cong \frac{R_1/N}{J/N} \quad \text{e} \quad \frac{R_1}{N} \text{ é finito,}$$

temos que R_1/J é finito; logo, R/J é finito e, portanto, R é nilpotente-por-finito.

Finalmente, se R/R_1 é nilpotente, então, R/J é finito-por-nilpotente, pois R_1/J é um ideal finito de R/J tal que $(R/J)/(R_1/J)$ é nilpotente, uma vez que é isomorfo a R/R_1 . Assim, pela proposição anterior, R/J é nilpotente-por-finito.

Seja, então, I um ideal de R tal que I/J é um ideal nilpotente de R/J com $(R/J)/(I/J)$ finito. Nestas condições, R/I é finito, pois é isomorfo a $(R/J)/(I/J)$, e, além disso, I é nilpotente, uma vez que I/J e J são nilpotentes.

Portanto, R é nilpotente-por-finito. $\square$

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ALBERT, A.A., *"Structure of Algebras"*, Amer. Math.Soc. Colloq. Publ., Vol.24, New York City, 1939.
- [2] COHN, P.M., *"Universal Algebra"*, Harper, New York, 1965.
- [3] HERSTEIN, I.N., *"Noncommutative Rings"*, Math. Assoc. Amer., Carus Monograph, nº15, 1968.
- [4] JACOBSON, N., *"Structure of Rings"*, Amer. Math. Soc. Colloq. Publ., Vol.37, Providence, R.I., 1956.
- [5] JACY MONTEIRO, L.H., *"Elementos de Álgebra"*, Ao Livro Técnico S.A., Rio de Janeiro/Guanabara, 1969.
- [6] KRUSE, R.L., *Identities Satisfied by a Finite Ring*, J. Alg., Vol.26, Nº2, 1973, 298-318.
- [7] KRUSE, R.L., PRICE, D.T., *"Nilpotent Rings"*, Gordon and Breach, New York, London, Paris, 1969.
- [8] LEWIN, J., *"Subrings of Finite Index in Finitely Generated Rings"*, J. Alg. 5, 1967, 84-88.
- [9] NEUMANN, H., *"Varieties of Groups"*, Springer-Verlag, Ergeb. d. Math. B.37, New York, Berlin, 1967.