A N É I S D E H I L B E R T

MATIAS JOSÉ QUADROS NETO

ORIENTADOR

PROF. DR. HU SHENG

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do título de Mestre em Matemática.

Este trabalho foi realizado com o auxílio financeiro da CAPES e da Fundação Universidade Estadual de Londrina.

Julho de 1.979

À Miriam

Alexandre

e Cesar

Agradeço:

Ao Prof. Dr. HU SHENG pela proposta do presente trabalho, por sua atenção e disponibilidade, pela orientação segura e pelo estímulo e encorajamento;

Aos amigos e professores por seus estímulos e ensinamentos;

À CAPES e FUEL que me apoiaram financei.amente na realização deste trabalho.

ÍNDICE

I N T R O D U Ç Ã O

A forma original do Teorema do número de zeros, o HILBERT NULLSTELLENSATZ é que se a polinomial $f(x_1,x_2,\ldots,x_n)$ se anula em todos os zeros de um ideal $I \subset K[x_1,x_2,\ldots,x_n]$ (K corpo) então alguma potência de f está em I. Com base nesse resultado pode se estabelecer uma correspondência biunívoca entre ideais maximais de $K[x_1,x_2,\ldots,x_n]$ e pontos do espaço afim n-dimensional sôbre o fêcho algébrico de K. (A.10)

Usando essa correspondência o HILBERT NULLSTELLENSATZ pode ser reenunciado do seguinte modo: " A intersecção de todos os ideais maximais que contem I é o radical de I". Se considerarmos o anel quociente $K[x_1,x_2,\ldots,x_n]/I$ então é evidente que coincidem os conceitos de radical de Jacobson e de nilradical [1]. Assim $K[x_1,x_2,\ldots,x_n]$ é um exemplo de uma classe de aneis A tal que em A/I (I um ideal qualquer) as duas noções de radical coincidem. Como veremos posteriormente (secção 3.3) este fato implica no HILBERT NULLSTELLENSATZ [2]. Se A é um anel arbitrário desta classe, e desde que o radical dum ideal I de A é a intersecção dos ideais primos que o contem, é evidente que todo ideal primo de A é uma intersecção de ideais maximais de A.

(1) Por esse motivo alguns autores [2] denominam os anéis no qual essa propriedade vale de ANEL DE JACOBSON.

(2) Por esta razão tais anéis são chamados ANÉIS DE HILBERT.

Passamos agora a fazer rápidos comentários a respeito do conteudo de cada capítulo deste trabalho:

CAPÍTULO 1: Foram colocados neste capítulo quase todos os resultados necessários ao desenvolvimento do texto. Entre êles constam resultados referentes a anéis e ideais, anéis de polinômios e séries formais, dependência integral, corpos e anéis noetherianos.

CAPÍTULO 2: Consiste de dois paragrafos.

G-DOMÍNIOS: Observando que um ideal maximal de $K[x_1, x_2, \ldots, x_n]$ (K corpo) tem contração nula em K, isto é, $M \cap K = (0)$ se M é o ideal maximal em questão, consideraremos todos os domínios A tal que vale igual resultado(2.1.15). Em honra a OSCAR GOLDMAN tais domínios são chamados G-DOMÍNIOS. São apresentados vários exemplos de G-domínios, bem como várias condições equivalentes. São estudadas as extensões de G-domínios bem como as relações com os anéis de polinômios correspondentes.

G-IDEAIS: São estudados os ideais dum anel A que são contrações de ideais maximais de $A[x]$. Esses ideais são chamados G-IDEAIS e observamos que o quociente A/I é um G-domínio. À luz do novo conceito reformulamos o teorema de Krull sobre o nilradical.

CAPÍTULO 3: Consiste de 3 parágrafos.

ANÉIS DE HILBERT: Neste trabalho definimos anel de HILBERT como aquele em que todo G-IDEAL é maximal. Provamos no decorrer da secção a equivalência entre nossa definição e a original de Goldman. Encerramos o parágrafo com a demonstração de que o anel das séries formais não é um anel de Hilbert.

ANÉIS DE HILBERT NOETHERIANOS: Examinamos quando um anel noetheriano é um anel de Hilbert. A ferramenta básica é o Teorema do Ideal Principal de Krull.

HILBERT NULLSTELLENSATZ: Este parágrafo é dedicado a este problema tradicional.

APÊNDICE: Tratamos de alguns temas elementares da Geometria Algébrica, fundamentalmente as versões geométricas do HILBERT NULLSTELLENSATZ e o corolário A.10 sobre a correspondência entre ideais maximais de $K[x_1,x_2,\ldots,x_n]$ onde K é um corpo algebricamente fechado, e pontos de K^n.

CAPÍTULO I

PRELIMINARES

Muito embora neste trabalho suponhamos um conhecimento da teoria dos ANÉIS, CORPOS, MÓDULOS e ALGEBRAS, daremos neste capítulo algumas definições e enunciaremos alguns resultados necessários ao desenvolvimento dos capítulos seguintes, cujas demonstrações são encontradas segundo as referências indicadas.

1.1 ANÉIS E IDEAIS

1.1.1 DEFINIÇÃO

Sob a designação ANEL entenderemos um anel comutativo com elemento unidade, isto é, $(A,+,.)$ é um anel se:

i) $(A,+)$ é um grupo abeliano;

ii) $(A,.)$ é um semi-grupo comutativo com elemento unidade; e

iii) $a(b + c) = ab + ac$ para todo $a,b,c \in A$.

1.1.2 DEFINIÇÃO

O anel A é um DOMÍNIO (ou anel de integridade) se, e somente se, vale a seguinte regra:

$$\forall\ a,b,c \in A,\ ab = ac \Leftrightarrow b = c$$

1.1.3 DEFINIÇÃO

Um subconjunto I do anel A é um IDEAL de A se, e somente se :

i) $\forall\ a,b \in I,\ a - b \in I$

ii) $\forall\ a \in I,\ \forall\ b \in A,\ ab \in I$

1.1.4 DEFINIÇÃO

Um ideal P do anel A é PRIMO se, e somente se:

$$ab \in P \Rightarrow a \in P \text{ ou } b \in P$$

1.1.5 DEFINIÇÃO

Um ideal M do anel A é MAXIMAL se, e somente se para P primo, $M \subset P \subset A \Rightarrow M = P$ ou $M = A$ isto é, não existe nenhum ideal próprio entre M e A.

1.1.6 PROPOSIÇÃO [1]

i) Todo anel não nulo possui ao menos um ideal maximal;

ii) Se I é um ideal próprio do anel A então existe um ideal maximal M que contem I.

1.1.7 PROPOSIÇÃO [1]

i) Sejam $P_1, P_2, \ldots, P_n$ ideais primos e I um ideal tal que $I \subset \cup P_i$ $(i = 1,2,\ldots,n)$. Então $I \subset P_i$, para algum i;

ii) Sejam $I_1, I_2, \ldots, I_n$ ideais de A e P um ideal primo de A tal que

$$P \supset \cap I_j \quad (j = 1,2,\ldots,n)$$

então $P \supset I_j$ para algum j.

1.1.8 DEFINIÇÃO

Seja A um anel. O NILRADICAL de A é o conjunto

$$N(A) = \{x \in A \mid \exists\, n \in N \text{ com } x^n = 0\}$$

1.1.9 PROPOSIÇÃO [1]

Se A é um anel então N(A) é um ideal de A igual a intersecção de todos os ideais primos de A.

1.1.10 DEFINIÇÃO

Seja A um anel. O RADICAL de JACOBSON de A (J(A)) é a intersecção de todos os ideais maximais de A.

1.1.11 PROPOSIÇÃO [1]

$x \in J(A)$ se, e somente se $1 - xy$ é unidade de A para todo $y \in A$.

1.1.12 DEFINIÇÃO

Seja I um ideal de A. O RADICAL de I é o conjunto

$$r(I) = \{x \in A \mid \exists\, n \in \mathbb{N} \text{ com } x^n \in I\}$$

1.1.13 COROLÁRIO

Se A é um anel, I um ideal de A então:

$$r(I) = N(A/I) = \cap P_i$$

onde cada P_i é primo e contem I.

DEMONSTRAÇÃO:

Imediata se considerarmos (1.1.8) e (1.1.12)

1.1.14 DEFINIÇÃO

Sejam A e B anéis. Uma função $\phi: A \to B$ tal que

i) $\phi(a + b) = \phi(a) + \phi(b)$, $\forall\, a,b \in A$

ii) $\phi(ab) = \phi(a)\phi(b)$, $\forall\, a,b \in A$ e

iii) $\phi(1) = 1$

é chamada um HOMOMORFISMO de anéis.

1.1.15 PROPOSIÇÃO [6]

Sejam A e B anéis e $\phi: A \to B$ um homomorfismo sobrejetor com núcleo N. Então existe uma correspondência biunívoca que preserva a ordem entre ideais de B e ideais de A que contem N. Tal correspondência associa ideais primos a ideais primos e ideais maximais a ideais maximais.

1.1.16 DEFINIÇÃO

Um subconjunto S do anel A é um SISTEMA MULTIPLICATIVO FECHADO se, $\forall\, s,t \in S \Rightarrow st \in S$. $(0 \notin S, 1 \in S)$

Exemplos:

1) Se P é um ideal primo de A, então $S = A - P$ é um sistema multiplicativo fechado:

2) Se $x \in A$ não é nilpotente então $\{x^n : n \geq 0 \}$ é um sistema multiplicativo fechado.

1.1.17 PROPOSIÇÃO [7]

Seja A um anel e $S \subset A$ um sistema multiplicativo fechado. Se P é um ideal de A, maximal com respeito a exclusão de S, (isto é, $P \cap S = \phi$ e se $Q \supset P$ então $Q \cap S \neq \phi$) então P é primo.

Observação: Se $S \subset A$ é um sistema multiplicativo fechado e I é um ideal de A tal que $I \cap S = \phi$ então uma aplicação do lema de Zorn nos possibilita "extender" I a um ideal P maximal com respeito a exclusão de S, e consequentemente a um ideal primo.

1.1.18 PROPOSIÇÃO [7]

Seja A um anel, I um ideal de A e $I \subset P$ um ideal primo de A. Então P pode ser "reduzido" a um primo minimal entre todos os ideais primos contendo I.

1.1.19 LEMA

Seja A um anel, P = (p) um ideal primo principal e $J = \bigcap_1^\infty P^n$. Se J = (0) então P é minimal.

DEMONSTRAÇÃO:

Seja Q um ideal primo tal que $Q \subsetneq P$. Então $p \notin Q$.

Afirmamos que $Q \subset J = (0)$. Realmente, se $q \in Q \subset P$ temos $q = pq_1 \in Q$ o que acarreta $q_1 \in Q$, já que $p \notin Q$. Novamente, $q_1 = pq_2$ com $q_2 \in Q$ e assim sucessivamente.

Mas então,

$$q = pq_1 = p^2q_2 = p^3q_3 = \dots = p^nq_n = \dots$$

e portanto $q \in \bigcap_1^\infty P^n = (0)$

1.1.20 DEFINIÇÃO

Sejam: A um anel e $S \subset A$ um sistema multiplicativo fechado. O ANEL DE FRAÇÕES de A por S é o conjunto

$$S^{-1}A = \{\frac{a}{s}, a \in A, s \in S\}$$

munido das operações:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad \text{e}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$ e onde

vale a seguinte relação:

$$\frac{a}{s} = \frac{b}{t} \Leftrightarrow \exists s' \in S \text{ com } s'(at - bs) = 0$$

Com as definições acima pode-se provar que $(S^{-1}A,+,.)$ é um anel comutativo com elemento unidade. Ver [1]

1.1.21 OBSERVAÇÕES

i) Se P é um ideal primo de A e $S = A - P$ então escrevemos A_P ao inves de $S^{-1}A$;

ii) Se A é um domínio e $S = A - \{0\}$ então $S^{-1}A$ é o CORPO de FRAÇÕES de A.

1.1.22 DEFINIÇÃO

O anel A é um ANEL LOCAL se A tem um único ideal maximal.

1.1.23 LEMA

Se P é um ideal primo de A então o anel A_P é local.

DEMONSTRAÇÃO:

Seja $P_P = \{\frac{a}{s}, a \in P \text{ e } s \notin P\}$. Facilmente se verifica que P_P é um ideal de A_P. Se um elemento de A_P não é elemento de P_P então é uma unidade de A_P.

Assim P_P é o único ideal maximal de A_P.

1.1.24 PROPOSIÇÃO

Seja A um anel local com ideal maximal M. Então $a \in A$ é uma unidade de A se, e somente se $a \notin M$.

DEMONSTRAÇÃO:

Imediata, considerando (1.1.22) e (1.1.11)

1.1.25 PROPOSIÇÃO [1]

Seja A um anel e S um sistema multiplicativo fechado de A. Então existe uma correspondência biunívoca entre ideais primos de $S^{-1}A$ e ideais primos de A que não interceptam S.

1.2 ANÉIS DE POLINÔMIOS e o ANEL DAS SÉRIES FORMAIS.

1.2.1 DEFINIÇÃO

Um ideal I do anel A é chamado PRINCIPAL se, e somente se, existe $a \in A$ com

$$I = aA = \{ax \mid x \in A\}$$

Um domínio A chama-se DOMÍNIO PRINCIPAL (P.I.D.) se, e somente se todo ideal de A é principal.

1.2.2 DEFINIÇÃO

Um domínio A é um DOMÍNIO de FATORIZAÇÃO ÚNICA (UFD) (ou tambem ANEL FATORIAL) se, todo elemento não nulo de A, ou é unidade ou pode ser escrito como um produto finito de elementos irredutíveis de A, de modo único.

1.2.3 PROPOSIÇÃO [10]

Se A é um P.I.D. então A é um U.F.D.

1.2.4 PROPOSIÇÃO [6]

Seja A um P.I.D. e $I \neq (0)$ um ideal de A. As seguintes alternativas são equivalentes:

i) I é um ideal primo;

ii) I é um ideal maximal;

iii) $I = pA$, p um elemento irredutível de A.

1.2.5 COROLÁRIO

Seja A um P.I.D. e $L = \{p \in A,\ p \text{ irredutível}\}$. Se L é infinito então $\bigcap_{p \in L} pA = (0)$.

DEMONSTRAÇÃO:

Como A é um P.I.D. temos que A é um U.F.D. Se $x \neq 0$, $x \neq 1$ é elemento de

$$\bigcap_{p \in L} pA$$

então, por um lado x tem um número finito de fatores irredutíveis e por outro todo elemento de L é fator de x, uma contradição

1.2.6 PROPOSIÇÃO [6]

Se K é um corpo então $K[x]$, o anel dos polinômios com coeficientes em K, é um P.I.D.

1.2.7 PROPOSIÇÃO

Se K é um corpo então $K[x]$ tem uma infinidade de ideais primos.

DEMONSTRAÇÃO:

$K[x]$ é um P.I.D. (1.2.6) portanto é um U.F.D. (1.2.3)

Suponha que $p_1K[x]$, $p_2K[x]$, ..., $p_nK[x]$ sejam todos os ideais primos de $K[x]$. Então p_1, p_2, ..., p_n são irredutíveis em $K[x]$ (1.2.4).

Considere $p = p_1p_2 \ldots p_n + 1$. Concluímos que p é irredutível e consequentemente $pK[x]$ é um ideal primo, distinto dos acima citados, uma contradição.

1.2.8 DEFINIÇÃO

Seja A um anel. O ANEL das SÉRIES FORMAIS com coeficiente em A é o conjunto:

$$A[\![x]\!] = \{\sum_0^\infty a_i x^i,\ a_i \in A\}$$

Por questão de conveniência, se

$$f = a_o + a_1x + \ldots + a_nx^n + \ldots$$

é um elemento de $A[\![x]\!]$, escreveremos (ver [11])

$$f = a_f + xf_1$$ onde

$a_f = a_o \in A$ e $f_1 = a_1 + a_2x + \ldots + a_nx^{n-1} + \ldots \in A[\![x]\!]$

1.2.9 PROPOSIÇÃO

Um elemento $f = a_f + xf_1$ de $A[\![x]\!]$ é uma unidade de $A[\![x]\!]$ se, e somente se, a_f é uma unidade de A.

DEMONSTRAÇÃO:

Se f é uma unidade de $A[\![x]\!]$ então existe $g = a_g + xg_1$ em $A[\![x]\!]$ tal que $fg = a_fa_g + x(a_gf_1 + a_fg_1 + xf_1g_1) = 1$ donde $a_fa_g = 1$ e a_f é uma unidade de A.

Por outro lado, suponha que $f = a_f + xf_1$ onde a_f é uma unidade de A. Sem perda de generalidade podemos supor que $a_f = 1$. Assim, $f = 1 + xf_1$.

Seja $b = -xf_1$, isto é, $f = 1 - b$

Como $\sum_0^{\infty} b^i \in A[\![x]\!]$ temos $\sum_0^{\infty} b^i = \sum_0^{\infty} c_i x^i$ com $c_i \in A$.

Para um $n \in \mathbb{N}$ arbitrário, seja:

$$\begin{aligned} f.\sum_0^n c_i x^i &= f.[\sum_0^{\infty} c_i x^i - \sum_{n+1}^{\infty} c_i x^i] \\ &= f.[\sum_0^{\infty} b^i - \sum_{n+1}^{\infty} c_i x^i] \\ &= f.[\sum_0^n b^i + \sum_{n+1}^{\infty} b^i - \sum_{n+1}^{\infty} c_i x^i] \\ &= f.\sum_0^n b^i + f.[\sum_{n+1}^{\infty} b^i - \sum_{n+1}^{\infty} c_i x^i] \\ &= (1 - b)\sum_0^n b^i + f.[\sum_{n+1}^{\infty} b^i - \sum_{n+1}^{\infty} c_i x^i] \\ &= 1 - b^{n+1} + f.[\sum_{n+1}^{\infty} b^i - \sum_{n+1}^{\infty} c_i x^i] \ . \end{aligned}$$

Claramente, o menor expoente de x nesta última expressão é maior que n.

Então, existe $\sum_0^{\infty} c_i x^i \in A[\![x]\!]$ tal que $f.\sum_0^{\infty} c_i x^i = 1$ e portanto f é uma unidade de $A[\![x]\!]$.

1.2.10 LEMA

Se P é um ideal primo de A então

$$P^* = \{ \sum_0^{\infty} a_i x^i \in A[\![x]\!] \ , \ a_i \in P\}$$

é um ideal primo de $A[\![x]\!]$.

DEMONSTRAÇÃO:

Claramente, P^* é um ideal de $A[\![x]\!]$. Se $f,g \in A[\![x]\!]$ tal que $fg \in P^*$ e $f \notin P^*$ e $g \notin P^*$. Então existem $j,k \in \mathbb{N}$ tal que se $f = \sum_0^{\infty} a_i x^i$ então $a_j \notin P$ mas, $a_i \in P$ para $i < j$ e

se $g = \sum_0^{\infty} b_i x^i$ então $b_k \notin P$ mas, $b_i \in P$ para $i < k$.

Mas então:

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)\, x + \ldots + (a_0 b_{j+k} + \ldots + a_j b_k + \ldots) x^{j+k} + \ldots \in P^*$$ e portanto

$a_o b_{j+k} + \ldots + a_{j-1}b_{k+1} + a_j b_k + a_{j+1}b_{k-1} + \ldots + a_{j+k}b_o \in P$ e como $a_o, a_1, \ldots, a_{j-1}, b_{j-1}, \ldots, b_o \in P$ segue que $a_j b_k \in P$ o que é absurdo pois $a_j \notin P$ e $b_k \notin P$.

1.2.11 PROPOSIÇÃO

Existe uma correspondência biunívoca entre ideais maximais $\underline{M}$ de A e ideais maximais M de A⟦x⟧ tal que $\underline{M} \leftrightarrow M$ se, e somente se, $M = \langle \underline{M}, x \rangle$.

DEMONSTRAÇÃO:

Seja $\underline{M}$ um ideal maximal de A. Então

$$A[\![x]\!] / \langle \underline{M}, x \rangle \cong A/\underline{M}$$

donde $\langle \underline{M}, x \rangle$ é um ideal maximal de $A[\![x]\!]$.

Seja M um ideal maximal de $A[\![x]\!]$ e considere

$$\underline{M} = \{a \in A : a + xf \in M, \text{ onde } f \in A[\![x]\!]\}$$

É facil ver que $\underline{M}$ é um ideal de A. Provemos que é maximal. Se $\underline{M} \neq A$, então $M \subset \langle \underline{M}, x \rangle$ e daí $M = \langle \underline{M}, x \rangle$ pois M é maximal; Se $\underline{M} = A$ segue que $1 + xf \in M$. Como $1 + xf$ é unidade de $A[\![x]\!]$, deveria ser $M = A[\![x]\!]$, uma contradição.

1.2.12 DEFINIÇÃO

O COMPRIMENTO de uma CADEIA de ideais primos de um anel A é n se:

$$P_o \subset P_1 \subset P_2 \subset \ldots \subset P_n \quad \text{(inclusão estrita)}$$

onde n é finito e P_i é um ideal primo de A.

1.2.13 DEFINIÇÃO

A DIMENSÃO de KRULL do anel A, que denotaremos por dim A, é o supremo dos comprimentos das cadeias de ideais primos de A.

A dimensão de um anel não nulo é um inteiro não negativo ou infinita.

Observações: i) dim A = 0 se, e somente se, todo ideal primo de A é maximal;

ii) Se $\dim A = 0$ e A é um domínio, então A é um corpo.

1.2.14 COROLÁRIO

Se K é um corpo então $K[\![x]\!]$ é um anel local cujo ideal maximal é (x). Alem disso $\dim K[\![x]\!] = 1$.

1.3 DEPENDÊNCIA INTEGRAL

1.3.1 DEFINIÇÃO

Seja A um anel, S uma A-álgebra e $x \in S$. Dizemos que x é integral sobre A se, e somente se, existem elementos $a_1, a_2, \ldots, a_n \in A$ tal que

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

1.3.2 DEFINIÇÃO

Seja A um anel e S uma A-álgebra. Dizemos que S é integral sobre A se todo elemento de S é integral sobre A.

1.3.3 PROPOSIÇÃO [7]

Seja S uma álgebra comutativa sobre o anel A. Então os elementos de S integrais sobre A constituem um subanel de S.

1.3.4 COROLÁRIO

Se T é um subanel de S, integral sobre A e $u \in S$ é integral sobre A, então $T[u]$ é integral sobre A.

1.3.5 PROPOSIÇÃO [1]

Sejam $A \subset B$ domínios, com B integral sobre A. Então B é um corpo se, e somente se, A é um corpo.

1.3.6 PROPOSIÇÃO

Sejam $A \subset B$ domínios, com B integral sobre A. Se P é um ideal de B e $P' = P \cap A$ então B/P é integral sobre A/P'.

DEMONSTRAÇÃO

Seja $\overline{b} = b + P \in B/P$. Como b é integral sobre A temos

$$b^n + a_1 b^{n-1} + \ldots + a_n = 0$$

com $a_1, a_2, \ldots, a_n \in A$, e portanto,

$$b^n + a_1 b^{n-1} + \ldots + a_n + P = P$$

isto é,

$$\overline{b}^n + (a_1 + P')\overline{b}^{n-1} + \dots + (a_n + P') = \overline{0} .$$

Assim, $\overline{b}$ é integral sobre A/P'.

1.3.7 DEFINIÇÃO

Sejam $A \subset B$ anéis.

Dizemos que vale a propriedade LO (Lying Over) se para todo ideal primo P de A existe um ideal primo Q de B tal que $P = Q \cap A$.

Dizemos que vale a propriedade GU (Going Up) se dados ideais primos $P_1 \subset P_2$ em A e Q_1 ideal primo de B com $Q_1 \cap A = P_1$, existe Q_2 ideal primo de B tal que $Q_1 \subset Q_2$ e $Q_2 \cap A = P_2$.

Dizemos que vale a propriedade GD (Going Down) se dados ideais primos $P_1 \supset P_2$ em A e Q_1 ideal primo de B com $Q_1 \cap A = P_1$ existe Q_2 ideal primo de B tal que $Q_1 \supset Q_2$ e $Q_2 \cap A = P_2$.

Dizemos que vale a propriedade INC (Incomparabilidade) se dados P_1, P_2 ideais primos de B com

$$P_1 \cap A = P_2 \cap A$$

P_1 e P_2 não podem ser comparados por $\subset$, isto é, $P_1 \not\subset P_2$ e $P_2 \not\subset P_1$.

1.3.8 PROPOSIÇÃO [7]

Sejam $A \subset B$ aneis, B integral sobre A. Então valem as propriedades INC, GU e LO.

1.4 CORPOS - EXTENSÕES DE CORPOS

1.4.1 DEFINIÇÃO

Um domínio K chama-se CORPO se todo elemento não nulo de K é uma unidade.

1.4.2 DEFINIÇÃO

Seja A um domínio. O CORPO QUOCIENTE de A é o conjunto

$$K = \{\frac{a}{b} : a,b \in A,\ b \neq 0\}$$

onde

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

e

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

1.4.3 PROPOSIÇÃO [6]

Seja A um anel e M um ideal de A. M é um ideal maximal de A se, e somente se, A/M é um corpo.

1.4.4 PROPOSIÇÃO [1]

Seja A um anel não nulo. As seguintes alternativas são equivalentes:

i) A é um corpo;

ii) Os únicos ideais de A são (0) e A ;

iii) Todo homomorfismo não nulo de A num anel S não nulo, é injetor.

1.4.5 DEFINIÇÃO

Sejam $K \subset L$ corpos e $a \in L$. Dizemos que a é ALGÉBRICO sobre K se, e somente se, existe $f(x) \in K[x]$ $f(x) \neq 0$ tal que $f(a) = 0$.

De um modo geral, se $A \subset B$ são anéis, então um elemento $a \in B$ é dito algébrico sobre A se existe um polinômio não nulo $f(x) \in A[x]$ tal que $f(a) = 0$.

Se todo elemento de B é algébrico sobre A, dizemos que B é algébrico sobre A.

1.4.6 LEMA [9]

Se u é algébrico sobre o corpo K então K[u] é um corpo.

1.4.7 PROPOSIÇÃO [9]

Sejam $A \subset B$ domínios, B algébrico sobre A, K e L os corpos quocientes de A e B respectivamente. Então L é algébrico sobre K.

1.4.8 DEFINIÇÃO

Um corpo K é dito ALGEBRICAMENTE FECHADO se cada $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_o \in K[x]$ com $a_n \neq 0$ tem uma raíz r em K, isto é, existe $r \in K$ tal que $f(r) = 0$.

1.4.9 PROPOSIÇÃO [9]

As seguintes alternativas são equivalentes:

i) K é um corpo algebricamente fechado;

ii) Todo polinômio irredutível de K[x] é linear;

iii) Qualquer polinômio de K[x] pode ser escrito como produto finito de polinômios lineares.

1.4.10 TEOREMA [9]

Seja K um corpo. Então existe um único (a menos de isomorfismo) corpo $\overline{K}$, extensão de K tal que $\overline{K}$ é algebricamente fechado. ($\overline{K}$ chama-se o FÊCHO ALGÉBRICO de K).

1.4.11 LEMA

Seja K um corpo algebricamente fechado. Então M é um ideal maximal de K[x] se, e somente se, $M = (x-a)$ com $a \in K$.

DEMONSTRAÇÃO:

Como $K[x]/(x-a) \cong K$, segue-se que $M = (x - a)$ é um ideal maximal de K[x].

Por outro lado, (1.2.4) M é gerado por um polinômio irredutível f. Mas então, (1.4.9) f deve ser linear.

1.4.12 PROPOSIÇÃO

Seja K um corpo e $a_i \in K$, ($i = 1,2,\ldots,n$). Então $M = (x_1 - a_1, x_2 - a_2,\ldots,x_n - a_n)$ é um ideal maximal de $K[x_1,x_2,\ldots,x_n]$.

DEMONSTRAÇÃO:

Consideremos a K-álgebra homomorfismo

$$\phi : K[x_1,x_2,\ldots,x_n] \to K$$

definido por $\phi(f(x_1,x_2,\ldots,x_n) = f(a_1,a_2,\ldots,a_n)$.

Claramente ϕ é sobrejetora e então temos que

$$K[x_1,x_2,\ldots,x_n]/\mathrm{Ker}\phi \cong K$$

Portanto Ker ϕ é maximal e desde que Kerϕ = M, segue o resultado.

1.5 ANÉIS E MÓDULOS NOETHERIANOS

1.5.1 DEFINIÇÃO

Seja M um A-módulo. M é NOETHERIANO se toda sequência

$$M_o \subset M_1 \subset M_2 \subset \dots \subset M_n \subset \dots$$

de submódulos de M for estacionária, isto é, existe r inteiro positivo tal que $M_r = M_{r+1} = M_{r+2} = \dots$

Esta condição é chamada CONDIÇÃO DE CADEIA ASCENDENTE (c.c.a.).

1.5.2 DEFINIÇÃO

Um anel A é noetheriano se vale (c.c.a) para ideais, isto é, se

$$P_o \subset P_1 \subset P_2 \subset \dots \subset P_n \subset \dots$$

então existe r inteiro positivo tal que

$$P_r = P_{r+1} = P_{r+2} = \dots.$$

1.5.3 PROPOSIÇÃO [1]

a) Um A-módulo M é noetheriano, se, e somente se, todo submódulo de M é finitamente gerado;

b) Um anel A é noetheriano se, e somente se, todo ideal de A é finitamente gerado.

1.5.4 PROPOSIÇÃO [1]

Se A é um anel noetheriano então as imagens homomorfas de A são aneis noetherianos.

1.5.5 PROPOSIÇÃO [1]

Se A é um anel noetheriano e S é um sistema multiplicativo fechado de A então $S^{-1}A$ é noetheriano.

1.5.6 TEOREMA DE BASE DE HILBERT [1]

Se A é um anel noetheriano então $A[x_1, x_2, \dots, x_n]$ é noetheriano.

1.5.7 DEFINIÇÃO

Uma cadeia de submódulos de um módulo M é uma sequência (M_i) $(0 \leq i \leq n)$ de submódulos de M tal que

$$M = M_o \subset M_1 \subset \ldots \subset M_n = 0$$ (inclusão estrita).

O COMPRIMENTO da cadeia é o número de "elos" da mesma. O comprimento da cadeia acima é n.

Uma SÉRIE DE COMPOSIÇÃO de M é uma cadeia maximal. (Ver [1])

1.5.8 PROPOSIÇÃO [1]

As seguintes afirmativas são equivalentes:

i) A é um anel noetheriano e dim A = 0;

ii) Qualquer A-módulo finitamente gerado tem comprimento finito.

1.5.9 TEOREMA [7]

Seja A um anel noetheriano, I um ideal de A. Então r(I) é uma intersecção finita de ideais primos de A.

1.5.10 COROLÁRIO [7]

Seja A um anel noetheriano e I um ideal de A. Então só existe um número finito de ideais primos de A que são minimais sobre I.

C A P Í T U L O 2

G-DOMÍNIOS e G-IDEAIS

2.1 G-DOMÍNIOS

2.1.1 DEFINIÇÃO

Um domínio A é chamado G-DOMÍNIO se seu corpo quociente K é um anel finitamente gerado sobre A, isto é, se

$$K = A[t_1, t_2, \ldots, t_n] \quad \text{com } t_i = \frac{a_i}{b_i},\ a_i, b_i \in A, b_i \neq 0$$

A proposição a seguir nos dá um critério mais simples para caracterizar um G-domínio.

2.1.2 PROPOSIÇÃO

Seja A um domínio, K o corpo de frações de A. Então A é um G-domínio se, e somente se, K, como anel, é gerado sobre A por um só elemento.

DEMONSTRAÇÃO:

Se K é um anel gerado sobre A por um só elemento isto é, $K = A[u]$, $u \in K$ então A é um G-domínio, por definição.

Reciprocamente, se A é um G-domínio, teremos:

$$K = A[\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}] \quad \text{com } a_i, b_i \in A$$

Tomando $b = b_1 b_2 \ldots b_n$ teremos $K = A[b^{-1}]$ como queríamos.

A seguir procuramos resultados equivalentes a " A é um G-domínio". Para tal é interessante estabelecer a seguinte definição.

2.1.3 DEFINIÇÃO

Se A é um anel então o PSEUDO RADICAL de A, denotado por P(A), é a intersecção de todos os ideais primos não nulos de A. (Ver [3])

OBSERVAÇÃO: Se A não é um domínio, P(A) coincide com N(A). No entanto, se A é um domínio, P(A) $\neq$ N(A).

2.1.4 TEOREMA

Seja A um domínio, K o corpo quociente de A e $u \in A$, $u \neq 0$. Então são equivalentes:

i) $u \in P(A)$;

ii) Todo ideal primo não nulo de A contem u;

iii) Todo ideal não nulo de A contem uma potência de u;

iv) $K = A[u^{-1}]$ e portanto A é um G-domínio.

DEMONSTRAÇÃO:

i) → ii) Imediata

ii) → iii) Seja I um ideal não nulo de A e suponha que

$$I \cap \{ u^n, n \geq 0\} = \phi$$

Como $\{u^n, n \geq 0\}$ é um sistema multiplicativo fechado, podemos extender I a um ideal P, maximal com respeito a exclusão de $\{u^n, n \geq 0\}$. Mas então P é primo por (1.1.17) e

$$P \cap \{ u^n, n \geq 0 \} = \phi.$$

contradiz a hipótese $u \in P$.

iii) → iv) Seja $\frac{1}{b} \in K$. Se considerarmos o ideal bA temos, por iii), $bA \cap \{u^n, n \geq 0 \} \neq \phi$. Assim, existe $k \geq 0$ tal que $u^k \in bA$ e assim $u^k = bc$ para algum $c \in A$. Tiramos então $b^{-1} = c.u^{-k}$ e finalmente,

$$K = A[u^{-1}]$$

donde concluímos que A é um G-domínio.

iv) → i) Seja P um ideal primo não nulo de A e considere $b \in P$, $b \neq 0$. Temos $b^{-1} \in K = A[u^{-1}]$ donde temos

$$b^{-1} = \sum_0^n a_i (u^{-1})^i = u^{-n} \sum_0^n a_i u^{n-i}$$

Como $\sum_0^n a_i u^{n-i} = c \in A$, temos $b^{-1} = c.u^{-n}$ e assim $u^n = bc \in P$ e então $u \in P$. Assim, $u \in P(A)$.

2.1.5 COROLÁRIO

Se A é um domínio com um número finito de ideais primos, então A é um G-domínio.

DEMONSTRAÇÃO:

Seja $\{P_1, P_2, \ldots, P_n\}$ o conjunto dos ideais primos não nulos de A e considere $x_i \in P_i$ ($i = 1,2,\ldots,n$) com $x_i \neq 0$.

Então $u = x_1 x_2 \ldots x_n$ é não nulo e $u \in P_i$ para todo i tal que $1 \leq i \leq n$ e consequentemente $u \in P(A)$.

2.1.6 PROPOSIÇÃO

Se A é um PID então A é um G-domínio se, e somente se, A tem apenas um número finito de ideais primos.

DEMONSTRAÇÃO:

Se A é um G-domínio então existe $u \in A$, $u \neq 0$ tal que u é elemento de todo ideal primo não nulo de A. Como A é um UFD (1.2.3) só podemos ter um número finito de tais ideais primos.

A recíproca é o corolário 2.1.5.

2.1.7 EXEMPLOS de G-DOMÍNIOS

a) Todo corpo é um G-domínio;

b) $K[\![x]\!]$ é um G-domínio se K é um corpo (1.2.14)

c) Seja $A = \mathbb{Z} + x.\mathbb{Q}[\![x]\!]$ o anel das séries de potências com coeficientes racionais e termo constante inteiro. Então A é um G-domínio com uma infinidade de ideais maximais (e portanto primos), como veremos:

<u>LEMA I</u>: Se $p \in \mathbb{Z}$, $p \neq 0$ então pA é um ideal maximal de A, se p é um inteiro primo.

DEMONSTRAÇÃO:

Seja $f \in A$. Então

$$f = n + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots \text{ onde}$$

$n \in \mathbb{Z}$, $a_i \in \mathbb{Q}$, $i = 1,2,\ldots$

Mas, dados n e p inteiros, existem $q, r \in \mathbb{Z}$ tal que $n = pq + r$, $0 \leq r < p$ de modo que

$$f = r + (pq + a_1 x + \ldots + a_n x^n + \ldots)$$

$$= r + p(q + p^{-1} a_1 x + \ldots + p^{-1} a_n x^n + \ldots)$$

ou seja, $\bar{f} = \bar{r} + pA \in A/pA$.

Consequentemente $A/pA \cong \mathbb{Z}_p$ e se p é primo, A/pA é corpo e pA é maximal.

Assim provamos que A tem um número infinito de ideais maximais.

<u>LEMA II</u>: A é um G-domínio.

DEMONSTRAÇÃO:

Afirmamos que $x \in P$, para todo ideal primo P, não nulo.

Consideremos o menor inteiro positivo r tal que

$$r + a_1x + \ldots + a_nx^n + \ldots \in P.$$

Claramente $r \neq 1$ pois senão tal elemento seria uma unidade de A e P = A.

Se existe tal inteiro $r > 1$ então

$$r + a_1x + \ldots + a_nx^n + \ldots = r(1 + r^{-1}a_1x + \ldots + r^{-1}a_nx^n + \ldots) \in P$$

e portanto $r \in P$ e então $rA \subset P$.

Para qualquer $f \in P$,

$f = n + b_1x + b_2x^2 + \ldots = t + rq + b_1x + b_2x^2 + \ldots$ onde $q,t \in \mathbb{Z}$ e $0 \leq t < r$. Como $rq \in P$ e $t < r$ temos $t = 0$ e então

$$f = r(q + r^{-1}b_1x + r^{-1}b_2x^2 + \ldots) \in rA$$

Portanto $P = rA$ e daí

$$x = r(0 + r^{-1}x + 0x^2 + 0x^3 + \ldots) \in rA = P$$

Se não existe o inteiro $r > 0$ então todo elemento de P tem a forma:

$$f = a_1x + a_2x^2 + \ldots \quad \text{com } a_i \in \mathbb{Q}.$$

Como $P \neq (0)$, existe $g \in P$,

$$g = a_ix^i + a_{i+1}x^{i+1} + \ldots \quad \text{com } a_i \in \mathbb{Q}$$ e

$a_i \neq 0$. Então:

$$g = x^i(a_i + a_{i+1}x + \ldots)$$ e como

$a_i + a_{i+1}x + \ldots \notin P$ devemos ter $x^i \in P$ e daí $x \in P$.

Portanto, $P(A) = (x) \neq (0)$

Algumas informações sobre extensões de G-domínios são as seguintes:

2.1.8 PROPOSIÇÃO

Seja A um domínio, K o corpo quociente de A e T um anel tal que $A \subset T \subset K$. Se A é um G-domínio então T é um G-domínio.

DEMONSTRAÇÃO:

Temos $K = A[u^{-1}]$ para algum $u \in A$, $u \neq 0$ e portanto $K \subset T[u^{-1}]$. Como o corpo de frações de T é K, $T[u^{-1}] \subset K$ e então $K = T[u^{-1}]$ e T é um G-domínio.

2.1.9 PROPOSIÇÃO

Se A é um domínio e x uma indeterminada sobre A então $A[x]$ não pode ser um G-domínio.

DEMONSTRAÇÃO:

Se K é o corpo quociente de A e F é o corpo quociente de $A[x]$, temos: $A[x] \subset K[x] \subset F$.

Se $A[x]$ é um G-domínio então $K[x]$ é um G-domínio (2.1.8). Mas $K[x]$ é um PID com um número infinito de ideais primos (1.2.7). Assim $A[x]$ não pode ser um G-domínio. (2.1.6).

2.1.10 LEMA

Sejam R_1 e R_2 domínios tais que $1_{R_1} = 1_{R_2}$ e $R_1 \subset R_2$. Sejam $P(R_i)$ o pseudo radical de R_i e $J(R_i)$ o radical de Jacobson de R_i ($i = 1,2$). Temos:

i) Se para todo ideal $I_2 \neq (0)$ de R_2, $I_2 \cap R_1 \neq 0$ então $P(R_1) \subset P(R_2) \cap R_1$;

ii) Se R_2 é integral sobre R_1 então:

a) $P(R_1) = P(R_2) \cap R_1$

b) $J(R_1) = J(R_2) \cap R_1$.

DEMONSTRAÇÃO de i)

Se $P(R_1) = (0)$ então o resultado vale trivialmente.

Se $x \in P(R_1)$, $x \neq 0$, seja P_2 um ideal primo de R_2

Por hipótese $P_2 \cap R_1 \neq (0)$ e $P_2 \cap R_1$ é primo. Assim o elemento x pertence a $P_2 \cap R_1$ para todo P_2 ideal primo não nulo de R_2 e portanto $x \in P(R_2) \cap R_1$.

DEMONSTRAÇÃO de ii)

a) Se $P(R_2) \cap R_1 = (0)$ então, pela parte i) deste lema teríamos $P(R_1) = (0)$.

Se $P(R_2) \cap R_1 \neq (0)$, seja $x \neq 0$ um de seus elementos, isto é, $x \in R_1$ e x é elemento de todo ideal primo não nulo de R_2. Como R_2 é integral sobre R_1, (1.3.8) para cada primo P_1 de R_1 existe um ideal primo P_2 de R_2 tal que $P_2 \cap R_1 = P_1$. Logo $x \in P(R_1)$ e então $P(R_2) \cap R_1 \subset P(R_1)$ e com a parte i) deste lema, temos a igualdade.

b) Se $x \notin J(R_1)$ então existe M ideal maximal de R_1 tal que $x \notin M$ e por (1.3.8) existe M' ideal primo de R_2 tal que $M = M' \cap R_1$. Assim $x \notin M'$, logo $x \notin J(R_2) \cap R_1$. Consequentemente, $J(R_2) \cap R_1 \subset J(R_1)$.

Por outro lado, seja M_2 ideal maximal de R_2. Temos $M_2 \cap R_1$ maximal em R_1. (Se $M_2 \cap R_1$ não é maximal, existe M_2' tal que $M_2 \cap R_1 \subset M_2'$ e com 1.1.15 chegaríamos a uma contradição).

Assim, se $x \in J(R_1)$, x é elemento de todo ideal maximal de R_1 e consequentemente elemento de todo ideal maximal de R_2, e assim, $x \in J(R_2)$ donde $J(R_1) \subset J(R_2) \cap R_1$.

2.1.11 TEOREMA

Sejam $A \subset B$ domínios, e B integral sobre A. Então A é G-domínio, se, e somente se, B é G-domínio.

DEMONSTRAÇÃO:

Por (2.1.10) temos $P(A) = P(B) \cap A$.

Se A é G-domínio então $P(A) \neq (0)$ e portanto $P(B) \neq (0)$ donde B é G-domínio.

Se B é G-domínio, suponha $P(A) = (0)$. Assim, existe $x \in P(B)$, $x \neq 0$ com $x \notin A$. Como x é integral sobre A, seja n o menor inteiro positivo tal que:

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \text{ onde } a_i \in A.$$

Temos:

$$x(x^{n-1} + a_1x^{n-2} + \ldots + a_{n-1}) = -a_n \quad (-a_n \in A)$$

e $x(x^{n-1} + a_1x^{n-2} + \ldots + a_{n-1}) \in P(B)$.

Deste modo,

$$x(x^{n-1} + \ldots + a_{n-1}) \in P(B) \cap A = (0)$$

donde $x(x^{n-1} + \ldots + a_{n-1}) = 0$ o que acarreta ($x \neq 0$) que

$$x^{n-1} + a_1x^{n-2} + \ldots + a_{n-1} = 0$$

uma contradição com a escolha de n. Assim $P(A) \neq (0)$ e A é um G-domínio.

2.1.12 TEOREMA

Sejam $A \subset T$ domínios, T algébrico sobre A. Então

i) Se A é G-domínio, T é G-domínio;

ii) Se T é finitamente gerado como anel sobre A e T é G-domínio então A é G-domínio.

DEMONSTRAÇÃO de i):

Sejam K e L os corpos de frações de A e T respectivamente. Se A é G-domínio temos $K = A[u^{-1}]$ com $0 \neq u \in A$ Evidentemente temos, $T[u^{-1}] \subset L$.

Agora, T algébrico sobre A acarreta T é integral sobre K donde $T[u^{-1}]$ é integral sobre K ($u^{-1} \in K \subset L$) (1.3.4) Mas então $T[u^{-1}]$ é um corpo (1.3.5) e como $T[u^{-1}] \subset L$ temos $L = T[u^{-1}]$ e T é um G-domínio.

DEMONSTRAÇÃO de ii):

Se T é um G-domínio temos $L = T[v^{-1}]$ com $v \in T$, $v \neq 0$, e como T é finitamente gerado sobre A temos

$$T = A[w_1, w_2, \ldots, w_n], \quad w_i \in T$$

Os elementos $v^{-1}, w_1, w_2, \ldots, w_n$ são algébricos sobre A, logo temos:

$$\begin{cases} a_o(v^{-1})^n + a_1(v^{-1})^{n-1} + \ldots + a_n = 0 \text{ com } a_i \in A \\ b_{oi}w_i^{n_i} + b_{1i}w_i^{n_i-1} + \ldots + b_{n_i i} = 0 \ (i = 1,2,\ldots,n \end{cases}$$

e $b_{ji} \in A$

Seja A_1 o anel $A[a_o^{-1}, b_{o1}^{-1}, \ldots, b_{on}^{-1}]$. Evidentemente $A \subset A_1 \subset K$.

Como $L = T[v^{-1}] = A[w_1,w_2,\ldots,w_n][v^{-1}]$ e

$A_1 \subset K \subset L$ é imediato que

$$L = A_1[v^{-1},w_1,w_2,\ldots,w_n].$$

Mas agora, v^{-1}, $w_1,w_2,\ldots,w_n$ são integrais sobre A_1 e portanto L é integral sobre A_1. Assim (1.3.5) A_1 é um corpo e necessariamente $K = A_1 = A[a_o^{-1}, b_{o1}^{-1},\ldots,b_{on}^{-1}]$. Assim A é um G-domínio.

2.1.13 COROLÁRIO

Sejam $A \subset T$ domínios e $u \in T$.

Se $A[u]$ é G-domínio então u é algébrico sobre A e A é G-domínio.

DEMONSTRAÇÃO:

Se u não é algébrico sobre A então a aplicação

$$\phi : A[x] \to A[u]$$

definida por $\phi(f(x)) = f(u)$ é um isomorfismo de anéis. Por (2.1.9) $A[u]$ não é um G-domínio.

Agora, $A[u]$ é um anel finitamente gerado sobre A algébrico sobre A e portanto por (2.1.12) A é um G-domínio.

2.1.14 PROPOSIÇÃO

Seja A um domínio, K o corpo de frações de A e suponhamos que $K = A[x_1,x_2,\ldots,x_n,\ldots]$ com $x_i \in K$, isto é, K é enumeravelmente gerado sobre A como anel. Então A é um G-domínio, se, e somente se, K não pode ser escrito como reunião de uma cadeia de subanéis próprios de K, crescente e contendo A.

DEMONSTRAÇÃO:

Se A é um G-domínio, existe $u \in A$, $u \neq 0$ tal que $K = A[u^{-1}]$. Se

$$A \subset A_1 \subset A_2 \subset \dots \subset A_n \subset \dots$$

é uma cadeia de subanéis próprios de K e $K = \cup A_i$ então $u^{-1} \in \cup A_i$ e consequentemente, existe j tal que

$$u^{-1} \in A_j$$

Como $A \subset A_j$ temos $K = A_j$, uma contradição.

Reciprocamente, se A não é um G-domínio então K não é finitamente gerado sobre A como anel (2.1.12).

Seja $K = A[x_1, x_2, \dots, x_n, \dots]$ tal que x_{i+1} não é elemento de $A[x_1, x_2, \dots, x_i]$ para todo i inteiro positivo, e considere a cadeia:

$$A \subset A_1 \subset A_2 \subset \dots \subset A_n \subset \dots \qquad \text{onde}$$

$A_i = A[x_1, x_2, \dots, x_i]$. Claramente $A_i \neq A_{i+1}$ para todo i e $K = \bigcup_0^\infty A_i$ como queríamos.

OBSERVAÇÃO: $\mathbb{Q} = \mathbb{Z}[1/2, 1/3, \dots, 1/p, \dots]$ (p primo) e $\mathbb{Z}$ não é G-domínio.

Nosso próximo resultado expõe a conexão existente entre um G-domínio A e ideais maximais dos anéis $A[x]$ e $A[x_1, x_2, \dots, x_n]$.

2.1.15 TEOREMA

Seja A um domínio com corpo quociente K. As seguintes afirmativas são equivalentes:

i) A é um G-domínio;

ii) Existe um polinômio linear $f(x) \in A[x]$ tal que o ideal $(f(x))$ é maximal e minimal em $A[x]$;

iii) Existe um ideal primo M de $A[x]$ que é maximal e minimal em $A[x]$;

iv) Existe um ideal maximal M de $A[x]$ tal que $M \cap A = (0)$;

v) Existe um ideal maximal N de $A[x_1, x_2, \dots, x_n]$ tal que $N \cap A = (0)$.

DEMONSTRAÇÃO:

i) $\to$ ii) Temos $K = A[u^{-1}]$ com $u \in A$, $u \neq 0$. Seja

$$\phi : A[x] \to A[u^{-1}] \qquad \text{onde}$$

$\phi(f(x)) = f(u^{-1})$. Podemos verificar que ϕ é um homomorfismo sobrejetor e portanto

$$A[x]/\mathrm{Ker}\phi \equiv A[u^{-1}] = K$$

Assim, $\mathrm{Ker}\phi$ é um ideal maximal de $A[x]$. Provemos que $\mathrm{Ker}\phi = (ux - 1)$.

É imediato que $(ux - 1) \subset \mathrm{Ker}\phi$. Por outro lado, se $g(x) = a_o + a_1x + \ldots + a_nx^n \in \mathrm{Ker}\phi$ então $g(x) + a_o(ux - 1) = (a_1 + a_ou)x + a_2x^2 + \ldots +$

$$+ a_nx^n$$

é um elemento de $\mathrm{Ker}\phi$, isto é,

$$x[(a_1 + a_ou) + a_2x + \ldots + a_nx^{n-1}] \in \mathrm{Ker}\phi,$$

donde concluímos que

$$(a_1 + a_ou) + a_2x + \ldots + a_nx^{n-1} \in \mathrm{Ker}\phi,$$

já que $x \notin \mathrm{Ker}\phi$.

Podemos então utilizar indução: Se $ax + b$ pertence a $\mathrm{Ker}\phi$ temos $au^{-1} + b = 0$ ou seja,

$$b = -au^{-1} \in A \qquad \text{assim}$$

$ax + b = ax - au^{-1} = au^{-1}(ux - 1) \in (ux - 1)$. Portanto $\mathrm{Ker}\phi = (ux - 1)$ como queríamos.

Resta mostrar que $(ux - 1)$ é minimal o que decorre imediatamente de (1.1.19)

ii) $\to$ iii) Basta tomar $M = (ux - 1)$

iii) $\to$ iv) Seja M ideal maximal e minimal em $A[x]$.

Se $M \cap A = P$ temos $PA[x] \subset M$. Como

$$A[x]/PA[x] \cong (A/P)[x]$$ e desde

que $(A/P)[x]$ não é corpo segue-se $PA[x] \neq M$. Como P e $PA[x]$ são primos, $PA[x] \subset M$ acarreta $P = (0)$ já que M é minimal.

iv) $\rightarrow$ v) Utilizando-nos de iii) seja M um ideal maximal (e minimal) de $A[x_1]$ tal que $M \cap A = (0)$.

Temos que $MA[x_1,x_2,\dots,x_n]$ é um ideal próprio de $A[x_1,x_2,\dots,x_n]$ e portanto existe N ideal maximal de $A[x_1,x_2,\dots,x_n]$ contendo $MA[x_1,x_2,\dots,x_n]$.

Agora, $N \cap A[x_1] = M$ e assim $N \cap A = M \cap A = (0)$, como queríamos.

v) $\rightarrow$ i) Seja M ideal maximal de $A[x_1,x_2,\dots,x_n]$. Então

$$A[x_1,x_2,\dots,x_n]/M$$

é um corpo e contem A.

Como $A[x_1,x_2,\dots,x_n]/M \cong A[t_1,t_2,\dots,t_n]$ onde $t_i = x_i + M$, é um G-domínio, (2.1.13) nos garante que A é um G-domínio.

Alguns resultados interessantes advem quando investigamos domínios de valorização. Para tal estabeleceremos algumas definições.

2.1.16 DEFINIÇÃO

A é um ANEL de VALORIZAÇÃO se, e somente se, P,Q são ideais de A então $P \subset Q$ ou $Q \subset P$.

2.1.17 DEFINIÇÃO

Seja P um ideal primo do anel A. Uma cadeia de ideais primos distintos e não nulos do tipo:

$$P = P_o \supset P_1 \supset P_2 \supset \dots \supset P_n$$

tem comprimento n. O PÔSTO de P é então o supremo dos comprimentos de todas as cadeias decrescentes a partir de P e formada por ideais primos distintos e não nulos.

2.1.18 PROPOSIÇÃO

Seja A um domínio de valorização. A é um G-domínio se, e somente se, A possui um ideal primo de posto 1.

DEMONSTRAÇÃO:

Se A é um G-domínio temos $P(A) \neq (0)$. Provaremos que $P(A)$ é um ideal primo e portanto de posto 1.

Seja $ab \in P(A)$ e suponha que $a \notin P(A)$ bem como $b \notin P(A)$. Então existe P ideal primo de A tal que $a \notin P$ e existe Q ideal primo de A tal que $b \notin Q$. Como A é um domínio de valorização devemos ter

$$P \subset Q \quad \text{ou} \quad Q \subset P$$

Se $P \subset Q$ segue-se que $b \notin P$ acarretando que $ab \notin P$ o que é absurdo, já que $ab \in P(A)$.

Por outro lado, seja Q um ideal de posto 1 de A. Se P é um outro ideal primo de A teremos forçosamente $Q \subset P$, já que $P \subset Q$ acarreta $P = Q$ ou $P = (0)$.

Assim $Q \subset P(A)$ e portanto $P(A) \neq (0)$ o que acarreta A é um G-domínio.

2.1.19 PROPOSIÇÃO

Seja A um G-domínio. Então cada ideal primo não nulo de A contem um ideal primo de posto 1.

DEMONSTRAÇÃO:

É uma aplicação imediata de (1.1.18) onde se tomará $I = P(A)$.

2.2 G-IDEAIS

Se A é um anel e P é um ideal primo de A então A/P é um domínio. Nesta seção estudaremos condições sobre o ideal primo P de tal modo que A/P seja um G-domínio.

Note que se P é um ideal maximal então A/P é um G-domínio, mas veremos que não há necessidade de P ser maximal. Para tanto estabelecemos a seguinte definição:

2.2.1 DEFINIÇÃO

Seja A um anel comutativo com elemento unidade e P um ideal primo de A. Diremos que P é um G-IDEAL de A se o anel quociente A/P é um G-domínio.

2.2.2 EXEMPLOS:

a) Se K é um corpo então o ideal (x) é um G-ideal de $K[x]$ pois $K[x]/(x) \cong K$.

b) Um ideal maximal M do anel A é um G-ideal de A.

c) Se $A = K[x,y]$ onde K é um corpo então o ideal (y) é primo mas não é um G-ideal de A (2.1.9).

d) Este exemplo é interessante. Seja

$$A = \mathbb{Z} + x\,\mathbb{Q}[\![x]\!] .$$ Então A é um G-domínio (2.1.7, (c)) mas $A/(x) \cong \mathbb{Z}$ não é um G-domínio. (2.1.6)

A noção de G-IDEAL permite reformular o teorema de KRULL sobre o nilradical (1.1.9), que pode ser re-enunciado como segue:

2.2.3 TEOREMA (KRULL)

O nilradical do anel A é a intersecção de todos os G-ideais de A.

DEMONSTRAÇÃO:

Seja N(A) o nilradical de A. Se $x \in N(A)$ então $x \in P$, para todo P ideal primo de A. Como G-ideais são primos, x é elemento de todo G-ideal e temos

$$N(A) \subset \cap P_i$$

onde cada P_i é um G-ideal de A.

Por outro lado, se $x \notin N(A)$ então $x^n \neq 0$ para todo n inteiro positivo, isto é, $(0) \cap \{x^n, n \geq 1\} = \phi$. Podemos então "expandir" (0) até um ideal I, maximal com respeito a exclusão de $\{x^n, n \geq 1\}$. Por (1.1.17) I é um ideal primo de A. Para terminar a demonstração provemos que I é um G-ideal, ou seja, que A/I é um G-domínio.

Seja $\gamma : A \to A/I$ o homomorfismo natural e $\overline{x} = \gamma(x)$.

$$\begin{tikzcd}
A \arrow[r, "\gamma"] \arrow[d, dash] & A/I \arrow[d, dash] \\
J \arrow[r, dash] \arrow[d, dash] & \overline{J} \arrow[d, dash] \\
I \arrow[r, dash] & (0)
\end{tikzcd}$$

No diagrama acima, se $\overline{J}$ é um ideal primo não nulo de A/I então sua contração J contem I e portanto

$$J \cap \{x^n, n \geq 1\} \neq \phi$$

acarretando $x \in J$, já que J é primo. Assim, $\overline{x} \in \overline{J}$, para todo $\overline{J}$ ideal primo não nulo de A/I e portanto o pseudo-radical de A/I é não nulo donde A/I é um G-domínio, como queríamos.

Nosso próximo objetivo é estudar o comportamento dos G-ideais frente a homomorfismos.

2.2.4 PROPOSIÇÃO

Sejam A e B anéis e $\phi: A \to B$ um homomorfismo sobrejetor com $\operatorname{Ker}\phi = N$. Então existe uma correspondência biunívoca entre ideais de B e ideais de A que contem N. Nessa correspondência, a G-ideais estão associados G-ideais.

Daremos a demonstração só da última afirmativa.
Considere o diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ | & & | \\ I & \text{——} & I' \\ | & & | \\ N & \text{——} & (0) \end{array}$$

Se I é um G-IDEAL de A então A/I é um G-domínio e existe $u \in A$, $u \neq 0$ com $u \in P$ para todo ideal primo $P \supset I$ e $u \notin I$.

Sejam $u' = \phi(u)$ e I' o ideal de B correspondente a I (cuja existência é garantida pela primeira parte desta proposição).

Afirmamos que $u' \in P'$ para todo ideal primo P' de B com $P' \supset I'$. Se isso não ocorresse existiria P_1' ideal primo de B com $u' \notin P_1'$ e assim $u \notin \phi^{-1}(P_1')$ o que é absurdo pois $\phi^{-1}(P_1')$ é um ideal primo de A e contem I.

Reciprocamente, se I' é um G-ideal de B, existe $u' \in B$, $u' \neq 0$, tal que $u' \in P'$ para todo P' ideal primo de B com $P' \supset I'$. Como ϕ é sobrejetor, existe ao menos um $u \in A$ tal que $\phi(u) = u'$. Assim $u \in \phi^{-1}(P')$ para todo $P' \supset I'$. Utilizando-nos da primeira parte desta proposição concluímos que $I = \phi^{-1}(I')$ é um G-ideal de A.

Observação: A imagem homomorfa de um G-ideal sempre é um G-ideal, mesmo que o homomorfismo não seja sobrejetor. O mesmo não ocorre com a imagem inversa, como vemos:

(0) é G-ideal de $\mathbb{Q}$ e se $\phi\colon \mathbb{Z} \to \mathbb{Q}$ então $\phi^{-1}((0)) = (0)$ não é um G-ideal de $\mathbb{Z}$.

2.2.5 PROPOSIÇÃO

Seja A um anel, I um ideal de A e r(I) o radical de I. Então r(I) é a intersecção todos os G-ideais de A que contem I.

DEMONSTRAÇÃO:

Com base na proposição anterior e (1.1.13) a conclusão sai imediata.

Nosso próximo objetivo é relacionar G-ideais de A com a contração de ideais maximais de $A[x]$. Com esse objetivo provaremos o seguinte lema.

2.2.6 LEMA

Se A é um domínio, I um ideal de A, $A^* = A/I$ e $IA[x] = \{\sum_0 a_i x^i : a_i \in I\}$ então

$$A[x]/IA[x] \cong (A/I)[x] = A^*[x]$$

DEMONSTRAÇÃO:

Definamos $h: A[x] \mapsto A^*[x]$ por

$$h(\sum_0^n a_i x^i) = \sum_0^n (a_i + I)x^i$$

Como h é um homomorfismo sobrejetor e é fácil ver que $\operatorname{Ker} h = IA[x]$, segue pelo Teorema do Isomorfismo:

$$A[x]/IA[x] \cong (A/I)[x] = A^*[x].$$

2.2.7 TEOREMA

Um ideal I do anel A é um G-ideal de A, se, e somente se, existe um ideal maximal M de $A[x]$ tal que $M \cap A = I$.

DEMONSTRAÇÃO:

Tomando os anéis quocientes $A^* = A/I$ (2.2.6) podemos fazer a seguinte reformulação do enunciado:

"O ideal (0) do anel A^* é um G-IDEAL de A^*, se, e somente se, existe um ideal maximal M' de $A^*[x]$ tal que $M' \cap A^* = (0)$.

Mas então, temos:

Se (0) é um G-ideal de A^*, A^* é um G-domínio e (2.1.15) existe M' ideal maximal de $A^*[x]$ tal que $M' \cap A^* = (0)$.

Reciprocamente, se existe M' ideal maximal de $A^*[x]$ tal que $M' \cap A^* = (0)$ então A^* é um G-domínio (2.1.15), donde decorre que I é um G-ideal de A.

Faremos a seguir algumas observações a respeito de G-ideais.

OBSERVAÇÃO 1: Por definição um G-ideal é primo. No entanto nem todo primo é um G-ideal. De fato, o ideal (0) de $\mathbb{Z}$ é primo mas $\mathbb{Z} \equiv \mathbb{Z}/(0)$ não é um G-domínio e consequentemente (0) não é um G-ideal;

OBSERVAÇÃO 2: Todo ideal maximal de A é um G-ideal de A mas nem todo G-ideal de A é maximal como vemos: Seja $A = [\mathbb{Z} + x\,\mathbb{Q}[\![x]\!]][y]$. O ideal (y) é um G-ideal de A, mas não é maximal. Ver (2.1.7, c).

A seguir estabeleceremos um resultado muito importante para o desenvolvimento do próximo capítulo.

2.2.8 TEOREMA

Seja M um ideal maximal de $A[x]$ tal que temos $M \cap A = N$ é um ideal maximal de A. Então M pode ser gerado por N e mais um elemento $f \in A[x]$ tal que a imagem natural de f em $(A/N)[x]$ seja um polinômio irredutível.

DEMONSTRAÇÃO:

Tomemos o quociente por N, e seja $A^* = A/N$, um corpo. O enunciado pode ser reformulado para: "Seja M' ideal maximal de $A^*[x]$ tal que $M' \cap A^* = (0)$. Então M' pode ser gerado por $f \in A^*[x]$ com f irredutível".

Como A^* é um corpo, temos que $A^*[x]$ é um PID (1.2.6) e portanto $M' = (f)$ com f irredutível sobre A^* (1.2.4).

Se $\phi: A[x] \to A^*[x]$ é o homomorfismo do lema 2.2.6 temos, de acordo com o diagrama:

$$\begin{tikzcd}
A[x] \arrow[r, "\phi"] \arrow[d, dash] & A^*[x] \arrow[d, dash] \\
M \arrow[r, dash] \arrow[d, dash] & M' = (f) \arrow[d, dash] \\
NA[x] \arrow[r, dash] & (0)
\end{tikzcd}$$

$M = (N, f_o)$ onde f_o é uma pré-imagem unitária do polinômio f irredutível sobre A/N.

OBSERVAÇÃO: Se o corpo A/N é algebricamente fechado então o polinômio $f \in A^*[x]$ deve ser do tipo $x - \overline{a}$ por (1.4.9) com $\overline{a} \in A^*$ e f_o será da forma $x - a$ com $\overline{a} = a+N$. Assim, teríamos, $M = (N, x - a)$.

C A P Í T U L O 3

ANÉIS de HILBERT

3.1 ANEIS DE HILBERT

Vimos no capítulo precedente que todo ideal maximal do anel A é um G-ideal de A. Neste paragrafo estudaremos os anéis A onde a recíproca é verdadeira, isto é, - anéis onde todo G-ideal é maximal.

3.1.1 DEFINIÇÃO:

Um anel A é chamado ANEL de HILBERT (ou ANEL de JACOBSON [2]) se todo G-IDEAL de A é maximal.

3.1.2 EXEMPLOS:

i) Todo corpo é um anel de Hilbert;

ii) Se A é um anel de dimensão 0, todo ideal primo de A é maximal e consequentemente (2.2.1) todo G-ideal de A é maximal. Portanto A é um anel de Hilbert.

iii) $A = [\mathbb{Z} + x\,\mathbb{Q}[\![x]\!]][y]$ não é anel de Hilbert, mas A é noetheriano (2.1.7, (c)).

Nosso próximo resultado será estabelecer condições para que um anel A seja um anel de Hilbert.

3.1.3 PROPOSIÇÃO

As seguintes afirmativas são equivalentes:

i) A é um anel de Hilbert;

ii) Se I é um ideal de A então r(I) é a intersecção dos ideais maximais de A que contem I;

iii) Se P é um ideal primo de A então P é a intersecção dos ideais maximais de A que o contem;

iv) Todo G-ideal de A é a intersecção dos ideais maximais de A que o contem.

DEMONSTRAÇÃO:

i) $\to$ ii) De (2.2.5) e (3.1.1) segue o resultado.

ii) $\to$ iii) Como $r(P) = P$, segue o resultado.

iii) $\to$ iv) Se Q é um G-ideal de A então Q é primo e o resultado segue imediato.

iv) $\to$ i) Seja P um G-ideal de A. Devemos provar que P é maximal. Se P não é maximal, seja

$$T = \{M_i : M_i \text{ é maximal em } A \text{ e } P \subsetneq M_i\}$$

Diante do exposto, $T \neq \phi$. Por iv) $P = \cap M_i$ onde $M_i \in T$.

Agora, temos: $(0) = \cap\ (M_i/P) \quad (M_i \in T)$

Por outro lado, A/P é um G-domínio, logo temos $P(A/P) \neq (0)$. Temos então uma contradição, pois:

$$(0) \neq P(A/P) \subset \cap(M_i/P) = (0) .$$

3.1.4 COROLÁRIO

Se A é um anel de Hilbert com um número finito de ideais maximais então $\dim A = 0$.

DEMONSTRAÇÃO:

Se P é um ideal primo de A temos $P = \bigcap_{1}^{k} M_i$ onde cada M_i $(1 \leq i \leq k)$ é maximal em A.

Se $\dim A > 0$ existe P ideal primo de A tal que $P \subset M_i$ (inclusão estrita), para todo M_i ideal maximal de A.

Assim podemos encontrar $x_i \in M_i$ $(i = 1,2,\ldots,k)$ e $x_i \notin P$.

Mas então $\prod_{1}^{k} x_i \in M_1.M_2.\ldots.M_k \subset \bigcap_{1}^{k} M_i = P$

uma contradição. Assim, P deve ser maximal e $\dim A = 0$.

OBSERVAÇÕES:

i) $K[\![x]\!]$, (K corpo) não é anel de Hilbert pois $\dim K[\![x]\!] = 1$. No entanto $K[\![x]\!]$ é local. (1.2.14)

ii) $\mathbb{Z}$ é um anel de Hilbert (com $\dim \mathbb{Z} = 1$) pois todo ideal primo não nulo de $\mathbb{Z}$ é maximal. Observe que (0) é primo mas não é G-ideal.

iii) Se K é corpo então $K[x]$ é um anel de Hilbert por (1.2.4) e (1.2.6).

3.1.5 PROPOSIÇÃO:

Seja A um PID e $L = \{p \in A: p$ é irredutível$\}$. Então A é um anel de Hilbert se, e somente se, $|L| = \infty$.

DEMONSTRAÇÃO:

Se A é um anel de Hilbert e $L = \{p_1, p_2, \ldots, p_n\}$ é um conjunto finito então p_iA $(i = 1, 2, \ldots, n)$ são os únicos ideais primos não nulos de A.

Como (0) é um ideal primo de A e A é um anel de Hilbert, devemos ter, por (3.1.3, (iii))

$$(0) = \cap\, p_iA$$

Mas $0 \neq x \in \cap\, p_iA$, onde $x = \Pi\, p_i$ o que é absurdo.

Reciprocamente, como A é um PID qualquer ideal primo não nulo é maximal e portanto verifica (3.1.3, (iii) Tambem o ideal primo (0) é tal que (1.2.5)

$$(0) = \cap\, pA$$

onde $p \in L$.

Assim A é um anel de Hilbert.

3.1.6 PROPOSIÇÃO

Seja $\phi: A \to B$ um homomorfismo. Se A é um anel de Hilbert então $\phi(A) = S \subset B$ é um anel de Hilbert.

DEMONSTRAÇÃO:

Como existe uma correspondência biunívoca entre ideais de A que contem $\mathrm{Ker}\phi$ e ideais de S, correspondência esta que preserva a ordem, segue o resultado uma vez que a G-ideais correspondem G-ideais e que a ideais maximais correspondem ideais maximais (2.2.4)

3.1.7 COROLÁRIO.

Se A é um G-domínio e um anel de Hilbert então A é um corpo.

DEMONSTRAÇÃO:

Como $A = A/(0)$ é um G-domínio, segue-se que (0) é um G-ideal de A. Como A é um anel de Hilbert, (0) é maximal e portanto, A é um corpo.

3.1.8 PROPOSIÇÃO

Sejam $A \subset B$ anéis com B integral sobre A. Então A é um anel de Hilbert, se, e somente se, B é um anel de Hilbert.

DEMONSTRAÇÃO:

Seja A um anel de Hilbert, P um G-ideal de B e $P' = P \cap A$.

Como B/P é integral sobre A/P' (1.3.6) e B/P é um G-domínio segue de (2.1.11) que A/P' é um G-domínio e portanto P' é maximal. Por (1.3.8) P é maximal.

Reciprocamente, se P' é um G-ideal de A, e como B é integral sobre A, existe P ideal primo de B tal que $P \cap A = P'$ (1.3.8). Como B/P é integral sobre A/P' e A/P' é um G-domínio então B/P é um G-domínio (2.1.11). Como B é um anel de Hilbert temos P maximal e por (1.3.8) P' é maximal.

3.1.9 PROPOSIÇÃO

Seja A um anel comutativo e x uma indeterminada sobre A. Então A é um anel de Hilbert se, e somente se para todo ideal maximal M de $A[x]$, $M \cap A$ é maximal em A.

DEMONSTRAÇÃO:

Assuma que A é um anel de Hilbert e seja M um ideal maximal de $A[x]$ com $N = M \cap A$. Por (2.2.7) N é um G-ideal de A e portanto N é maximal.

Reciprocamente, seja P um G-ideal de A. Utilizando (2.2.7), existe M_o ideal maximal de $A[x]$ tal que $M_o \cap A = P$. Por hipótese, P é maximal e A é, portanto, um anel de Hilbert.

OBSERVAÇÃO: Temos $Z \subset Q$ anéis de Hilbert, (0) ideal maximal de Q mas $(0) \cap Z = (0)$ não é um ideal maximal de Z.

3.1.10 PROPOSIÇÃO

Se A é um anel de Hilbert e todo ideal maximal de A é finitamente gerado então todo ideal de A[x] é finitamente gerado.

DEMONSTRAÇÃO:

Seja M um ideal maximal de A[x]. Por (3.1.9) $M \cap A$ é maximal e portanto finitamente gerado. Assim, usando (2.2.8) temos que M pode ser gerado por $M \cap A$ e mais um elemento f de A[x]. Portanto M é finitamente gerado.

3.1.11 PROPOSIÇÃO

Seja A um domínio e x uma indeterminada sobre A. Então A[x] é um anel de Hilbert se A é um anel de Hilbert e $M \cap A = (0)$ para todo G-ideal M de A[x].

DEMONSTRAÇÃO:

Seja M um G-ideal de A[x]. Precisamos provar que M é maximal. Consideremos o homomorfismo natural:

$$\phi : A[x] \to A[x]/M$$

e seja $u = \phi(x) = x + M$. Assim, como $M \cap A = (0)$

$$A[u] \equiv (A/M\cap A)[u] \equiv A[x]/M$$

Como M é um G-ideal de A[x], A[u] é um G-domínio. Por (2.1.13) u é algébrico sobre A e A é um G-domínio. Como A é um anel de Hilbert (3.1.7) A é um corpo.

Assim, $A[u] \equiv A[x]/M$ é um corpo (1.4.6) e portanto M é maximal.

3.1.12 TEOREMA

Seja A um anel comutativo e x uma indeterminada sobre A. Então A[x] é um anel de Hilbert se, e somente se, A é um anel de Hilbert.

DEMONSTRAÇÃO:

Se A[x] é um anel de Hilbert, seja

$$\phi : A[x] \to A$$
$$p(x) \to p(0)$$

Facilmente se vê que ϕ é um homomorfismo sobrejetor. Assim (3.1.6) A é um anel de Hilbert.

Reciprocamente, seja M um G-ideal de $A[x]$ e

$$N = M \cap A$$

Como A é um anel de Hilbert, A/N é um anel de Hilbert (3.1.6). Da proposição anterior (3.1.11) temos $(A/N)[x]$ é um anel de Hilbert, já que N é primo como contração de um ideal primo.

Consideremos o homomorfismo natural

$$\lambda : A[x] \to A[x]/NA[x] \equiv (A/N)[x]$$

Como M é um G-ideal de $A[x]$ sua imagem $M/NA[x]$ é um G-ideal de $(A/N)[x]$ e portanto maximal. Mas então M é maximal (2.2.4)

O seguinte corolário segue imediatamente:

3.1.13 COROLÁRIO

Seja A um anel comutativo e $x_1, x_2, \ldots, x_n$ um conjunto finito de indeterminadas sobre A. Então A é um anel de Hilbert se, e somente se, $A[x_1, x_2, \ldots, x_n]$ é um anel de Hilbert.

3.1.14 PROPOSIÇÃO

$A[[x]]$ não é um anel de Hilbert.

DEMONSTRAÇÃO:

Seja M um ideal maximal de A e considere

$$M^* = \{\sum_0^\infty a_i x^i : a_i \in M\}$$

M^* é um ideal primo de $A[[x]]$ (1.2.10) e verificamos que $M^* \subset (M,x)$ (inclusão estrita) pois $x \notin M^*$.

Agora, se $A[[x]]$ é um anel de Hilbert então $A[[x]]/M^*$ tambem é um anel de Hilbert (3.1.6).

Ocorre que $A[[x]]/M^*$ só tem um ideal maximal, que é $(M,x)/M^*$. (Realmente, se Q é um ideal maximal de

$A[\![x]\!]/M^*$ então existe um ideal maximal Q' em $A[\![x]\!]$ tal que $Q'/M^* = Q$. Mas, por (1.2.11) $Q' = \langle M,x \rangle$ pois Q' tambem corresponde a M em A.)

Finalmente, (3.1.4) dim $A[\![x]\!]/M^* = 0$ o que é absurdo pois M^* é primo, $M^* \subset \langle M,x \rangle$ donde decorre que

$$(\overline{0}) \subset \langle M,x\rangle/M^* \quad \text{(inclusão estrita)}$$

e portanto dim $A[\![x]\!]/M^* > 0$.

3.2 ANÉIS DE HILBERT NOETHERIANOS

O objetivo deste paragrafo e responder a seguinte questão: "Quando é que um anel noetheriano é um anel de Hilbert?".

Para responder tal pergunta, o resultado básico deste parágrafo é o "Teorema do Ideal Principal" de Krull

Para um bom entendimento do que trataremos agora, é indispensável um conhecimento da Teoria dos Módulos

Se A é um domínio e $u,v \in A$, podemos considerar

$$(u,v)/(u)$$

como um A-módulo, bem como o faremos com $(u^2,uv)/(u^2)$ $(u)/(u^2)$, $(u^2,v)/(u^2,uv)$ etc.

Após essas observações, temos:

3.2.1 LEMA

Sejam u,y elementos não nulos do domínio A. Então:

a) Os A-módulos $(u,y)/(u)$ e $(u^2,uy)/(u^2)$ são isomorfos;

b) Os A-módulos $(u)/(u^2)$ e $(u^2,y)/(u^2,uy)$ são isomorfos se for válida a condição adicional (*)

$$(*)\quad tu^2 \in (y) \Rightarrow tu \in (y) \quad \text{para } t \in A.$$

DEMONSTRAÇÃO:

a) Seja $\phi: (u,y) \to (u^2,uy)/(u^2)$ a aplicação definida por $\phi(x) = xu + (u^2)$ para todo $x \in (u,y)$.

Claramente, ϕ é um homomorfismo sobrejetor pois se $v \in (u^2,uy)/(u^2)$ então

$$\begin{aligned} v &= au^2 + buy + (u^2), \ (a,b \in A) \\ &= (au + by)u + (u^2) \\ &= \phi(au + by) \end{aligned}$$

Afirmamos que $\mathrm{Ker}\phi = (u)$. Realmente,

$$\phi(au) = au^2 + (u^2) = (u^2)$$ e se

$\phi(au + by) = \overline{0} = (u^2)$ então $au^2 + buy \in (u^2)$ e dai tiramos $buy = ru^2$ para algum $r \in A$, e portanto,

$$au + by = au + ru = (a + r)u \in (u).$$

Finalmente, pelo Teorema do Isomorfismo:

$$(u,y)/\ker\phi = (u,y)/(u) \cong (u^2,uy)/(u^2)$$

b) Temos, evidentemente,

$$(u)/(u^2) = \{au + (u^2) : a \in A\} = \{a\bar{u}: a \in A\} = \bar{u}A$$

e

$$(u^2,y)/(u^2,uy) = \{ay + (u^2,uy) : a \in A\} = \bar{y}A$$

Definamos ϕ: $\bar{u}A \to \bar{y}A$ por $\phi(a\bar{u}) = a\bar{y}$ para todo $a \in A$.

É evidente que ϕ é um A-módulo homomorfismo sobrejetor. Se for válida a condição (*) veremos que ϕ é injetora. Realmente, se $\phi(a\bar{u}) = \bar{0}$, isto é, $ay \in (u^2,uy)$ então existem $c, d \in A$ tal que:

$$ay = cu^2 + duy \qquad \text{e dai}$$

$$(a - du)y = cu^2 \qquad \text{donde tiramos}$$

que $cu^2 \in (y)$. A condição (*) nos dá então $cu \in (y)$, isto é, $cu = ey$ para algum $e \in A$.

Assim, $ay = (cu)u + duy = euy + duy = (e + d)uy$.

Como $y \neq 0$ e A é um domínio, temos:

$$a = (e + d)u \qquad \text{e portanto}$$

$$a \in (u)$$

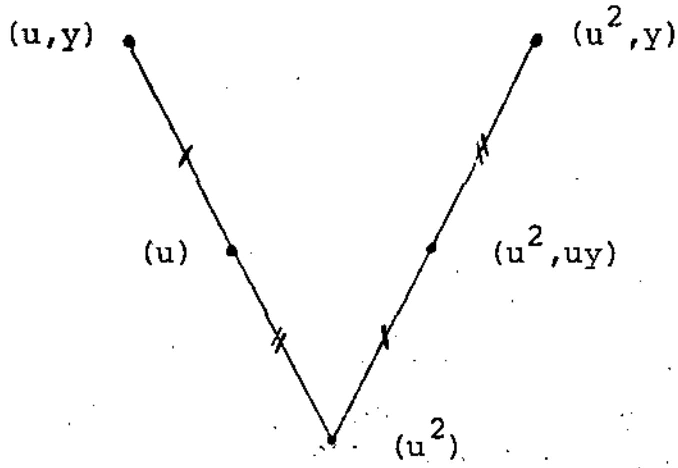
Mas se isto ocorre, isto é, $a = hu$ para algum $h \in A$ então:

$$a\bar{u} = (hu)u + (u^2) = (u^2).$$

Portanto, na presença de (*) temos:

$$(u)/(u^2) \cong (u^2,y)/(u^2,uy).$$

O diagrama da página seguinte esclarece melhor o que foi provado.



Temos então que $(u,y)/(u^2)$ e $(u^2,y)/(u^2)$ são isomorfos "por pedaços" na presença de (*).

3.2.2 TEOREMA

Se A é um domínio noetheriano local com ideal maximal M, se $x \in M$ é não nulo e M é um primo minimal sobre o ideal (x) então posto $M \leq 1$.

DEMONSTRAÇÃO:

Se assumirmos o contrário, existe Q primo tal que

$$M \supset Q \supset (0) \quad \text{(inclusão estrita)}$$

Escolhamos $y \in Q$, $y \neq 0$ e consideremos

$$I_k = \{t \in A : tx^k \in (y),\ k \in \mathbb{N}\}$$

É facil ver que cada I_k é um ideal de A e que

$$I_1 \subset I_2 \subset I_3 \subset \dots \subset I_n \subset \dots$$

Como A é noetheriano, existe $n \in \mathbb{N}$ tal que

$$I_n = I_{n+1} = \dots$$ e, em particular

$$I_n = I_{2n}$$

Seja $u = x^n$. Então teremos:

(*) $tu^2 \in (y) \Rightarrow tu \in (y)$ para todo $t \in I_n$.

$$
\begin{tikzcd}
A \arrow[r] \arrow[d, dash] & A/(u^2) = T \arrow[d, dash] \\
M \arrow[r, dash] \arrow[d, dash] & M/(u^2) \arrow[d, dash] \\
(u) \arrow[r, dash] \arrow[d, dash] & (u)/(u^2) \arrow[d, dash] \\
(u^2) \arrow[r, dash] & (\overline{0})
\end{tikzcd}
$$

No diagrama acima, $M/(u^2)$ é o único ideal primo não nulo do anel $T = A/(u^2)$, pois se houvesse um outro $N/(u^2)$ deveríamos ter $N/(u^2) \subset M/(u^2)$ e sua pré-imagem N (um ideal primo de A) deveria conter (u^2), isto é, $u^2 = x^{2n} \in N$ e portanto $x \in N$, e assim M não seria minimal sobre (x). Portanto $\dim T = 0$ e, é claro, T é noetheriano.

Por (1.5.8) qualquer T-módulo finitamente gerado tem comprimento finito.

Considere o A-módulo $(u,y)/(u^2)$, cujo anulador é (u^2): podemos pensá-lo como um $A/(u^2)$-módulo, isto é, como um T-módulo. O mesmo se passa com $(u^2,y)/(u^2)$.

Então, desde que $(u,y)/(u^2)$ e $(u^2,y)/(u^2)$ são isomorfos "por pedaços" (3.2.1) devem ter o mesmo comprimento.

Assim, temos: $(u,y) = (u^2,y)$, isto é,
$u \in (u^2,y)$ e portanto
$u = ru^2 + sy$ para algum $r,s \in A$. Donde concluímos que $(1 - ru)u \in (y)$, e como $u = x^n \in M = J(A)$ segue-se que $1 - ru$ é unidade de A (1.1.11) e portanto $u \in (y) \subset Q$.

Assim, $u = x^n \in Q \Rightarrow x \in Q$ uma contradição pois M é minimal sobre (x).

3.2.3 COROLÁRIO (TEOREMA do IDEAL PRINCIPAL de KRULL)

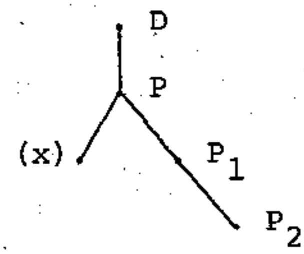
Seja D um anel noetheriano, $x \neq 0$ uma não-unidade de D e P um ideal primo minimal sobre o ideal (x). Então posto $P \leq 1$.

DEMONSTRAÇÃO:

Se supomos o contrário, existem P_1 e P_2 ideais primos de D tal que :

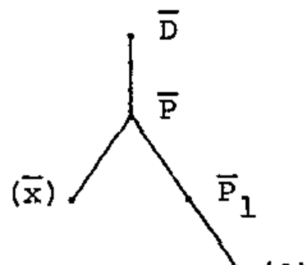
$$P \supset P_1 \supset P_2 \quad \text{(inclusão estrita)}$$

e de tal modo que $x \notin P_2$, conforme diagrama:



Consideremos o quociente $D/P_2 = \overline{D}$. Como D é noetheriano (1.5.4) $\overline{D}$ é um domínio noehteriano.

A aplicação de (1.1.15) nos assegura que o ideal $\overline{P} = P/P_2$ é minimal sobre $(\overline{x}) = (x)/P_2$. Ao final teríamos a seguinte situação:



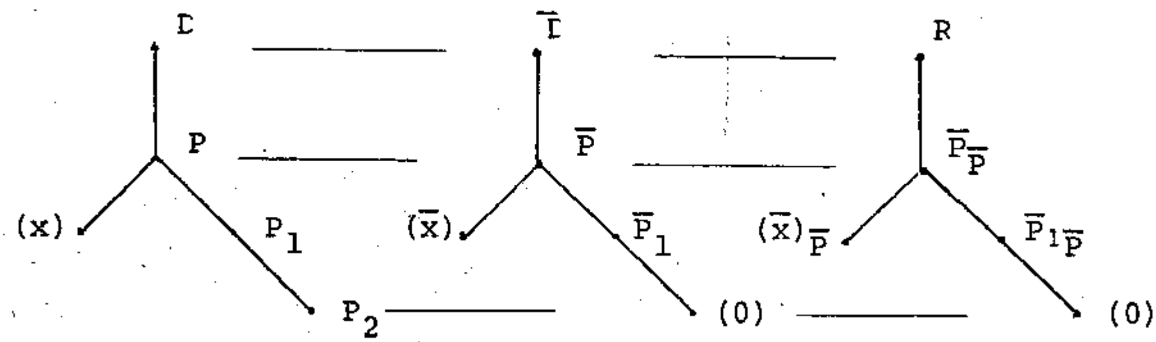
com $\overline{P}$ minimal sobre $(\overline{x})$ e $\overline{D}$ um domínio noetheriano.

Façamos agora uma localização em $\overline{P}$, isto é, consideremos

$$R = \overline{D}_{\overline{P}}$$

Por (1.5.5) R é um domínio noetheriano local com ideal maximal $\overline{P}_{\overline{P}}$. Dado que existe uma correspondência (que preserva a ordem) entre ideais primos de $\overline{D}$ contidos em $\overline{P}$ e ideais primos de R (1.1.25) segue que $\overline{P}_{\overline{P}}$ é minimal sobre $(\overline{x})_{\overline{P}}$.

O diagrama a seguir resume o que fizemos:



Mas nesta situação final aplica-se o lema anterior (3.2.2) e não podemos ter

$$\overline{P}_{\overline{P}} \supset \overline{P}_{\overline{P}} \supset (0)_{\overline{P}}$$

e consequentemente não podemos ter

$$P \supset P_1 \supset P_2$$

donde segue que posto $P \leq 1$.

3.2.4 LEMA

Sejam P, Q ideais primos num anel noetheriano A com $P \subset Q$. Se existe I ideal primo de A com $P \subset I \subset Q$ (inclusão estrita) então existe uma infinidade deles na mesma situação.

DEMONSTRAÇÃO:

A passagem a A/P (o que mantem todas as hipóteses) permite que consideremos $P = (0)$.

Se aceitarmos a existência de um número finito

$$P_1, P_2, \ldots, P_n$$

de ideais primos tal que

$$(0) \subset P_i \subset Q \quad \text{(inclusão estrita)}$$

então, por (1.1.7) não podemos ter $Q \subset \bigcup_1 P_i$ de modo que podemos obter $x \in Q$, $x \notin P_i$ ($i = 1, 2, \ldots, n$).

Mas então Q é minimal sobre (x) e a suposição de que existe I tal que $Q \supset I \supset (0)$ nos fornece posto de $Q \geq 2$, em contradição ao Teorema do Ideal Principal de Krull.

3.2.5 LEMA

Seja A um domínio noetheriano. Suponhamos que A tem um número infinito de ideais primos minimais. Então a intersecção deles é o ideal (0).

DEMONSTRAÇÃO:

Seja $\{P_i, i \in \Lambda\}$ o conjunto dos ideais primos minimais de A, com $|\Lambda| = \infty$.

Se $0 \neq x \in P_i$ então P_i é minimal sobre (x) para todo $i \in \Lambda$ em contradição com (1.5.10).

3.2.6 TEOREMA

Um domínio noetheriano A é um G-domínio se, e somente se, dim $A \leq 1$ e A tem só um número finito de ideais maximais.

DEMONSTRAÇÃO:

Se A é um G-domínio então $P(A) \neq (0)$ e então A só pode ter um número finito de ideais primos minimais em conformidade com (3.2.5).

Suponha que exista algum ideal primo P de posto 2. Então existe Q tal que $P \supset Q \supset (0)$ (inclusão estrita). Mas então (3.2.4) nos assegura a existência de uma infinidade de ideais nessa situação (minimais) em contradição com a primeira parte desta demonstração. Assim devemos ter dim $A \leq 1$ e todos os ideais minimais são maximais.

Reciprocamente, como dim $A \leq 1$ e A é domínio temos que (0) é ideal primo e toda cadeia maximal de ideais primos devem ter no máximo dois "elos", isto é, da forma

$$(0) \subset P$$

Assim, todo ideal primo não nulo é maximal e por hipótese, A só tem um número finito de ideais primos. Assim (2.1.5) nos garante que A é um G-domínio.

3.2.7 TEOREMA

Uma condição necessária e suficiente para que um anel noetheriano A seja um anel de Hilbert é: "Para todo ideal primo P tal que dim(A/P) = 1 existe uma infinidade de ideais maximais contendo P".

DEMONSTRAÇÃO:

Seja P tal que dim(A/P) = 1. Como A é um anel de Hilbert, A/P é um anel de Hilbert. Se A/P tem só um número finito de ideais maximais, segue (3.2.6) que A/P é um G-domínio e portanto P é um G-ideal (2.2.1). Assim P é maximal e A/P é um corpo, donde dim(A/P) = 0 , um absurdo.

Reciprocamente, seja P um G-ideal de A. Então A/P é um G-domínio noetheriano e por (3.2.6) dim(A/P) $\leq$ 1 e existe só um número finito de ideais primos em A/P. Mas então não pode ser dim(A/P) = 1 e portanto temos que dim(A/P) = 0 e A/P é corpo. Assim P é maximal e A é um anel de Hilbert.

3.3 HILBERT NULLSTELLENSATZ

Este parágrafo será dedicado ao "TEOREMA do NÚMERO de ZEROS" de Hilbert - o famoso HILBERT NULLSTELLENSATZ (Ver [5], [8])

Na pesquisa bibliográfica que empreendemos encontramos diversos enunciados equivalentes ao HILBERT NULLSTELLENSATZ. No próximo teorema provaremos todas essas formas.

3.3.1 TEOREMA (HILBERT NULLSTELLENSATZ)

Seja K um corpo, L seu fêcho algébrico e $\{x_1,x_2,\dots,x_n\}$ um conjunto finito de indeterminadas sobre K. Então:

i) $K[x_1,x_2,\dots,x_n]$ é um anel de Hilbert;

ii) Se M é um ideal maximal de $K[x_1,x_2,\dots,x_n]$ então

$$T = K[x_1,x_2,\dots,x_n]/M$$

é um corpo algébrico sobre K de $\dim_K T = n + 1$;

iii) Seja B uma K-álgebra finitamente gerada. Se B é um corpo então B é uma extensão algébrica finita de K;

iv) Os únicos ideais maximais de $L[x_1,x_2,\dots,x_n]$ são da forma $(x_1-a_1, x_2-a_2,\dots,x_n-a_n)$, com $a_i \in L$;

v) Sejam $f, g_1,g_2,\dots,g_r \in L[x_1,x_2,\dots,x_n]$. Se f se anula em todos os zeros comuns de $g_1,g_2,\dots,g_r$ então existe $n \in \mathbb{N}$ tal que $f^n \in (g_1,g_2,\dots,g_r)$;

vi) As polinomiais $f_1,f_2,\dots,f_r \in L[x_1,x_2,\dots,x_n]$ não tem zeros comuns se, e somente se, $(f_1,f_2,\dots,f_r)$ coincide com $L[x_1,x_2,\dots,x_n]$.

DEMONSTRAÇÃO:

i) Como K é um corpo, é um anel de Hilbert. Mas então (3.1.13) nos garante que $K[x_1,x_2,\dots,x_n]$ é um anel de Hilbert;

ii) Inicialmente temos $M \cap K = (0)$ donde segue que $K/(M \cap K) \cong K$.

Considere agora

$$K \xrightarrow{i} K[x_1,x_2,\ldots,x_n] \xrightarrow{\phi} T = K[x_1,x_2,\ldots,x_n]/M$$

onde i é a inclusão e ϕ é o homomorfismo natural. Se $h = \phi i$ temos que h é um homomorfismo injetor (pois $M \cap K = (0)$) o que permite considerar K como subcorpo de T.

Agora,

$$T = K[x_1,x_2,\ldots,x_n]/M \cong (K/M \cap K)[\bar{x}_1,\bar{x}_2,\ldots,\bar{x}_n]$$

$$\cong K[\bar{x}_1,\bar{x}_2,\ldots,\bar{x}_n]$$

onde $\bar{x}_1,\bar{x}_2,\ldots,\bar{x}_n$ são os M-resíduos de $x_1,x_2,\ldots,x_n$ isto é, $\bar{x}_i = x_i + M$.

Assim T é uma extensão de anéis finitamente gerada de K e uma aplicação de (2.1.13) fornece $\bar{x}_1,\bar{x}_2,\ldots,\bar{x}_n$ algébricos sobre K.

Como $\beta = \{1, \bar{x}_1,\bar{x}_2,\ldots,\bar{x}_n\}$ é uma base para o espaço vetorial T sobre o corpo K, temos $\dim_K T = n + 1$;

iii) Como B é uma K-álgebra finitamente gerada, por definição, existe $h : K[x_1,x_2,\ldots,x_n] \to B$, um homomorfismo sobrejetor. Como B é corpo e

$$B \cong K[x_1,x_2,\ldots,x_n]/\operatorname{Ker} h$$

segue que $\ker h$ é maximal. Assim, valem as hipóteses de (ii) e B é uma extensão algébrica finita de K;

iv) Por (1.4.12) os ideais $(x_1-a_1,\ldots,x_n-a_n)$ são maximais em $L[x_1,x_2,\ldots,x_n]$. Resta mostrar que um ideal maximal M de $L[x_1,x_2,\ldots,x_n]$ é da forma em questão.

Utilizaremos indução sobre n.

Para $n = 1$ o resultado é imediato (1.4.11).

Admitamos o resultado válido para todo $k < n$ e seja $R = L[x_1,x_2,\ldots,x_{n-1}]$. R é um anel de Hilbert por (i).

Se M é um ideal maximal de $R[x_n]$ então o ideal $N = M \cap R$ é maximal (3.1.9). Pela hipótese de indução temos:

$$N = (x_1 - a_1, x_2 - a_2, \ldots, x_{n-1} - a_{n-1})$$

Mas então (2.2.8) M pode ser gerado por N e mais um elemento f de $R[x_n]$ tal que a imagem de f em $(R/N)[x_n] \cong L[x_n]$ por (ii) seja irredutível. Portanto $f = x_n - a_n$ com $a_n \in L$ e então

$$M = (x_1 - a_1, x_2 - a_2, \ldots , x_n - a_n)$$

v) Se $(a_1,a_2,\ldots,a_n) \in L^n$ é um zero comum de $g_1,g_2,\ldots,g_r$ então $f, g_1, g_2,\ldots, g_r \in (x_1 - a_1,\ldots,x_n-a_n)$ um ideal maximal de $L[x_1,x_2,\ldots,x_n]$ e portanto f pertence a todo ideal maximal de $L[x_1,x_2,\ldots,x_n]$ que contem o ideal $I = (g_1, g_2, \ldots, g_r)$ e consequentemente à intersecção desses ideais maximais. Por (2.2.5) a intersecção de todos os ideais maximais (ou de G-ideais, no caso) é o radical de I. Assim $f \in r(I)$ e portanto existe $n \in \mathbb{N}$ tal que

$$f^n \in I = (g_1,g_2,\ldots,g_r)$$

vi) Se $(f_1,f_2,\ldots,f_r) \neq L[x_1,x_2,\ldots,x_n]$ existe um ideal maximal M de $L[x_1,x_2,\ldots,x_n]$ tal que

$$(f_1,f_2,\ldots,f_r) \subset M$$

Como $M = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ segue que $f_i(a_1,a_2,\ldots,a_n) = 0$ para todo $i = 1,2, \ldots, r$ e portanto as polinomiais em questão tem um zero em comum.

3.3.2 COROLÁRIO

Seja K um corpo algebricamente fechado e seja $R = K[x_1,x_2,\ldots,x_n]$. Sejam $f_1, f_2, \ldots f_r \in R$. As equações

$$f_i = 0 \quad (i = 1, 2, \ldots, r)$$

tem solução comum se, e somente se, não existem $g_1,g_2,\ldots, g_r$ elementos de R com

$$f_1g_1 + f_2g_2 + \ldots + f_rg_r = 1$$

DEMONSTRAÇÃO:

Se as equações $f_i = 0$ ($i = 1, 2, \ldots, r$)

não tem solução comum então (3.3.1, vi) devemos ter que

$$(f_1, f_2, \ldots, f_r) = R$$

e portanto existem $g_i \in R$ ($i = 1, 2, \ldots, n$) tal que

$$f_1 g_1 + f_2 g_2 + \ldots + f_r g_r = 1$$

Por outro lado, se $(a_1, a_2, \ldots, a_n)$ é uma solução comum de $f_i = 0$ ($i = 1,2,\ldots,n$) então para todo $g_i \in R$ ($i = 1,2,\ldots,n$) teremos:

$$1 = \sum_1^n f_i(a_1, a_2, \ldots, a_n) g_i(a_1, a_2, \ldots, a_n) = 0$$

o que é uma contradição.

3.3.3 PROPOSIÇÃO

Seja K um corpo (não necessariamente algebricamente fechado). Então um ideal maximal de $R = K[x_1, x_2 \ldots, x_n]$ pode ser gerado por n elementos.

DEMONSTRAÇÃO:

Faremos a demonstração por indução sobre n.

. Se $n = 1$ temos que $K[x_1]$ é um PID e portanto um ideal maximal é gerado por um elemento.

Assumindo o resultado para todo $k < n$ temos:

$$R = K[x_1, x_2, \ldots, x_n] \equiv K[x_1, x_2, \ldots, x_{n-1}][x_n]$$

onde lembramos que R e $K[x_1, x_2, \ldots, x_{n-1}]$ são anéis de Hilbert.

Se M é um ideal maximal de R, temos:

$$M \cap K[x_1, x_2, \ldots, x_{n-1}] = N$$

é maximal em $K[x_1, x_2, \ldots, x_{n-1}]$ (3.1.9) e pela hipótese de indução é gerado por n-1 elementos. Finalmente, por (2.2.8) M pode ser gerado por N e mais um elemento $f \in R$ e portanto M é gerado por n elementos.

3.3.4 PROPOSIÇÃO

Seja A um anel de Hilbert tal que todo ideal maximal de A pode ser gerado por k elementos. Então qualquer ideal maximal de $A[x_1, x_2, \ldots, x_n]$ pode ser gerado por $k + n$ elementos.

DEMONSTRAÇÃO:

Faremos a demonstração por indução sobre n.

Se $n = 1$ então, como A e $A[x_1]$ são anéis de Hilbert, a contração de um ideal maximal M de $A[x_1]$ em A é maximal (3.1.9). Assim, (2.2.8) se aplica e M pode ser gerado por $k + 1$ elementos.

Assuma-se o resultado para todo $k < n$ e proceda-se como no lema anterior.

3.3.5 PROPOSIÇÃO

Seja M um ideal maximal em $T = A[x_1, x_2, \ldots, x_n]$ tal que $M \cap A = (0)$. Então M pode ser gerado por $n + 1$ elementos.

DEMONSTRAÇÃO:

Por (2.1.15) A é um G-domínio e então K, o corpo quociente de A é tal que $K = A[u^{-1}]$ com $u \in A$, $u \neq 0$.

Como $u \in A \subset T$ temos $\bar{u} \in T/M$ e $\bar{u} \neq 0$ (pois por hipótese $M \cap A = (0)$). Assim, existe $\bar{g} \in T/M$ tal que $\bar{u}\bar{g} = \bar{1}$ o que nos permite considerar $g \in T$ de modo que $ug - 1 \in M$.

Seja $S = T/(ug-1)$ e $\phi : K \to S$ definida por:

$\phi(r) = \bar{r} = r + (ug-1)$ para todo $r \in A$ e

$\phi(u^{-1}) = \bar{g} = g + (ug-1)$, um homomorfismo não nulo.

Então ϕ é injetor (1.4.4) e portanto S contem uma cópia de K. Assim, $S \cong \phi(K)[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n] \cong K[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n]$ onde $\bar{x}_i = x_i + (ug-1)$.

Agora, se M é maximal em T, sua imagem em S é $M/(ug-1)$ que é maximal pois:

$$[T/(ug-1)]/[M/(ug-1)] \cong T/M$$

que é um corpo. Agora, por (3.3.3) $M/(ug-1)$ pode ser gerado por n elementos e consequentemente M pode ser gerado por $n+1$ elementos.

A P Ê N D I C E

HILBERT NULLSTELLENSATZ e GEOMETRIA ALGÉBRICA

Neste apêndice provaremos alguns resultados elementares da Geometria Algébrica utilizando-nos dos resultados obtidos nos capítulos anteriores. Um dos objetivos deste apêndice é examinar as versões algebro-geométricas do HILBERT - NULLSTELLENSATZ (Teorema A-5 e A-6).

Sejam: K um corpo algebricamente fechado, K^n o K - espaço vetorial das n-uplas sobre K e $K[x_1,x_2,\ldots,x_n]$ o anel dos polinômios em n variáveis sobre K.

A.1 DEFINIÇÃO

Se I é um ideal de $K[x_1,x_2,\ldots,x_n]$, seja:

$$V(I) = \{(a_1,a_2,\ldots,a_n) \in K^n : f(a_1,a_2,\ldots,a_n) = 0,\ \forall f \in I\}$$

O conjunto $V(I)$ será denominado uma VARIEDADE ALGÉBRICA AFIM ou simplesmente VARIEDADE.

OBSERVAÇÕES: i) Se $I = K[x_1,x_2,\ldots,x_n]$ então $V(I) = \phi$;
ii) Se $I = (0)$ então $V(I) = K^n$.

A.2 DEFINIÇÃO

Se $S \subset K^n$, seja:

$$J(S) = \{f \in K[x_1,x_2,\ldots,x_n] : f(a_1,a_2,\ldots,a_n)=0\ \forall (a_1,\ldots,a_n) \in S\}$$

O conjunto $J(S)$ denomina-se IDEAL da variedade S.

OBSERVAÇÕES: i) Se $S = K^n$ então $J(S) = (0)$;
ii) Se $S = \phi$ então $J(S) = K[x_1,x_2,\ldots,x_n]$.

A.3 LEMA

Com as notações anteriores, temos:

i) Se $S \subset K^n$ então $J(S)$ é um ideal de $K[x_1,x_2,\ldots,x_n]$

ii) Se $S \subset T$ então $J(T) \subset J(S)$;

iii) Se $P \subset Q$ são ideais de $K[x_1,x_2,\ldots,x_n]$ então vale $V(Q) \subset V(P)$;

iv) Se I é um ideal de $K[x_1,x_2,\ldots,x_n]$ então temos $J(V(I)) \supset I$;

v) Se $S \subset K^n$ então $V(J(S)) \supset S$.

DEMONSTRAÇÃO:

Imediatas, a partir das definições.

A.4 LEMA

Nas notações anteriores, temos:

i) $V(I) = V(r(I))$, para todo I ideal de $K[x_1,x_2,\ldots,x_n]$;

ii) $V(I \cap J) = V(I) \cup V(J)$ para todos I,J ideais de $K[x_1,x_2,\ldots,x_n]$;

iii) $V(\sum_{\alpha\in\Lambda} I\alpha) = \bigcap_{\alpha} V(I\alpha)$ onde $\{I\alpha\}_{\alpha\in\Lambda}$ é uma família de ideais de $K[x_1,x_2,\ldots,x_n]$.

DEMONSTRAÇÃO:

i) Como $I \subset r(I)$ temos $V(I) \supset V(r(I))$ por (A.3 ii).

Por outro lado, se $P \in V(I)$ então $f(P) = 0$ para todo $f \in I$ donde $g(P) = 0$ para todo $g \in r(I)$ já que $g^n \in I$ para algum $n \in \mathbb{N}$, e $g^n(P) = [g(P)]^n = 0$ o que fornece $g(P) = 0$.

Assim, $V(I) \subset V(r(I))$ e temos a igualdade.

ii) Como $I \cap J \subset I$ e $I \cap J \subset J$ temos (A.3, iii) que $V(I \cap J) \supset V(I)$ e $V(I \cap J) \supset V(J)$ donde $V(I \cap J) \supset V(I) \cup V(J)$.

Reciprocamente, se existe $P \in V(I \cap J) - V(I) \cup V(J)$ então existem $g \in I$ e $h \in J$ tal que $g(P) \neq 0$ e $h(P) \neq 0$, mas com $f = gh \in IJ \subset I \cap J$. Mas então temos $f(P) = g(P)h(P) = 0$ o que implica $g(P) = 0$ ou $h(P) = 0$, um absurdo. Assim, temos:

$$V(I \cap J) \subset V(I) \cup V(J).$$

iii) Como $I\alpha \subset \sum_{\alpha\in\Lambda} I\alpha$, para todo $\alpha \in \Lambda$ temos que (A.3) $V(\sum_{\alpha\in\Lambda} I\alpha) \subset \bigcap_{\alpha} V(I\alpha)$.

Seja $P \in \bigcap_{\alpha} V(I_\alpha)$. Se $g \in \sum_{\alpha\in\Lambda} I\alpha$ então $g = \sum t\alpha f\alpha$ onde $t_\alpha \in K[x_1,x_2,\ldots,x_n]$ e $f\alpha \in I\alpha$ e todos os t_α são nulos, exceto um número finito. Mas nessas condições, temos:

$$g(P) = \sum t_\alpha(P) f_\alpha(P) = 0$$

e daí segue que $P \in V(\sum_{\alpha\in\Lambda} I\alpha)$.

OBSERVAÇÃO: Seja $T = \{V(I)\colon I$ é um ideal de $K[x_1,x_2,\ldots,x_n]\}$. Então (K^n,T) é um espaço topológico onde os $V(I)$ são os fechados de K^n.

A.5 TEOREMA (Forma Fraca do HILBERT NULLSTELLENSATZ)

Seja I um ideal próprio de $K[x_1,x_2,\ldots,x_n]$. Então $V(I) \neq \phi$.

DEMONSTRAÇÃO:

Como $I \neq K[x_1,x_2,\ldots,x_n]$ existe um ideal maximal M de $K[x_1,x_2,\ldots,x_n]$ tal que $I \subset M$. É bastante provar que $V(M) \neq \phi$ pois $V(M) \subset V(I)$.

Mas (3.3.1,iv) $M = (x_1-a_1,x_2-a_2,\ldots,x_n-a_n)$ onde $a_i \in K$, e é imediato que $V(M) = \{(a_1,a_2,\ldots,a_n)\}$.

A.6 TEOREMA (Forma Forte do HILBERT NULLSTELLENSATZ)

Seja I um ideal próprio de $K[x_1,x_2,\ldots,x_n]$. Então $J(V(I)) = r(I)$.

DEMONSTRAÇÃO:

Por (A.3, iv) e (A.4,i) temos:

$$r(I) \subset J(V(r(I))) = J(V(I))$$

Por outro lado observamos que $K[x_1,x_2,\ldots,x_n]$ é um anel de Noetheriano (1.5.6) e portanto I é finitamente gerado (1.5.3), digamos:

$$I = (g_1,g_2,\ldots,g_r)$$

onde $g_i \in K[x_1,x_2,\ldots,x_n]$.

Se $f \in J(V(I))$ então $f(P) = 0$ para todo ponto $P \in V(I) = V(g_1,g_2,\ldots,g_r)$. Por (3.3.1,v) existe $n \in \mathbb{N}$ tal que $f^n \in I = (g_1,g_2,\ldots,g_r)$ e dai $f \in r(I)$.

A.7 PROPOSIÇÃO

i) A aplicação $V : \mathcal{I} \to \mathcal{A}$ é uma correspondência biunívoca entre o conjunto $\mathcal{I}$ dos ideais radicais I e o conjunto $\mathcal{A}$ das variedades algébricas afins.

ii) $V = VJV$ e $J = JVJ$

DEMONSTRAÇÃO:

ii) Como $V(J(V(I))) = V(r(I)) = V(I)$ por (A.6) e (A.4,i), para todo ideal I, temos:

$$VJV = V$$

Tambem, para $V(I) \in \mathcal{A}$, temos:

$$J(V(I)) = J(VJV(I)) = JVJ(V(I))$$

e então

$$JVJ = J$$

i) Se $V(I) \in \mathcal{A}$ então $J(V(I))$ é (A.3,i) um ideal de $K[x_1,x_2,\ldots,x_n]$. Dai (A.6) temos que

$$r(J(V(I))) = JV(JV(I)) = JVJ(V(I)) = J(V(I)) \text{ por ii}$$

Daí, $J(V(I)) \in \mathcal{I}$ e $V(J(V(I))) = V(I)$ e a aplicação é sobre.

Se $V(I) = V(K)$ onde $I,K \in \mathcal{I}$, isto é, $I = r(I)$ e $K = r(K)$ então:

$$I = r(I) = J(V(I)) = J(V(K)) = r(K) = K$$

e a aplicação é injetora.

OBSERVAÇÃO: Os conjuntos $\mathcal{A}$ e $\mathcal{I}$ são latices completos, como veremos:

Sejam: $V(I) \wedge V(J) = V(I + J)$ e

$V(I) \vee V(J) = V(IJ)$

Com isso teremos:

$$\begin{tikzcd}[column sep=small] & V(IJ) \arrow[dl, dash] \arrow[dr, dash] & \\ V(I) \arrow[dr, dash] & & V(J) \arrow[dl, dash] \\ & V(I+J) & \end{tikzcd}$$

Para ideais radicais sejam:

$I \wedge J = I \cap J$ e

$I \vee J = r(I + J)$

Com isso teremos:

$$\begin{tikzcd}[column sep=small] & r(I+J) \arrow[dl, dash] \arrow[dr, dash] & \\ I \arrow[dr, dash] & & J \arrow[dl, dash] \\ & I \cap J & \end{tikzcd}$$

Assim sendo, $\mathcal{A}$ o conjunto das variedades algébricas afins é um latice, bem como o conjunto $\mathcal{I}$ dos ideais radicais.

Tais latices são completos pois se $A \subset \mathcal{A}$ e $B \subset \mathcal{I}$, então A e B tem infimos e supremos, os quais são:

i) O ínfimo de A é $V(\sum I\alpha)$ onde $V(I\alpha) \in A$, para todo α;

ii) O supremo de A é $V(\prod_{\alpha} I\alpha)$

iii) O ínfimo de B é $\bigcap_{\alpha} I\alpha$, onde $I\alpha \in B$ para todo α.

iv) O supremo de B é $r(\sum_{\alpha} I\alpha)$.

A.8 DEFINIÇÃO

Uma variedade algébrica afim é IRREDUTÍVEL se, e somente se, $V(I) = V(A) \cup V(B) \Rightarrow V(I) = V(A)$ ou $V(I) = V(B)$, onde $V(A), V(B) \in \mathcal{A}$.

A.9 PROPOSIÇÃO

Seja I um ideal radical de $K[x_1, x_2, \ldots, x_n]$. Então I é primo se, e somente se, V(I) é irredutível.

DEMONSTRAÇÃO:

Seja I um ideal primo e suponha que

$$V(I) = V(A) \cup V(B) = V(A \cap B) \quad (A.4)$$

Por (A.6) temos:

$I = r(I) = J(V(I)) = J(V(A \cap B)) = r(A \cap B) \supset A \cap B \supset AB$.

Então $A \subset I$ ou $B \subset I$ pois I é primo. Daí, (A.3) $V(I) \subset V(A)$ ou $V(I) \subset V(B)$. Como devemos ter $V(I) = V(A) \cup V(B)$ segue que $V(I) = V(A)$ ou $V(I) = V(B)$.

Reciprocamente, se I não é primo, seja $fg \in I$ com $f \notin I$ e $g \notin I$. Provaremos que

$$V(I) = [V(I) \cap V(f)] \cup [V(I) \cap V(g)]$$

onde $V(f) = V((f))$ e $V(g) = V((g))$.

A inclusão $\supset$ vale trivialmente.

Por outro lado, se $P \in V(I)$ então $(fg)(P) = 0$ e portanto $f(P).g(P) = 0$ acarretando $f(P) = 0$ ou $g(P) = 0$. Assim, temos que $P \in V(f)$ ou $P \in V(g)$ e portanto $P \in V(I) \cap V(f)$ ou $P \in V(I) \cap V(g)$ e finalmente

$$P \in [V(I) \cap V(f)] \cup [V(I) \cap V(g)]$$

Agora é fácil ver que $V(I + (f)) \neq V(I)$ e tambem $V(I + (g)) \neq V(I)$ pois se tivessemos $V(I + (f)) = V(I) \cap V(f) = V(I)$ então $V(I) \subset V(f)$ e assim $f \in JV(f) \subset J(V(I) = r(I) = I$ o que é um absurdo.

Assim concluímos que $V(I)$ não é irredutível.

A.10 COROLÁRIO

i) A aplicação $V : \mathcal{P} \to A_I$ é uma correspondência biunívoca entre o conjunto $\mathcal{P}$ dos ideais primos de I e o conjunto A_I das variedades algébricas afins irredutíveis;

ii) A aplicação $V : \mathcal{M} \to \mathcal{P}$ é uma correspondência biunívoca entre o conjunto $\mathcal{M}$ de ideais maximais de I e o conjunto $\mathcal{P}$ de pontos de K^n.

DEMONSTRAÇÃO:

i) A.9

ii) (3.3.1, iv)

B I B L I O G R A F I A

[1] ATIYAH, M.F. e MACDONALD, H.G. Introduction to Commutative Algebra. Addison Wesley (1.969) London

[2] BOURBAKI, N. Elements of Mathematics, Commutative Algebra. Hermann (1.972) Paris.

[3] GILMER, R. The Pseudo-radical of a Commutative ring Pac.J.Math 19 (1.966), 275-284

[4] GILMER, R. Multiplicative Ideal Theory. Marcel Dekker. (1.972) New York

[5] GOLDMAN, O. Hilbert Rings and the Nullstellensatz. Math. Z. 54 (1.951) 136-140

[6] HERSTEIN, I.N. Tópics in Algebra. Blaisdell (1.965) New York

[7] KAPLANSKY, I. Commutative Rings. Allyn Bacon, Boston Mass.(1.970)

[8] KRULL, W. Jacobsonche Ringe; Hilbertscher Nullstellensatz Dimensionstheorie. Math. Z. 54 (1.951) 354-387

[9] LANG, S. Algebra. Addison Wesley Reading Mass.(1.967)

[10] MONTEIRO, L.H.J. Elementos de Algebra. Livros Técnicos e Científicos Editora S/A. Rio de Janeiro (1.974)

[11] NAGATA, M. Local Rings. New York Interscience (1.962)