L.H.Jacy Monteiro.

SÔBRE AS POTÊNCIAS SIMBÓLICAS DE UM IDEAL PRIMO DE UM ANEL DE POLINÔMIOS.

Tese apresentada à Faculdade de Filosofia, Ciências e Letras da Universidade de S.Paulo para doutoramento em Ciências (Matemática).

São Paulo.
1950

I N T R O D U Ç Ã O.

Trata a presente tese do seguinte problema: seja $\mathfrak{p}$ um ideal primo de um anel de polinômios $R_n = k[X_1, \ldots, X_n]$ ($\mathfrak{p} \neq R_n$, $\mathfrak{p} \neq (0)$), determinar o conjunto S formado por zero e por todos os polinômios f, $f \neq 0$ e gr. $f > 0$, de R_n, tais que todo ponto de $V = \mathcal{V}(\mathfrak{p})$ (variedade algébrica do S_n determinada pelo ideal $\mathfrak{p}$) seja um ponto múltiplo de ordem pelo menos ρ (ρ inteiro, $\rho \geq 1$) da hiper-superfície algébrica $H = \mathcal{V}(R_n.f)$. O resultado a que chegámos é o seguinte: $S = \mathfrak{p}^{(\rho)}$. Para demonstrarmos êste teorema estabelecemos, inicialmente, uma condição necessária e suficiente para que um polinômio f de R_n pertença à potência simbólica ρ-ésima de $\mathfrak{p}$. E' a seguinte: A) - $f \in \mathfrak{p}^{(\rho)}$ quando, e sòmente quando, tôdas as derivadas parciais mistas de f e de ordens $0, 1, \ldots, \rho-1$ pertencem a $\mathfrak{p}$. Para a demonstração dêste teorema são fundamentais os critérios das matrizes jacobianas e das matrizes jacobianas mistas, que caracterizam os pontos simples de uma variedade algébrica. No capítulo V fizemos uma exposição de alguns dos resultados, devidos a O.Zariski, sôbre pontos simples de uma variedade algébrica ([19](1)). No capítulo IV, estudámos, além das derivações de primeira ordem e dos aneis locais (necessários ao desenvolvimento do capítulo V) as derivações parciais e as derivações parciais mistas. Aqui adotámos a definição de F.K.Schmidt de derivação de ordem superior e fizemos uma nova exposição sôbre as propriedades destas derivações. No capítulo VI, pela aplicação do teorema A), obtivemos uma nova demonstração de um resultado de O.Zariski sôbre as funções de $\mathfrak{F}(V)$ (corpo de funções racionais sôbre a variedade algébrica irredutível V) que se anulam com uma dada ordem, em quasi todos os pontos de uma sub-variedade W de V.

Os capítulos I, II e III contêm uma exposição dos resultados fundamentais sôbre aneis noetherianos e aneis de quocientes, variedades algébricas e teoria da dimensão, que são necessários ao desenvolvimento dos capítulos seguintes.

Quero expressar aqui os meus agradecimentos ao Prof. O. Zariski pela sugestão do problema acima e pela orientação prestada durante a preparação dêste trabalho.

(1) Os números entre colchetes se referem à bibliografia citada no fim dêste trabalho.

CAPITULO I.

Aneis noetherianos e aneis de quocientes.

1. Aneis noetherianos.

Diremos que um anel comutativo R satisfaz à condição da base se todo ideal $\mathfrak{a}$ de R tiver uma base finita. Portanto, para todo ideal $\mathfrak{a}$ de R existem elementos $\alpha_1,\ldots,\alpha_s$ pertencentes a R e tais que o ideal por êles gerado coincide com $\mathfrak{a}$, isto é, todo elemento α de $\mathfrak{a}$ pode ser escrito sob a forma $\alpha = \sum_{i=1}^{s} a_i\alpha_i + \sum_{i=1}^{s} m_i\alpha_i$, onde $a_i \in R$ $(i=1,\ldots,s)$ e $m_i \in Z$ $(i=1,\ldots,s)$, Z anel dos números inteiros. Se R tiver elemento unidade, todo elemento α de $\mathfrak{a}$ poderá ser escrito, simplesmente, sob a forma $\alpha = \sum_{i=1}^{s} a_i\alpha_i$ $(a_i \in R,\ i=1,\ldots,s)$.

Diremos que um anel comutativo R satisfaz à condição das cadeias crescentes se tôda cadeia crescente de ideais

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_i \subset \ldots \tag{1}$$

tiver sòmente um número finito de têrmos distintos. Isto significa que existe um índice N tal que $\mathfrak{a}_i = \mathfrak{a}_{i+1}$ para todo $i \geqslant N$, ou seja, a cadeia (1) permanece estacionária a partir de um certo índice em diante.

Teorema 1 - Um anel R que satisfaz à condição da base também satisfaz à condição das cadeias crescentes e reciprocamente.

A demonstração pode ser encontrada em [13] pp.25-26 ou [15] pp.76-78 .

Um anel R que verifica uma dessas condições (e portanto as duas) é denominado anel noetheriano.

Seja X uma indeterminada sôbre um anel R, indicaremos por R[X] o anel formado por todos os polinômios em X com coeficientes em R.

Teorema 2 (Hilbert) - Se R for um anel noetheriano, R[X] será também um anel noetheriano.

Para a demonstração ver [13] pp.23-24 ou [15] pp. 74-75 . Dêste teorema decorrem, fàcilmente as proposições:

1. Se R for um anel noetheriano também $R[X_1,\ldots,X_n]$ (anel de polinômios em n indeterminadas $X_1,\ldots,X_n$ com coeficientes em R) será um anel noetheriano.
2. Se k for um corpo então $k[X_1,\ldots,X_n]$ será um anel noetheriano.

2. Decomposição de um ideal.

Diremos que um ideal $\mathfrak{p}$, de um anel comutativo R, é um ideal primo se for verificada a condição: $ab \in \mathfrak{p}$, $a \notin \mathfrak{p} \longrightarrow b \in \mathfrak{p}$ $(a,b \in R)$ ou, o que é equivalente, se $R/\mathfrak{p}$ for um campo de integridade.

Diremos que um ideal $\mathfrak{q}$, de um anel comutativo R, é um ideal primário se for verificada a condição: $ab \in \mathfrak{q}$, $a \notin \mathfrak{q} \longrightarrow b^\rho \in \mathfrak{q}$, onde ρ é um inteiro positivo conveniente; ou, o que é equivalente, se todo divisor do zero de $R/\mathfrak{q}$ for um elemento nilpotente.

Seja $\mathfrak{q}$ um ideal primário e consideremos o conjunto $\mathfrak{p}$ de todos os elementos a de R tais que exista um inteiro positivo conveniente ρ tal que $a^\rho \in \mathfrak{q}$. Demonstra-se que [15] pp.66-67 :

3. $\mathfrak{p}$ é um ideal primo.

Diremos que o ideal primo $\mathfrak{p}$, assim definido (e que também é chamado radical de $\mathfrak{q}$ e é indicado por $\mathfrak{p} = \text{Rad. } \mathfrak{q}$) está associado ao ideal primário $\mathfrak{q}$, e que o ideal primário $\mathfrak{q}$ pertence ao ideal primo $\mathfrak{p}$.

A caracterização de um ideal primário $\mathfrak{q}$ e do seu ideal primo associado $\mathfrak{p}$ é dada pelo seguinte [13,p.33], ou, [15 ,p.68]:

Teorema 3 - Sejam $\mathfrak{p}$ e $\mathfrak{q}$ dois ideais que verificam as condições:

1. $\mathfrak{q} \subset \mathfrak{p}$;
2. $ab \in \mathfrak{q}$, $b \notin \mathfrak{q} \longrightarrow a \in \mathfrak{p}$;
3. Se $a \in \mathfrak{p}$ então existe um inteiro positivo conveniente ρ tal que $a^\rho \in \mathfrak{q}$.

Então $\mathfrak{q}$ é um ideal primário e $\mathfrak{p}$ é o ideal primo associado a $\mathfrak{q}$.

Se R for noetheriano serão válidas as seguintes relações entre um ideal primário $\mathfrak{q}$ e o seu radical $\mathfrak{p}$:

4. $\mathfrak{q} \subset \mathfrak{p}$ e $\mathfrak{p}^{\rho} \subset \mathfrak{q}$, onde ρ é um inteiro positivo conveniente.

No que se segue sempre indicaremos por R um anel noetheriano. Diremos que um ideal $\mathfrak{a}$ de R é um ideal redutível se pudermos representar $\mathfrak{a}$ sob a forma $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$, onde $\mathfrak{a}_1$ e $\mathfrak{a}_2$ são ideais de R tais que $\mathfrak{a} \neq \mathfrak{a}_1$ e $\mathfrak{a} \neq \mathfrak{a}_2$. Um ideal não redutível chama-se ideal irredutível. Sendo R um anel noetheriano valem as seguintes proposições ([13] pp.35-37, ou, [15], pp.165-166 :

5. Todo ideal de R é intersecção de um número finito de ideais irredutíveis.
6. Todo ideal irredutível é primário.

Portanto, temos o

Teorema 4 (primeiro teorema da decomposição) - Todo ideal de um anel noetheriano é igual à intersecção de um número finito de ideais primários.

Assim, todo ideal $\mathfrak{a}$ de R pode ser escrito sob a forma:

$$(2) \qquad \mathfrak{a} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r],$$

onde $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ são ideais primários. Vejamos como podemos simplificar esta decomposição. Evidentemente, podemos suprimir os ideais primários que contêm a intersecção dos restantes. Ainda mais, temos ([13], pp.37-39, [15], p.169):

7. Se $\mathfrak{q}_1', \ldots, \mathfrak{q}_h'$ forem ideais primários pertencentes a um mesmo ideal primo $\mathfrak{p}$, então $\mathfrak{q}_1' \cap \ldots \cap \mathfrak{q}_h'$ será um ideal primário pertencente ao mesmo ideal primo $\mathfrak{p}$.
8. Sejam $\mathfrak{q}_1'$ e $\mathfrak{q}_2'$ dois ideais primários não pertencentes a um mesmo ideal primo, então $\mathfrak{q}_1' \cap \mathfrak{q}_2'$ não é um ideal primário.

Portanto, na decomposição (2) podemos substituir os ideais primários que pertencem a um mesmo ideal primo por um outro ideal primário pertencente ao mesmo ideal primo. Obteremos assim uma decomposição de $\mathfrak{a}$ como intersecção de ideais primários e que goza das seguintes propriedades: 1.Nenhum ideal primário é supérfluo, isto é, não contém a intersecção dos restantes; 2. todos os ideais primos associados aos ideais primários são distintos. Uma decomposição que tenha estas propriedades é denominada <u>decomposição normal do ideal</u> $\mathfrak{a}$. Temos então o

<u>Teorema 5</u> (segundo teorema da decomposição) - <u>Todo ideal de um anel noetheriano admite uma decomposição normal</u>.

Seja (2) uma decomposição normal do ideal $\mathfrak{a}$. Diremos que $\mathfrak{q}_1,\ldots,\mathfrak{q}_r$ são as <u>componentes primárias</u> de $\mathfrak{a}$ e que $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ (onde $\mathfrak{p}_i$ é o ideal primo associado ao ideal primário $\mathfrak{q}_i$, $i=1,\ldots,r$) são os <u>ideais primos</u> de $\mathfrak{a}$. As componentes primárias não são determinadas de modo único, no entretanto, podemos falar da unicidade dos ideais primos. Precisamente, temos o

<u>Teorema 6</u> (primeiro teorema da unicidade) - <u>Sejam</u> $\mathfrak{a} = [\mathfrak{q}_1,\ldots,\mathfrak{q}_r]$ e $\mathfrak{a} = [\mathfrak{q}'_1,\ldots,\mathfrak{q}'_s]$ <u>duas decomposições normais de um mesmo ideal</u> $\mathfrak{a}$. <u>Então temos</u> $r=s$ <u>e, usando uma notação conveniente,</u> $\mathfrak{p}_i = \mathfrak{p}'_i$ $(i=1,\ldots,r)$, <u>onde</u> $\mathfrak{p}_i = \text{Rad.}\,\mathfrak{q}_i$, $\mathfrak{p}'_i = \text{Rad.}\,\mathfrak{p}'_i$ $(i=1,\ldots,r)$.

A demonstração dêste teorema pode ser encontrada em [13], pp.39-41, ou, [15], pp.170-171.

Daremos agora um outro teorema de unicidade. Seja $\mathfrak{a} = [\mathfrak{q}_1,\mathfrak{q}_2,\ldots,\mathfrak{q}_r]$ uma decomposição normal de um ideal $\mathfrak{a}$ de R. Indiquemos por $\Sigma = \{\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{p}_r\}$ o conjunto dos ideais primos de $\mathfrak{a}$. Consideremos um sub-conjunto Σ' de Σ: $\Sigma' = \{\mathfrak{p}_{i_1},\mathfrak{p}_{i_2},\ldots,\mathfrak{p}_{i_h}\}$, onde $h \leq r$. Diremos que Σ' é um <u>sub-sistema isolado</u> quando for verificada a condição: se $\mathfrak{p}_\alpha \in \Sigma'$ e se $\mathfrak{p}_\alpha \supset \mathfrak{p}_\beta$, com $\mathfrak{p}_\beta \in \Sigma$, então $\mathfrak{p}_\beta \in \Sigma'$. Indiquemos por

$\mathfrak{A}_{\Sigma'}$ a intersecção dos ideais primários de $\mathfrak{A}$ pertencentes aos ideais primos de Σ' : $\mathfrak{A}_{\Sigma'} = [\mathfrak{q}_{i_1}, \mathfrak{q}_{i_2}, \ldots, \mathfrak{q}_{i_h}]$. Se Σ' for um sub-sistema isolado diremos que $\mathfrak{A}_{\Sigma'}$ é uma componente isolada de $\mathfrak{A}$. Pois bem, vale o seguinte ([13], pp.42-43, [15], pp.175-176):

Teorema 7 (segundo teorema da unicidade) - Tôda componente isolada de um ideal $\mathfrak{A}$ é determinada de modo único pelos correspondentes ideais primos.

Êste teorema nos diz que se considerarmos uma outra decomposição normal do ideal $\mathfrak{A}$: $\mathfrak{A} = [\mathfrak{q}'_1, \mathfrak{q}'_2, \ldots, \mathfrak{q}'_r]$ e se considerarmos a componente isolada correspondente ao mesmo sistema Σ' nesta nova decomposição, então as duas componentes isoladas coincidem (sem que, no entretanto, haja coincidência das componentes primárias destas componentes isoladas).

Se o sistema isolado Σ' tiver um único elemento $\mathfrak{p}_i$, diremos que $\mathfrak{p}_i$ é um ideal primo isolado de $\mathfrak{A}$; o correspondente ideal primário $\mathfrak{q}_i$ é, pela definição acima, uma componente isolada de $\mathfrak{A}$. Um ideal primo não isolado é denominado ideal primo de imersão de $\mathfrak{A}$.

3. Radical de um ideal.

Seja R um anel comutativo e $\mathfrak{A}$ um ideal de R. Chamaremos radical de $\mathfrak{A}$ ao conjunto de todos os elementos a de R tais que alguma potência (com expoente inteiro e positivo) de a esteja em $\mathfrak{A}$. Indicaremos o radical de um ideal pela notação Rad. $\mathfrak{A}$. E' imediato que Rad. $\mathfrak{A}$ é um ideal de R e também, se $\mathfrak{A}$ for primário, Rad. $\mathfrak{A}$ será o ideal primo associado a $\mathfrak{A}$. Suporemos, neste parágrafo, que o anel R seja noetheriano; algumas das propriedades que daremos a seguir são válidas mesmo sem esta hipótese. Temos as seguintes proposições ([15], pp.163-176, p.183):

9. $\mathfrak{A} \subset$ Rad. $\mathfrak{A}$;
10. Rad.(Rad. $\mathfrak{A}$) = Rad. $\mathfrak{A}$;
11. Seja $\mathfrak{A} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ uma decomposição normal de um ideal $\mathfrak{A}$, então Rad. $\mathfrak{A}$ = $= [\mathfrak{p}_1, \ldots, \mathfrak{p}_r]$, onde $\mathfrak{p}_i$ = Rad. $\mathfrak{q}_i$ (i=1,...,s).

Observando que Rad. $\mathfrak{p} = \mathfrak{p}$ se $\mathfrak{p}$ for um ideal primo virá, pela prop.11:

12. $\mathfrak{a} = \text{Rad.}\,\mathfrak{a}$ quando, e sòmente quando, $\mathfrak{a}$ for intersecção de um número finito de ideais primos.

Temos também:

13. $\text{Rad.}(\mathfrak{a}\mathfrak{b}) = \text{Rad.}(\mathfrak{a} \cap \mathfrak{b}) = \text{Rad.}\,\mathfrak{a} \cap \text{Rad.}\,\mathfrak{b}$.

Apliquemos esta última proposição ao caso do produto $\mathfrak{q}_1\mathfrak{q}_2$ de dois ideais primários $\mathfrak{q}_1$ e $\mathfrak{q}_2$, pertencentes a um mesmo ideal primo $\mathfrak{p}$. Teremos

$$\text{Rad.}(\mathfrak{q}_1\mathfrak{q}_2) = \text{Rad.}\,\mathfrak{q}_1 \cap \text{Rad.}\,\mathfrak{q}_2 = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p},$$

portanto, pela 11., o ideal primo $\mathfrak{p}$ é o único ideal primo isolado de $\mathfrak{q}_1\mathfrak{q}_2$. Considerando ainda o caso de uma potência $\mathfrak{p}^f$ de um ideal primo $\mathfrak{p}$, teremos (a 13. pode ser, fàcilmente, generalizada para um número maior de fatores): Rad. $\mathfrak{p}^f = \mathfrak{p}$. Portanto, na decomposição normal de $\mathfrak{p}^f$ há um ideal primário pertencente ao ideal primo $\mathfrak{p}$; ainda mais, $\mathfrak{p}$ é o único ideal primo isolado de $\mathfrak{p}^f$. Indicaremos a componente isolada de $\mathfrak{p}^f$, que pertence a $\mathfrak{p}$, por $\mathfrak{p}^{(\rho)}$ e a denominaremos <u>potência simbólica</u> ρ-<u>ésima</u> do ideal primo $\mathfrak{p}$. Observemos que pelo segundo teorema de unicidade (teorema 7) esta componente isolada $\mathfrak{p}^{(\rho)}$ permanece a mesma qualquer que seja a decomposição normal do ideal $\mathfrak{p}^f$. Um dos nossos resultados é a caracterização dos elementos de $\mathfrak{p}^{(\rho)}$, quando R é o anel de polinômios $k[X_1,\ldots,X_n]$ (capítulo VI).

4. <u>Aneis de quocientes</u>.

Sejam R e R' dois aneis comutativos com $R \subset R'$. Introduziremos duas operações entre os ideais de R e os de R'. Seja $\mathfrak{a}$ um ideal de R e consideremos o ideal $R'\mathfrak{a}$ gerado, em R', pelos elementos de $\mathfrak{a}$. Portanto, todo elemento de $R'\mathfrak{a}$ é da forma $a + \sum_i r'_i a_i$, onde $a \in \mathfrak{a}$, $a_i \in \mathfrak{a}$, $r'_i \in R'$ e a somatória só contém um número finito de têrmos. Se R' tiver elemento unidade, todo elemento de $R'\mathfrak{a}$ poderá ser escrito, simplesmente, sob a forma $\sum_i r'_i a_i$, onde $r'_i \in R'$ e $a_i \in \mathfrak{a}$ e a somatória só

contém um número finito de têrmos. O ideal $\mathfrak{a}' = R'\mathfrak{a}$ é denominado ideal extensão de $\mathfrak{a}$ ao anel R'. Seja agora $\mathfrak{a}'$ um ideal de R' e consideremos a intersecção $\mathfrak{a} = \mathfrak{a}' \cap R$; é imediato que $\mathfrak{a}$ é um ideal de R. O ideal $\mathfrak{a} = \mathfrak{a}' \cap R$ é denominado projeção do ideal $\mathfrak{a}'$ no anel R. Daremos aqui um resumo das principais propriedades das operações extensão e projeção; as suas demonstrações podem ser encontradas em [15], pp.200-205:

14. Se $\mathfrak{a} \subset \mathfrak{b}$ então $R'\mathfrak{a} \subset R'\mathfrak{b}$;
15. $R'(\mathfrak{a} + \mathfrak{b}) = R'\mathfrak{a} + R'\mathfrak{b}$;
16. $R'(\mathfrak{a}\,\mathfrak{b}) = R'\mathfrak{a}\,.R'\mathfrak{b}$;
17. $R'(\mathfrak{a} \cap \mathfrak{b}) \subset R'\mathfrak{a} \cap R'\mathfrak{b}$;
18. $R'(\mathfrak{a} : \mathfrak{b}) \subset R'\mathfrak{a} : R'\mathfrak{b}$;
19. $(\mathfrak{a}' + \mathfrak{b}') \cap R \supset \mathfrak{a}' \cap R + \mathfrak{b}' \cap R$;
20. $(\mathfrak{a}'\mathfrak{b}') \cap R \supset (\mathfrak{a}' \cap R)(\mathfrak{b}' \cap R)$;
21. $(\mathfrak{a}' \cap \mathfrak{b}') \cap R = (\mathfrak{a}' \cap R) \cap (\mathfrak{b}' \cap R)$;
22. $(\mathfrak{a}' : \mathfrak{b}') \cap R \subset (\mathfrak{a}' \cap R) : (\mathfrak{b}' \cap R)$.

Nestas relações $\mathfrak{a}$ e $\mathfrak{b}$ são dois ideais de R, $\mathfrak{a}'$ e $\mathfrak{b}'$ dois ideais de R'. Também temos:

23. A projeção de um ideal primário $\mathfrak{q}'$ pertencente ao ideal primo $\mathfrak{p}'$ é um ideal primário pertencente à projeção $\mathfrak{p}' \cap R$ de $\mathfrak{p}'$.

Em particular:

24. A projeção de um ideal primo de R' é um ideal primo de R.

Seja $\mathfrak{a}$ um ideal de R; consideremos o ideal extensão $R'\mathfrak{a}$ e apliquemos a êste último a operação de projeção. Obteremos um ideal $R'\mathfrak{a} \cap R = \mathfrak{a}^*$ de R que é denominado ideal reduzido de $\mathfrak{a}$. Do mesmo modo, seja $\mathfrak{a}'$ um ideal de R'; pela operação de projeção obteremos um ideal $\mathfrak{a}' \cap R$ de R e se a êste último aplicarmos a operação de extensão obteremos um ideal $R'(\mathfrak{a}' \cap R) = \mathfrak{a}'^*$ de R', que é denominado ideal reduzido de $\mathfrak{a}'$. São imediatas as propriedades:

25. $\mathfrak{a} \subset \mathfrak{a}^*$ e $\mathfrak{a}'^* \subset \mathfrak{a}'$.

Seja R um anel comutativo tal que nem todos os seus elementos sejam divisores do zero. Consideremos as frações

a/b, onde $a \in R$, $b \in R$ e b não é um divisor do zero. Definiremos: $a/b = c/d \longleftrightarrow ad = bc$; $a/b + c/d = (ad+bc)/bd$ e $a/b.c/d = ac/bd$. E' fácil ver que o conjunto Σ' de tôdas estas frações é um anel com elemento unidade ($= b/b$, onde $b \in R$ e b não é um divisor do zero). Σ' é denominado anel total de quocientes. A aplicação $a \in R \longrightarrow ab/b \in \Sigma'$ é um isomorfismo de R em Σ', portanto, podemos considerar R como um sub-anel de Σ'. Consideremos agora um sub-conjunto S de R que verifica as propriedades: 1. $S \neq \emptyset$; 2. $a \in S$, $b \in S \longrightarrow ab \in S$ e 3. Nenhum elemento de S é um divisor do zero. Um sub-conjunto S que verifica as três condições acima é denominado sistema multiplicativo. Repetindo a mesma construção anterior para as frações a/b, com $a \in R$ e $b \in S$, obteremos um sub-anel $R' = R_S$ do anel Σ'. O anel $R'=R_S$ é denominado anel de quocientes de R em relação ao sistema multiplicativo S. E' imediato que podemos considerar R como um sub-anel de R'.

Um caso muito importante é aquele em que $S = R - \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal primo de R, $\mathfrak{p} \neq R$, e, além disso, $\mathfrak{p}$ contém todos os divisores do zero de R.

Aos aneis R e $R'=R_S$ podemos aplicar as propriedades 14,15,....,25; aqui ainda valem outras propriedades provenientes do fato que R' é um anel de quocientes de R. Como estas propriedades serão importantes para o desenvolvimento dos capítulos III e V, daremos aqui as suas demonstrações (Crf. 15 ,pp.213-223). No que se segue suporemos que R tenha elemento unidade.

Teorema 8 - Todo ideal de R' é extensão de um ideal de R.

Com efeito, seja $\mathfrak{A}'$ um ideal de R' e consideremos a sua projeção sôbre R: $\mathfrak{A} = \mathfrak{A}' \cap R$. Temos $R'\mathfrak{A} \subset \mathfrak{A}'$. Seja a/b ($a \in R$, $b \in S$) um elemento qualquer de $\mathfrak{A}'$, como $b \in R'$ teremos $a = (a/b).b \in \mathfrak{A}' \cap R = \mathfrak{A}$. Por outro lado, temos $a/b = a.(1/b)$, logo, $a/b \in R'\mathfrak{A}$. Estabelecemos assim a inclusão $\mathfrak{A}' \subset R'\mathfrak{A}$ que com a anterior nos dá $\mathfrak{A}' = R'\mathfrak{A}$. (q.e.d.).

Demonstrámos ao mesmo tempo que todo ideal de R' é igual ao seu ideal reduzido.

Seja $\mathfrak{A}$ um ideal qualquer de R; então todo elemen

to a' de $R'\mathfrak{a}$ é da forma $a' = \sum_i' b_i' a_i$, onde $b_i' \in R'$ e $a_i \in \mathfrak{a}$. Mas $b_i' = b_i/c$ ($b_i \in R$ e $c \in S$), portanto, $a' = (\sum_i' b_i a_i)/c$, onde $\sum_i' b_i a_i \in \mathfrak{a}$ e $c \in S$. Provámos assim que todo elemento de $R'\mathfrak{a}$ é da forma a/c, onde $a \in \mathfrak{a}$ e $c \in S$. D'aqui podemos demonstrar o

Teorema 9 - Um elemento a^* de R pertence ao ideal reduzido $\mathfrak{a}^*$ de $\mathfrak{a}$ quando, e sòmente quando, existe um elemento conveniente c de S tal que $a^*c \in \mathfrak{a}$.

Com efeito, seja a^* um elemento de $\mathfrak{a}^* = R'\mathfrak{a} \cap R$; teremos $a^* \in R'\mathfrak{a}$, logo, $a^* = a/c$, onde $a \in \mathfrak{a}$ e $c \in S$. D'aqui vem $a^*c = a \in \mathfrak{a}$. Recìprocamente, seja a^* um elemento de R que multiplicado por um elemento c de S nos dá um elemento de $\mathfrak{a}$: $a^*c = a$. Desta relação vem $a^* = a/c \in R'\mathfrak{a}$, mas $a^* \in R$, logo, $a^* \in R'\mathfrak{a} \cap R = \mathfrak{a}^*$. (q.e.d.).

Teorema 10 - Se R for um anel noetheriano, então R' é também um anel noetheriano.

E' imediato, pois todo ideal $\mathfrak{a}$ de R tem uma base finita: $\mathfrak{a} = R.(a_1,\ldots,a_s)$ e para o ideal extensão $\mathfrak{a}' = R'\mathfrak{a}$ temos $\mathfrak{a}' = R'.(a_1,\ldots,a_s)$; a tese do teorema segue-se agora do teorema 8.

Consideremos agora uma decomposição normal de um ideal $\mathfrak{a}$ de R (anel noetheriano com elemento unidade): $\mathfrak{a} = [\mathfrak{q}_1,\ldots,\mathfrak{q}_s]$. Ponhamos $\mathfrak{p}_i = \text{Rad. } \mathfrak{q}_i$ $(i=1,\ldots,s)$. Indiquemos por A o conjunto dos índices $\{1,2,\ldots,s\}$. Seja B o sub-conjunto de A formado pelos índices β, $\beta \in A$, tais que $\mathfrak{p}_\beta \cap S = \emptyset$ e seja C o complemento de B em A. Demonstraremos o

Teorema 11 - O ideal reduzido de $\mathfrak{a}^*$ é dado pela intersecção das componentes primárias de $\mathfrak{a}$ cujos ideais primos não têm nenhum elemento comum com S, isto é,

$$\mathfrak{a}^* = \bigcap_{\beta \in B} \mathfrak{q}_\beta .$$

Demonstração - Se $B = \emptyset$ teremos $\mathfrak{p}_i \cap S \neq \emptyset$ para $i=1,2,\ldots,s$; desta última relação tiramos $\mathfrak{q}_i \cap S \neq \emptyset$ e, portanto, $\mathfrak{A} \cap S \neq \emptyset$. Então existe um elemento c de S pertencente a $\mathfrak{A}$, logo, $c/c = c.(1/c) = 1$ pertence a $R'\mathfrak{A}$, isto é, $R'\mathfrak{A} = R'$, de onde vem, $\mathfrak{A} = R$. Isto demonstra o teorema no caso em que $B = \emptyset$. Suponhamos que $B \neq \emptyset$. Seja a^* um elemento de $\mathfrak{A}^*$; pelo teorema 9 existe um elemento c de S tal que $a^*c \in \mathfrak{A}$, logo, $a^*c \in \mathfrak{q}_\beta$ $(\beta \in B)$. Mas $c \notin \mathfrak{p}_\beta$ $(\beta \in B)$, portanto, $\mathfrak{q}_\beta:(c) = \mathfrak{q}_\beta$; então de $a^*c \in \mathfrak{q}_\beta$ vem $a^* \in \mathfrak{q}_\beta:(c) = \mathfrak{q}_\beta$, de onde, $a^* \in \bigcap_{\beta \in B} \mathfrak{q}_\beta$. Isto nos mostra que $\mathfrak{A}^* \subset \bigcap_{\beta \in B} \mathfrak{q}_\beta$. Se $B = A$ teremos $\mathfrak{A}^* \subset \mathfrak{A}$, então, pela proposição 25 virá $\mathfrak{A} = \mathfrak{A}^*$, o que demonstra o teorema acima. Suponhamos que $B \neq A$. De $\mathfrak{p}_\gamma \cap S \neq \emptyset$ $(\gamma \in C)$ vem $\mathfrak{q}_\gamma \cap S \neq \emptyset$, portanto, $(\bigcap_{\gamma \in C} \mathfrak{q}_\gamma) \cap S \neq \emptyset$. Seja c um elemento pertencente a esta intersecção e seja x um elemento qualquer de $\bigcap_{\beta \in B} \mathfrak{q}_\beta$. O produto **xc** pertence a $\mathfrak{A}$, logo, pelo teorema 9, $x \in \mathfrak{A}^*$. Isto completa a demonstração do teorema 11.

Teorema 12 - Seja $\mathfrak{q}$ um ideal primário de R e suponhamos que $\mathfrak{p} \cap S = \emptyset$ $(\mathfrak{p} = \text{Rad.}\,\mathfrak{q})$. Então o ideal $\mathfrak{q}' = R'\mathfrak{q}$ é primário e temos $\text{Rad.}\,\mathfrak{q}' = \mathfrak{p}' = R'\mathfrak{p}$; ainda mais, $\mathfrak{q}' \cap R = \mathfrak{q}$.

Demonstração - Basta verificar as três condições do teorema 3 para os ideais $\mathfrak{q}'$ e $\mathfrak{p}'$, para concluirmos que $\mathfrak{q}'$ é primário e que $\mathfrak{p}' = R'\mathfrak{p}$ é o ideal primo que lhe pertence. E' imediato que $\mathfrak{q}' \subset \mathfrak{p}'$. Se $a/c \in \mathfrak{p}'$, teremos $a \in \mathfrak{p}$, logo, $a^\rho \in \mathfrak{q}$ (ρ inteiro positivo conveniente) e então $a^\rho/c^\rho \in \mathfrak{q}'$; isto verifica a condição 3. Se $(a_1/c_1)(a_2/c_2) \in \mathfrak{q}'$ e $(a_2/c_2) \notin \mathfrak{q}'$ teremos $a_1a_2 \in \mathfrak{q}$ e $a_2 \notin \mathfrak{q}$, logo, $a_1 \in \mathfrak{p}$ e então $a_1/c_1 \in \mathfrak{p}'$, o que verifica a condição 2. A relação $\mathfrak{q}' \cap R = \mathfrak{q}$ resulta, imediatamente, do teorema 11. Isto completa a demonstração do teorema 12.

Em particular, supondo-se $\mathfrak{q}$ um ideal primo teremos o

Corolário - Seja $\mathfrak{p}$ um ideal primo de R tal que $\mathfrak{p} \cap S = \emptyset$, então $\mathfrak{p}' = R'\mathfrak{p}$ é um ideal primo de R' e temos $\mathfrak{p}' \cap R = \mathfrak{p}$.

O teorema 12 nos mostra que a aplicação $\mathfrak{q} \subset R \longrightarrow \mathfrak{q}' = R'\mathfrak{q}$ é uma aplicação biunívoca dos ideais primários $\mathfrak{q}$ de R tais que $\mathfrak{p} \cap S = \emptyset$ ($\mathfrak{p} = \text{Rad.}\,\mathfrak{q}$) sôbre os ideais primários de R' (distintos de R').

Teorema 13 - Usando as mesmas notações que as empregadas no teorema 11, temos

$$R'\mathfrak{a} = \bigcap_{\beta \in B} \mathfrak{q}'_\beta, \text{ onde } \mathfrak{q}'_\beta = R'\mathfrak{q}_\beta$$

($\beta \in B$); ainda mais, esta é uma decomposição normal do ideal $R'\mathfrak{a}$.

Demonstração - Se $B = \emptyset$ já vimos que $R'\mathfrak{a} = R'$, o que demonstra o teorema. Suponhamos que $B \neq \emptyset$. Temos $R'\mathfrak{a} = R'\mathfrak{a}^* \subset \bigcap_{\beta \in B} R'\mathfrak{q}_\beta = \bigcap_{\beta \in B} \mathfrak{q}'_\beta$. Seja a/c um elemento de $\bigcap_{\beta \in B} \mathfrak{q}'_\beta$, teremos $a/c \in \mathfrak{q}'_\beta$ ($\beta \in B$) logo, pelo teorema 9, $a \in \mathfrak{q}_\beta$ ($\beta \in B$), portanto, $a \in \mathfrak{a}^*$ e então $a/c \; R'\mathfrak{a}^*$. Isto nos mostra que $\bigcap_{\beta \in B} \mathfrak{q}'_\beta \subset R'\mathfrak{a}$, logo, $R'\mathfrak{a} = \bigcap_{\beta \in B} \mathfrak{q}'_\beta$. A segunda parte do teorema é imediata..

Vamos agora considerar um caso mais particular, aquele em que $S = R - \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal primo de R ($\mathfrak{p} \neq R$) e R é um anel noetheriano com elemento unidade. Aqui precisamos supôr que $\mathfrak{p}$ contenha todos os divisores do zero de R. Neste caso, indicaremos por $R' = R_{\mathfrak{p}}$ o anel $R' = R_S$. Pelo que vimos anteriormente temos as proposições:

26. Se $\mathfrak{p}_1$ for um ideal primo tal que $\mathfrak{p}_1 \not\subset \mathfrak{p}$, então $R'\mathfrak{p}_1 = R'$.

27. Se $\mathfrak{p}_1$ for um ideal primo contido em $\mathfrak{p}$, o ideal $R'\mathfrak{p}_1 = \mathfrak{p}'_1$ será primo e $\mathfrak{p}'_1 \cap R = \mathfrak{p}_1$.

Por causa destas duas propriedades diremos que os únicos ideais primos que são conservados, quando passamos do anel R ao anel de quocientes $R' = R_{\mathfrak{p}}$, são os ideais contidos em $\mathfrak{p}$; todos os outros ideais são perdidos (isto é, têm por extensão o anel R').

De 26. e 27. e do teorema 8 resulta que

28. O ideal $\mathfrak{p}' = R'\mathfrak{p}$ é o único ideal máximal do anel $R' = R_{\mathfrak{p}}$.

Também temos:

29. A aplicação $\mathfrak{p}_1 \subset R \longrightarrow R'\mathfrak{p}_1 = \mathfrak{p}_1'$, é uma aplicação biunívoca dos ideais primos de R, contidos em $\mathfrak{p}$, sôbre os ideais primos de R' (distintos de R').

30. Seja $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ uma decomposição normal de um ideal $\mathfrak{a}$ de R; indiquemos por B o sub-conjunto de $\{1,2,\ldots,s\}$ tal que: se $\beta \in B$ então $\mathfrak{p}_\beta \subset \mathfrak{p}$. Então temos

a) $R'\mathfrak{a} = \bigcap_{\beta \in B} \mathfrak{q}'_\beta$, onde $\mathfrak{q}'_\beta = R'\mathfrak{q}_\beta$ $(\beta \in B)$; além disso os ideais primos de $R'\mathfrak{a}$ são $\mathfrak{p}'_\beta = R'\mathfrak{p}_\beta$ $(\beta \in B)$;

b) $\mathfrak{a}^* = \bigcap_{\beta \in B} \mathfrak{q}_\beta$.

Consideremos uma decomposição normal de $\mathfrak{p}^n$ (ver §3): $\mathfrak{p}^n = [\mathfrak{p}^{(n)}, \mathfrak{q}_1, \ldots, \mathfrak{q}_s]$, onde $\mathfrak{p} \subset \mathfrak{p}_i = \text{Rad.}\,\mathfrak{q}_i$ $(i=1,\ldots,s)$ e $\mathfrak{p}^{(n)}$ é a potência simbólica n-ésima de $\mathfrak{p}$. Pela proposição 30 virá:

31. $R'\mathfrak{p}^n = \mathfrak{p}'^n = R'\mathfrak{p}^{(n)}$ e $\mathfrak{p}'^n \cap R = \mathfrak{p}^{(n)}$, onde $\mathfrak{p}' = R'\mathfrak{p}$ e $R' = R_{\mathfrak{p}}$.

32. Seja $\mathfrak{p}_1$ um ideal primo de R contido em $\mathfrak{p}$. Então temos $R'\mathfrak{p}_1^{(n)} = \mathfrak{p}_1'^{(n)}$ e $\mathfrak{p}_1'^{(n)} \cap R = \mathfrak{p}^{(n)}$.

Esta última proposição é uma consequência imediata da proposição 30.

5. Intersecção das potências de um ideal.

Seja R um anel noetheriano com elemento unidade e consideremos um ideal $\mathfrak{a}$ de R, $\mathfrak{a} \neq R$. Demonstraremos o seguinte (Cfr. [1], p. 692):

Teorema 15 - Uma condição necessária e suficiente para que $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = (0)$, é que nenhum divisor do zero de R seja côngruo a 1, módulo $\mathfrak{a}$.

Demonstração - Suponhamos que $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = (0)$; devemos demonstrar que nenhum divisor do zero de R é côngruo a 1, módulo $\mathfrak{a}$. Ora, se existisse um divisor do zero a tal que $a \equiv 1 \pmod{\mathfrak{a}}$ teríamos $\mathfrak{a} \neq (0)$ e também $a \notin \mathfrak{a}$. Mas sendo a um divisor do zero existe $c \neq 0$, $c \in R$, tal que $ac = 0$; por outro lado, $a = 1+b$, com $b \in \mathfrak{a}$, logo, $c = -cb$, então, $c = c(-b)^n$, qualquer que seja n. Isto nos mostra que existe um elemento c, $c \neq 0$, comum a tôdas as potências de $\mathfrak{a}$, logo, $\bigcap_{n=1}^{\infty} \mathfrak{a}^n \neq (0)$. Fica assim demonstrado que a condição é necessária.

Passamos agora a demonstrar que a condição é também suficiente. Façamos $\delta = \bigcap_{n=1}^{\infty} \mathfrak{a}^n$ e seja $\delta\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$ uma decomposição normal do ideal $\delta\mathfrak{a}$. Provaremos, em primeiro lugar, que $\delta\mathfrak{a} = \delta$. Indiquemos por $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ os ideais primos de $\delta\mathfrak{a}$: $\mathfrak{p}_i = \text{Rad. } \mathfrak{q}_i$ $(i=1,\ldots,s)$. Para um dado i só podemos ter dois casos: ou $\mathfrak{a} \subset \mathfrak{p}_i$, ou, $\mathfrak{a} \not\subset \mathfrak{p}_i$. Se $\mathfrak{a} \subset \mathfrak{p}_i$ teremos $\mathfrak{a}^{\rho_i} \subset \mathfrak{q}_i$ (onde ρ_i é um inteiro tal que $\mathfrak{p}_i^{\rho_i} \subset \mathfrak{q}_i$); mas $\delta \subset \mathfrak{a}^{\rho_i}$, logo, $\delta \subset \mathfrak{q}_i$. Se $\mathfrak{a} \not\subset \mathfrak{p}_i$ teremos $\mathfrak{q}_i : \mathfrak{a} = \mathfrak{q}_i$. Por outro lado, $\delta \subset \delta\mathfrak{a} : \mathfrak{a} \subset \mathfrak{q}_i : \mathfrak{a}$, logo, $\delta \subset \mathfrak{q}_i$. Portanto, em ambos os casos temos $\delta \subset \mathfrak{q}_i$, logo, $\delta \subset \delta\mathfrak{a}$; mas é evidente que $\delta\mathfrak{a} \subset \delta$, então, $\delta = \delta\mathfrak{a}$. Provaremos agora que $\delta = (0)$. Seja $\{c_1, \ldots, c_r\}$ uma base de δ. Da igualdade $\delta = \delta\mathfrak{a}$ resulta que $c_i = \sum_{j=1}^{r} a_{ij} c_j$, onde $a_{ij} \in \mathfrak{a}$ e $i=1,\ldots,r$. Portanto, temos $\sum_{j=1}^{r} (\delta_{ij} - a_{ij}) c_j = 0$, onde δ_{ij} é o símbolo de Kronecker. Destas equações vem $\Delta\, c_j = 0$ $(j=1,\ldots,r)$, onde $\Delta = |\delta_{ij} - a_{ij}|$. Mas $\Delta \equiv 1 \pmod{\mathfrak{a}}$, portanto, Δ não é um divisor do zero; logo, de $\Delta\, c_j = 0$ vem $c_j = 0$ para $j=1,\ldots,r$. Isto nos mostra que $\delta = (0)$. (q.e.d.).

Teorema 17 - Seja R um anel noetheriano com elemento unidade e com um único ideal máximal $\mathfrak{m}$. Então temos

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0).$$

Demonstração - Seja a um elemento de R não pertencente a $\mathfrak{m}$. Consideremos o ideal principal R.a; como $\mathfrak{m}$ é o

único ideal máximal e $a \notin \mathfrak{M}$, teremos $R.a = R$. Isto nos mostra que todo elemento a de R, $a \notin \mathfrak{M}$ é um elemento unitário em R, portanto, nenhum divisor do zero de R pode ser côngruo a 1 módulo $\mathfrak{M}$. O teorema 17 é então uma consequência do teorema 16.

Teorema 18 - Seja R um anel noetheriano, com elemento unidade e com um único ideal máximal $\mathfrak{M}$. Temos

$$\bigcap_{n=1}^{\infty} (\mathfrak{A} + \mathfrak{M}^n) = \mathfrak{A},$$

onde $\mathfrak{A}$ é um ideal qualquer de R.

Demonstração - Se $\mathfrak{A} = R$, o teorema é imediato. Suponhamos que $\mathfrak{A} \neq R$, então $\mathfrak{A} \subset \mathfrak{M}$. Consideremos o anel resíduo $\bar{R} = R/\mathfrak{A}$, e seja τ o homomorfismo canônico de R sôbre $\bar{R}$. E' imediato que $\bar{R}$ é um anel noetheriano, com elemento unidade e com um único ideal máximal $\bar{\mathfrak{M}} = \tau\mathfrak{M}$. Portanto, pelo teorema 17, temos $\bigcap_{n=1}^{\infty} \bar{\mathfrak{M}}^n = (0)$. Aplicando a ambos os membros desta última relação, a imágem recíproca de τ, virá $\bigcap_{n=1}^{\infty} (\mathfrak{A} + \mathfrak{M}^n) = \mathfrak{A}$. (q.e.d.).

Faremos ainda uma outra aplicação do teorema 15. Seja R um campo de integridade noetheriano com elemento unidade e seja $\mathfrak{p} \neq R$ um ideal primo de R. E' imediato que nenhum divisor do zero de R é côngruo a 1, módulo $\mathfrak{p}$, portanto $\bigcap_{n=1}^{\infty} \mathfrak{p}^n = (0)$.

Teorema 19 - $\bigcap_{n=1}^{\infty} \mathfrak{p}^{(n)} = (0)$, onde $\mathfrak{p}$ é um ideal primo de um campo de integridade noetheriano R (com elemento unidade) e $\mathfrak{p} \neq R$.

Com efeito, consideremos o anel de quocientes $R' = R_{\mathfrak{p}}$; é imediato que R' é um campo de integridade noetheriano. Portanto $\bigcap_{n=1}^{\infty} \mathfrak{p}'^n = (0)$, onde $\mathfrak{p}' = R'\mathfrak{p}$. Por outro lado, pela proposição 31, temos $\mathfrak{p}^{(n)} = \mathfrak{p}'^n \cap R$, logo, $\mathfrak{p}^{(n)} \subset \mathfrak{p}'^n$ e então $\bigcap_{n=1}^{\infty} \mathfrak{p}^{(n)} = (0)$. (q.e.d.).

C A P I T U L O II.

Teorema dos zeros de Hilbert.

1. Variedades algébricas.

Seja k um corpo e consideremos uma extensão algébrica algèbricamente fechada $\bar{k}$ de k. Chamaremos ponto do espaço afim de n dimensões sôbre $\bar{k}$ a uma n-upla ordenada $(\alpha_1,\ldots,\alpha_n)$ de elementos de $\bar{k}$. O conjunto de todos os pontos é denominado espaço afim de n dimensões sôbre $\bar{k}$ e é indicado por $A_n^{\bar{k}}$. Diremos que dois pontos $P(\alpha_1,\ldots,\alpha_n)=P(\alpha)$ e $Q(\beta_1,\ldots,\beta_n)=Q(\beta)$ de $A_n^{\bar{k}}$ são pontos conjugados sôbre k quando, e sòmente quando, existe um k-isomorfismo σ de $k(\alpha_1,\ldots,\alpha_n)$ (que também indicaremos, abreviadamente, por $k(\alpha)$) sôbre $k(\beta_1,\ldots,\beta_n)$ tal que $\sigma(\alpha_i) = \beta_i$ $(i=1,\ldots,n)$. E' imediato que todo ponto do espaço $A_n^{\bar{k}}$ só tem um número finito de pontos conjugados. Separemos os pontos de $A_n^{\bar{k}}$ em classes, colocando numa mesma classe todos os pontos de $A_n^{\bar{k}}$ conjugados de um mesmo ponto. Obtemos assim uma partição de $A_n^{\bar{k}}$, isto é, dividimos $A_n^{\bar{k}}$ em classes tais que duas delas ou coincidem, ou, não têm nenhum elemento comum. Chamaremos ponto sôbre k a qualquer uma destas classes e indicaremos por S_n^k (ou também por S_n) o conjunto de tôdas estas classes. S_n^k é denominado espaço linear de n dimensões sôbre k. Indicaremos um ponto sôbre k por um dos pontos de $A_n^{\bar{k}}$ pertencente à correspondente classe.

Consideremos agora o anel de polinômios $R_n = k[X_1,\ldots,X_n]$ de n indeterminadas $X_1,\ldots,X_n$ com coeficientes em k. Seja $\mathfrak{M}$ um ideal de R_n. Diremos que um ponto $P(\alpha)$ de $A_n^{\bar{k}}$ é um zero de $\mathfrak{M}$ se tivermos $f(\alpha) = 0$ para todo f de $\mathfrak{M}$. E' imediato que se $P(\alpha)$ for um zero de $\mathfrak{M}$ então todos os conjugados de $P(\alpha)$ também serão zeros de $\mathfrak{M}$. Diremos que um ponto P de S_n é um zero de $\mathfrak{M}$ se um dos pontos (α) de $A_n^{\bar{k}}$ pertencente à classe P for um zero de $\mathfrak{M}$. O conjunto de todos os zeros de $\mathfrak{M}$ (pertencentes a S_n) é denominado variedade algébrica do ideal $\mathfrak{M}$ e é indicado por $\mathfrak{V}(\mathfrak{M})$. Pela prop.2,I, podemos dizer que a variedade algébrica de um ideal é o conjunto de todos os zeros comuns a um número finito de equações algébricas (formais): $f_1(X_1,\ldots,X_n) = 0,\ldots, f_s(X_1,\ldots,X_n) = 0$, onde $f_i \in R_n$

$(i=1,\ldots,s)$.

Seja W uma variedade algébrica no S_n; diremos que um polinômio f, de R_n, se anula sôbre W se todo ponto de W for um zero de f. Indicaremos por $\mathfrak{J}(W)$ o conjunto de todos os polinômios de R_n que se anulam sôbre W. O ideal $\mathfrak{J}(W)$ é denominado ideal da variedade algébrica W. Temos as seguintes proposições:

1. Se $\mathfrak{a} = R_n$ então $\mathfrak{V}(\mathfrak{a}) = \emptyset$; se $\mathfrak{a} = (0)$ então $\mathfrak{V}(\mathfrak{a}) = S_n$.
2. Se $\mathfrak{a}$ e $\mathfrak{b}$ forem dois ideais de R_n e se $\mathfrak{a} \subset \mathfrak{b}$ então $\mathfrak{V}(\mathfrak{a}) \supset \mathfrak{V}(\mathfrak{b})$.
3. $\mathfrak{V}(\mathfrak{a}+\mathfrak{b}) = \mathfrak{V}(\mathfrak{a}) \cap \mathfrak{V}(\mathfrak{b})$.
4. $\mathfrak{V}(\mathfrak{a}\mathfrak{b}) = \mathfrak{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{V}(\mathfrak{a}) \cup \mathfrak{V}(\mathfrak{b})$.
5. Se $W_1 \subset W$ (W_1 e W variedades algébricas no S_n) então $\mathfrak{J}(W_1) \supset \mathfrak{J}(W)$.
6. $\mathfrak{V}(\mathfrak{J}(W)) = W$.
7. Se $W = W_1 \cup W_2$, onde W, W_1 e W_2 são variedades algébricas, então $\mathfrak{J}(W) = \mathfrak{J}(W_1) \cap \mathfrak{J}(W_2)$.

As demonstrações destas proposições podem ser encontradas em [15], pp.78-81.

Diremos que uma variedade algébrica W é redutível quando $W = W_1 \cup W_2$, onde W_1 e W_2 são variedades algébricas e $W_1 \neq W$, $W_2 \neq W$. Uma variedade algébrica não redutível é denominada variedade algébrica irredutível. Temos o seguinte critério de irredutibilidade (15 ,pp.81-84):

Teorema 1 - Uma variedade algébrica W é irredutível quando, e sòmente quando, $\mathfrak{J}(W)$ é um ideal primo.

Ainda, neste parágrafo, daremos a decomposição de uma variedade algébrica em componentes irredutíveis. Das proposições 5 e 6 vem $\mathfrak{J}(W_1) \supset \mathfrak{J}(W)$, $\mathfrak{J}(W_1) \neq \mathfrak{J}(W)$ se $W_1 \subset W$, $W_1 \neq W$ (onde W e W_1 são variedades algébricas do S_n). Como R_n é um anel noetheriano (prop.2,I) resulta, imediatamente, que

8. Tôda cadeia decrescente de variedades algébricas do S_n tem sòmente um número finito de têrmos distintos, isto é, se $W_1 \supseteq W_2 \supset \ldots$ ($W_1, W_2, \ldots$ variedades algébricas) então existe um índice N tal que $W_i = W_{i+1}$ para todo $i \geq N$.

Desta proposição vem o

Teorema 2 - Tôda variedade algébrica é união de um número finito de variedades algébricas irredutíveis.

Seja W uma variedade algébrica; pelo teorema anterior podemos escrever

(1) $$W = W_1 \cup W_2 \cup \ldots \cup W_s,$$

onde tôdas as variedades algébricas $W_1,\ldots,W_s$ são irredutíveis. Se a decomposição (1) verificar a condição $W_i \not\subset W_1 \cup \ldots \cup W_{i-1} \cup W_{i+1} \cup \ldots \cup W_s$ $(i=1,\ldots,s)$, diremos que (1) é uma decomposição normal da variedade algébrica W. Evidentemente, se (1) não verificar esta última condição, basta suprimir as variedades algébricas W_i que estejam contidas na união das restantes, que obteremos uma decomposição normal de W. Portanto, temos

Teorema 3 - Tôda variedade algébrica admite uma decomposição normal.

Também temos o seguinte teorema de unicidade (a menos da ordem) da decomposição normal de uma variedade algébrica (15 ,pp.86-88):

Teorema 4 - Se $W=W_1 \cup \ldots \cup W_s$ e $W = W'_1 \cup \ldots \cup W'_r$ forem duas decomposições normais de uma variedade algébrica, então $r=s$ e, usando uma notação conveniente, teremos $W_i = W'_i$ $(i=1,\ldots,s)$.

2. Teorema dos zeros de Hilbert.

O problema que examinaremos, neste parágrafo, é o seguinte: dada uma variedade algébrica $W = \mathfrak{V}(\mathfrak{a})$ do S_n, determinar o conjunto de todos os polinômios f de R_n que se anulam sôbre W, isto é, determinar o ideal $\mathfrak{J}(W)$. A resposta é dada pelo

Teorema dos zeros de Hilbert - Se $\mathfrak{a}$ for um ideal de R_n então $\mathfrak{J}(\mathfrak{V}(\mathfrak{a})) = \mathrm{Rad}.\mathfrak{a}$, isto é, para todo polinômio f, que se anula sôbre $\mathfrak{V}(\mathfrak{a})$, existe uma potência conveniente de f que pertence a $\mathfrak{a}$.

Transcreveremos uma das demonstrações de O.Zariski (ver "A new proof of Hilbert's Nullstellensatz", Bull. A.M.S., vol. 53,nº4, pp.362-368). Em primeiro lugar demonstraremos o seguinte

Lema 1 - Se $V(\mathfrak{a}) = \emptyset$ então $\mathfrak{a} = (1)$.

Dêste lema, como foi observado por Rabinowitsch (Math. Ann., vol. 102 (1929), p.518) segue-se o teorema dos zeros de Hilbert. Com efeito, seja X_{n+1} uma outra indeterminada e consideremos o anel de polinômios $k[X_1,\ldots,X_n,X_{n+1}] = R_{n+1}$ e nele o ideal $\mathfrak{b} = \mathfrak{a} + (g)$, onde $g = 1 + X_{n+1}f$, f sendo um polinômio qualquer, $f \neq 0$, que se anula sôbre $V(\mathfrak{a})$. Temos $V(\mathfrak{b}) = \emptyset$, no espaço S_{n+1}, logo, pelo lema 1, $\mathfrak{b} = (1)$; então existe uma identidade da forma $\sum_i A_i h_i + gh = 1$, onde $A_i \in \mathfrak{a}$, $h \in R_{n+1}$ e $h_i \in R_{n+1}$. Substituindo X_{n+1} por $-1/f$ e eliminando os denominadores virá uma relação da forma $\sum_i A_i B_i = f^p$, onde $B_i \in R_n$. Isto nos mostra que $f \in \text{Rad.}\,\mathfrak{a}$, logo, $J(V(\mathfrak{a})) \subset \text{Rad.}\,\mathfrak{a}$; mas por outro lado, temos $\text{Rad.}\,\mathfrak{a} \subset J(V(\mathfrak{a}))$, então, $J(V(\mathfrak{a})) = \text{Rad.}\,\mathfrak{a}$. Assim, uma vez demonstrado o lema 1, estará demonstrado o teorema dos zeros de Hilbert. Provaremos agora que o lema 1 é uma consequência do

Lema 2 - Se um campo finito de integridade $I_n = k[\xi_1,\ldots,\xi_n]$ (1) for um corpo, então êle será uma extensão algébrica de k.

Com efeito, seja $\mathfrak{a}$ um ideal de R_n, $\mathfrak{a} \neq R_n$, e seja $\mathfrak{p}$ um ideal máximal de R_n que contenha $\mathfrak{a}$. Se provarmos que $V(\mathfrak{p}) \neq \emptyset$ resultará que $V(\mathfrak{a}) \neq \emptyset$, pois $\mathfrak{a} \subset \mathfrak{p}$ e então $V(\mathfrak{a}) \supset V(\mathfrak{p})$ (prop.2). Consideremos o anel resíduo $\bar{R}_n = R_n/\mathfrak{p} = k[\alpha_1,\ldots,\alpha_n]$, onde $\alpha_i = \mathfrak{p}$-resíduo de X_i $(i=1,\ldots,n)$. Pelo lema 2 virá que $\alpha_1,\ldots,\alpha_n$ são algébricos sôbre k, portanto, $P(\alpha_1,\ldots,\alpha_n)$ é um ponto do espaço afim $A_n^{\bar{k}}$. O ponto P de S_n, determinado por $(\alpha_1,\ldots,\alpha_n)$ é um zero de $\mathfrak{p}$, portanto, $V(\mathfrak{p}) \neq \emptyset$. Demonstrámos assim que de $\mathfrak{a} \neq R_n$ vem $V(\mathfrak{a}) \neq S_n$, isto é, demonstrámos o lema 1.

Passamos agora a demonstrar o lema 2. Se $n=1$ temos $I_1 = k[\xi_1]$ que, por hipótese, é um corpo, logo, $1/\xi_1 = f(\xi_1)$,

---

(1) Seja k um sub-corpo de um corpo K e consideremos n elementos $\xi_1,\ldots,\xi_n$ de K. O anel $I_n = k[\xi_1,\ldots,\xi_n]$, gerado pelos elementos $\xi_1,\ldots,\xi_n$ sôbre o corpo k é denominado campo finito de integridade.

onde f é um polinômio em uma indeterminada X com coeficientes em k. Portanto ξ_1 é raiz do polinômio $Xf(X)-1$, isto é, ξ_1 é algébrico sôbre k; isto demonstra o lema 2 para $n=1$. Suponhamos, por indução, o lema 2 verdadeiro para campos finitos de integridade com $n-1$ geradores e consideremos o campo finito de integridade $I_n = k[\xi_1,\ldots,\xi_n]$. Temos $I_n = k(\xi_1)[\xi_2,\ldots,\xi_n]$, portanto, ξ_i $(i=2,\ldots,n)$ é algébrico sôbre $k(\xi_1)$. Seja $f_i(X)$ um polinômio irredutível de ξ_i; podemos supôr que os coeficientes de f_i pertençam a $k[\xi_1]$. Indiquemos por b_i o coeficiente do têrmo de mais alto grau de $f_i(X)$. Seja ω, $\omega \neq 0$, um elemento qualquer de I_n, então $\omega = f(\xi_1,\ldots,\xi_n)$, onde f tem coeficientes em k. Se multiplicarmos ω por uma potência conveniente de $b_2\ldots b_n$ obteremos $(b_2\ldots b_n)^\rho \omega = \sum_{\mu=1}^{N} g_\mu \Omega_\mu$, onde $N=m_2\ldots m_n$ (m_i grau de f_i), $g_\mu \in k[\xi_1]$ e $\Omega_1,\ldots,\Omega_N$ indicam (numa certa ordem) todos os produtos $\xi_2^{\mu_2}\ldots\xi_n^{\mu_n}$, com $0 \leq \mu_i \leq m_i-1$ $(i=2,\ldots,n)$. Seja $r = [I_n : k(\xi_1)]$ e seja $\omega_1=1, \omega_2,\ldots,\omega_r$ uma base de I_n sôbre $k(\xi_1)$. Temos $\Omega_\mu = \sum_{j=1}^{r} a_{\mu j}\omega_j$, onde $a_{\mu j} \in k(\xi_1)$; portanto, para cada Ω_μ existe um elemento B_μ de $k[\xi_1]$ tal que $B_\mu\Omega_\mu = \sum_{j=1}^{r} A_{\mu j}\omega_j$, onde $A_{\mu j} \in k[\xi_1]$ $(j=1,\ldots,r)$. Pondo $b_1=B_1\ldots B_N$ e $b = b_1b_2\ldots b_n$ teremos $b^\rho\omega = \sum_{j=1}^{r} c_j\omega_j$, onde $c_j \in k[\xi_1]$ e b não depende de ω. Seja agora ζ um elemento qualquer de $k[\xi_1]$, $\zeta \neq 0$, e apliquemos a relação anterior para $\omega = 1/\zeta \in k(\xi_1)$. Teremos $b^\rho/\zeta = c_1 + c_2\omega_2 + \ldots + c_r\omega_r$ e sendo $\omega_1=1,\omega_2,\ldots,\omega_r$ uma base de I_n sôbre $k(\xi_1)$ virá $b^\rho/\zeta = c_1 \in k[\xi_1]$. Suponhamos que ξ_1 seja transcendente sôbre k; escolhendo ζ diferente de qualquer um dos fatores irredutíveis de b obteríamos um absurdo. Isto prova que ξ_1 é algébrico sôbre k, e, portanto, que I_n é uma extensão algébrica de k. (q.e.d.).

Daremos agora algumas consequências do teorema dos zeros. Consideremos o caso em que $\mathfrak{a}$ é um ideal primo $\mathfrak{p}$; teremos $\mathfrak{I}(\mathfrak{V}(\mathfrak{p})) = \text{Rad.}\,\mathfrak{p} = \mathfrak{p}$, portanto, pelo teorema 1, $\mathfrak{V}(\mathfrak{p})$ é uma variedade algébrica irredutível. Temos assim o

Corolário 1 - Se $\mathfrak{p}$ for um ideal primo de R_n, então $\mathfrak{V}(\mathfrak{p})$ será uma variedade algébrica irredutível.

Também temos:

Corolário 2 - A aplicação $\mathfrak{p} \longrightarrow \mathfrak{V}(\mathfrak{p})$, onde $\mathfrak{p}$ é um ideal primo de R_n, é uma aplicação biunívoca do conjunto dos ideais primos de R_n sôbre o conjunto das variedades algébricas irredutíveis do S_n.

Notemos que a aplicação inversa da descrita no corolário 2 é a seguinte: $W \longrightarrow \mathfrak{J}(W)$, onde W é uma variedade algébrica irredutível do S_n.

Seja P um ponto do espaço linear S_n; demonstraremos que $\mathfrak{J}(P)$ é um ideal máximal de R_n. Com efeito, $\mathfrak{J}(P)$ é formado por todos os polinômios f de R_n que se anulam num dos pontos (α) da classe P, portanto, $\mathfrak{J}(P)$ é o núcleo do homomorfismo: $f \in R_n \longrightarrow f(\alpha) \in k[\alpha]$. Mas $k[\alpha]$ é um corpo, logo, $\mathfrak{J}(P)$ é um ideal máximal. Demonstrámos, em particular, que todo ponto do espaço linear S_n é uma variedade algébrica irredutível. Seja agora $\mathfrak{p}$ um ideal máximal de R_n e consideremos a variedade algébrica de $\mathfrak{p}$. Pelo lema 1 temos $\mathfrak{V}(\mathfrak{p}) \neq \emptyset$; seja P um ponto de $\mathfrak{V}(\mathfrak{p})$. Temos $\{P\} \subset \mathfrak{V}(\mathfrak{p})$, portanto, $\mathfrak{J}(P) \supset \mathfrak{J}(\mathfrak{V}(\mathfrak{p}))$; mas $\mathfrak{J}(\mathfrak{V}(\mathfrak{p})) = \mathfrak{p}$, logo, $\mathfrak{J}(P) = \mathfrak{p}$ e então (prop.6) $\{P\} = \mathfrak{V}(\mathfrak{p})$. Demonstrámos assim que a variedade algébrica de um ideal máximal de R_n é um ponto do espaço linear S_n. E' fácil ver que a ideais máximais distintos de R_n correspondem pontos distintos de S_n e reciprocamente. Dêstes resultados tiramos o

Corolário 3 - A aplicação $\mathfrak{p} \longrightarrow \mathfrak{V}(\mathfrak{p})$, onde $\mathfrak{p}$ é um ideal máximal de R_n é uma aplicação biunívoca do conjunto de todos os ideais máximais de R_n sôbre o espaço linear S_n.

3. Ponto geral de uma variedade algébrica irredutível.

Seja W, $W \neq \emptyset$, uma variedade algébrica irredutível do espaço linear S_n. Diremos que uma n-upla $(\xi_1,\ldots,\xi_n)$, de elementos pertencentes a alguma extensão de k, é um ponto geral de W se estiver verificada a condição: se $f \in R_n = k[X_1,\ldots,X_n]$ então $f(\xi) = 0$ quando, e sòmente quando, $f(\alpha) = 0$ para todo ponto (α) de W. Seja $\mathfrak{p} = \mathfrak{J}(W)$ o ideal de W e consideremos o anel resíduo $\bar{R}_n = R_n/\mathfrak{p}$. $\bar{R}_n$ contém um corpo k' isomorfo a k; identificando k' com k e indicando por ξ_i o $\mathfrak{p}$-resíduo de X_i $(i=1,\ldots,n)$ teremos $\bar{R}_n = k[\xi_1,\ldots,\xi_n]$ que é um campo finito de integridade. Esta n-upla $(\xi_1,\ldots,\xi_n)$ é um ponto geral de W, pois se $f \in R_n$ teremos $f(\xi) = 0$ quando, e sòmente quando, $f \in \mathfrak{p}$ e, portanto, quando, e sòmente quando, $f(\alpha) = 0$ para todo ponto (α) de W.

Seja V uma variedade algébrica irredutível do S_n e seja $(\xi_1,\ldots,\xi_n)$ um ponto geral de V. O campo finito de integridade $k[\xi_1,\ldots,\xi_n]$ é denominado anel das coordenadas de V e é indicado por $\mathfrak{R}[V]$. O corpo de quocientes de $\mathfrak{R}[V]$ é denominado corpo das funções racionais sôbre V e é indicado por $\mathfrak{J}(V)$; notemos que $\mathfrak{J}(V) = k(\xi_1,\ldots,\xi_n)$. Seja W uma sub-variedade algébrica de V; temos, $\mathfrak{J}(V) \subset \mathfrak{J}(W)$, portanto, ao ideal $\mathfrak{J}(W)$ corresponde, pelo homomorfismo $\sigma : R_n \longrightarrow \mathfrak{R}[V]$ (que a $F \in R_n$ faz corresponder $F(\xi) \in \mathfrak{R}[V]$), um ideal de $\mathfrak{R}[V]$. Reciprocamente, se $\mathfrak{a}'$ for um ideal de $\mathfrak{R}[V]$ teremos $\sigma^{-1}(\mathfrak{a}') \supset \mathfrak{J}(V)$, portanto, a $\mathfrak{a}'$ corresponderá uma sub-variedade algébrica de V. Observemos que se $\mathfrak{a}'$ for um ideal primo então $\sigma^{-1}(\mathfrak{a}')$ também será um ideal primo e recìprocamente; é imediato que a ideais primos distintos de $\mathfrak{R}[V]$ correspondem, por meio de σ^{-1}, ideais primos distintos de R_n. Portanto, pelo corolário 2, teremos:

9. A aplicação $\mathfrak{p}' \longrightarrow \mathfrak{V}(\sigma^{-1}(\mathfrak{p}'))$ (onde $\mathfrak{p}'$ é um ideal primo de $\mathfrak{R}[V]$) é uma aplicação biunívoca do conjunto de todos os ideais primos de $\mathfrak{R}[V]$ sôbre o conjunto de tôdas as sub-variedades algébricas irredutíveis de V.

Sejam V e W duas variedades algébricas irredutíveis, com $W \subset V$; indiquemos por $(\xi_1,\ldots,\xi_n)$ um ponto geral de

V. Seja $p(W/V)$ o ideal primo de W em $\mathfrak{R}[V]$. Por um dos teoremas de isomorfismo (ver [4], p.36) teremos $R_n/\mathfrak{J}(W) \cong$ $\cong R_n/\mathfrak{J}(V) \Big/ \mathfrak{J}(V)/\mathfrak{J}(W) = \mathfrak{R}[V]/p(W/V)$, portanto, $\mathfrak{R}[V]/p(W/V) \cong$ $\cong k[\eta_1, \ldots, \eta_n]$, onde $(\eta_1, \ldots, \eta_n)$ é um ponto geral de W. Esta relação nos mostra que para obter um ponto geral de W é bastante tomar os $p(W/V)$-resíduos dos elementos $\xi_1, \ldots, \xi_n$.

Ainda, neste parágrafo, faremos algumas aplicações dos resultados sôbre aneis de quocientes (ver cap.I, §4). Seja V uma variedade algébrica irredutível e seja $\mathfrak{R}[V] = k[\xi_1, \ldots, \xi_n]$ o anel das coordenadas de V. Consideremos uma sub-variedade algébrica irredutível W de V e seja $p(W/V)$ o ideal primo de W no anel $\mathfrak{R}[V]$. O anel de quocientes $Q(W/V)$ de $\mathfrak{R}[V]$ em relação ao ideal primo $p(W/V)$ tem um único ideal máximal $m(W/V)$. Na passágem do anel $\mathfrak{R}[V]$ ao anel de quocientes $Q(W/V)$ só são conservados os ideais que estão contidos em $p(W/V)$ (proposições 26 e 27 do cap.I), portanto, podemos dizer que <u>só são conservadas as sub-variedades algébricas de V que contêm W</u>. Por êste motivo diremos que $Q(W/V)$ nos permite estudar a variedade algébrica V num entôrno da sub-variedade W. E' fácil demonstrar a relação:

10. $Q(W/V)/p(W/V) \cong \mathfrak{J}(W)$.

C A P I T U L O III.

Teoria da dimensão.

§1 - Grau de transcendência.

Seja k um sub-corpo de um corpo K (neste caso, K é também chamado extensão de k, ou, sôbre-corpo de k). Consideremos o anel de polinômios $R_n = k[X_1,\ldots,X_n]$.

Definição 1 - Diremos que n elementos $x_1,\ldots,x_n$ de K, são algébricamente independentes sôbre k (ou, relativamente a k) se para todo polinômio f, $f \in R_n$, $f \neq 0$, tivermos $f(x_1,\ldots,x_n) \neq 0$. Caso contrário, diremos que os elementos $x_1,\ldots,x_n$ são algébricamente dependentes sôbre k.

Definição 2 - Seja $X = (x_\alpha)_{\alpha\in A}$ um sub-conjunto de K. Diremos que X é um conjunto transcendente sôbre k (ou, que os elementos de X são algèbricamente independentes sôbre k, ou, que a família $(x_\alpha)_{\alpha\in A}$ é algèbricamente livre sôbre k) se os elementos de todo sub-conjunto finito de X forem algèbricamente independentes sôbre k.

Definição 3 - Diremos que um sub-conjunto X de K é uma base de transcendência sôbre k, se 1) X é um conjunto transcendente sôbre k; 2) K é uma extensão algébrica de $k(X) = k(x_\alpha)_{\alpha\in A}$.

Demonstram-se as seguintes proposições (ver [4], vol.I, pp.110-112):

1. Tôda extensão K de k tem uma base de transcendência sôbre k.
2. Seja X um sub-conjunto de K; se X for transcendente sôbre k, então X pode ser imerso numa base de transcendência de K sôbre k.

3. Se K tiver uma base de transcendência finita sôbre k, então qualquer base de transcendência de K sôbre k é finita e tem o mesmo número de elementos.

Definição 4 - Seja K uma extensão de k e suponhamos que K tenha uma base de transcendência finita sôbre k, então o número de elementos desta base é denominado grau de transcendência de K sôbre k e é indicado por gr.tr.K/k.

Demonstra-se o seguinte (ver [15],pp.251-252, ou, [4],vol.I,pp.113-114):

Teorema 1 - Seja K uma extensão de k e Ω uma extensão de K; suponhamos que os graus de transcendência de K sôbre k e de Ω sôbre K sejam finitos. Nestas condições temos: gr.tr.Ω/k = gr.tr.Ω/K + + gr.tr. K/k.

Definição 5 - Seja R um campo de integridade que contém um corpo k e seja Ω o corpo de quocientes de R; suponhamos que o grau de transcendência de Ω sôbre k seja finito. Então chama-se grau de transcendência de R sôbre k ao grau de transcendência de Ω sôbre k.

E' imediato que existe uma base de transcendência de Ω sôbre k cujos elementos pertencem a R.

Sejam R e R' dois campos de integridade que contêm um mesmo corpo k e suponhamos que exista um homomorfismo τ de R sôbre R'. Suponhamos ainda que o grau de transcendência de R sôbre k seja finito. E' imediata a proposição:

4. Se τ for um isomorfismo então gr.tr. R'/k = = gr.tr. R/k.

Demonstraremos o teorema (no qual estamos fazendo as mesmas hipóteses acima):

Teorema 2 - gr.tr. $R'/k \leq$ gr.tr. R/k; ainda mais, se gr.tr. $R'/k =$ gr.tr. R/k, então τ é um isomorfismo.

A primeira parte do teorema é imediata. Vejamos a segunda. Seja $\{x'_1,\ldots,x'_n\}$ $(x'_i \in R')$ uma base de transcendência de R' sôbre k; como τ é um homomorfismo de R sôbre R' existem elementos $x_1,\ldots,x_n$ em R tais que $\tau x_i = x'_i$ $(i=1,..,n)$. E' fácil ver que $\{x_1,\ldots,x_n\}$ é uma base de transcendência de R sôbre k. Precisamos demonstrar que se $u \in R$, $u \neq 0$, então $\tau u \neq 0$. Ora, u é algébrico sôbre $k[x_1,\ldots,x_n]$, portanto, u é raiz de uma equação da forma: $a_o(x)u^m + \ldots + a_m(x) = 0$, onde $a_i(x) \in k[x_1,\ldots,x_n]$ e $a_m(x) \neq 0$. Desta equação vem $a_o(x')u'^m + \ldots + a_m(x') = 0$, onde $a_i(x') \in k[x'_1,\ldots,x'_n]$, $u'=\tau u$ e $a'_m(x') \neq 0$ (pois $a_m(x)\neq 0$ e $\{x'_1,\ldots,x'_n\}$ é uma base de transcendência de R' sôbre k); portanto, $u' = \tau u \neq 0$. (q.e.d.).

Seja $\wp$ um ideal primo de um campo de integridade R; suponhamos que R contenha um corpo k e que gr.tr.$R/k = r$ (finito). Nestas condições daremos a seguinte

Definição 6 - Chama-se dimensão do ideal primo $\wp$ sôbre k ao grau de transcendência de $R'=R/\wp$ sôbre k, se $\wp \neq R$; se $\wp = R$ poremos, por definição, $\dim._k \wp = -1$.

Observemos que podemos supôr que $k \subset R'$ e, então, pelo teorema 2, o grau de transcendência de R' sôbre k é finito. Ainda pelo mesmo teorema temos $0 \leq \dim.\wp \leq r$ (se $\wp \neq R$) e $\dim.\wp = r$ quando, e sòmente quando, $\wp = (0)$. Portanto, se também supuzermos $\wp \neq (0)$ teremos $0 \leq \dim.\wp \leq r-1$, onde $\wp$ é um ideal primo de R, $\wp \neq R$.

Consideremos o anel resíduo $R' = R/\wp$ e seja $\wp_1$ um ideal primo que contenha $\wp$. Ao ideal $\wp_1$ corresponderá, pelo homomorfismo canônico de R sôbre R', um ideal primo $\wp'_1$ de R' e temos $\wp'_1 = \wp_1/\wp$. Mas $R'/\wp'_1 = R/\wp \,/\, \wp_1/\wp \cong R/\wp = R'$, portanto, $\dim._k \wp'_1 = \dim._k \wp_1$, isto é, as dimensões de dois ideais primos correspondentes, em campos de integridade homomorfos, são iguais. D'aqui podemos tirar a seguinte propriedade (onde estamos usando as mesmas notações e hipóteses):

5. Se $\wp \subset \wp_1$ e $\wp \neq \wp_1$ então $\dim._k \wp > \dim._k \wp_1$.

Com efeito, consideremos o anel resíduo $R/\wp = R'$ e nele o ideal primo $\wp_1' = \wp_1/\wp$; temos $\wp_1' \neq (0)$ pois $\wp_1 \neq \wp$. Portanto, pela proposição acima e pelo teorema 2, virá $\dim._k \wp_1 = \dim._k \wp_1' < \text{gr.tr.}R'/k = \dim._k \wp$. (q.e.d.).

Da proposição 5 resulta, imediatamente, o

Teorema 3 - Se no campo de integridade R ($k \subset R$ e gr.tr. $R/k = r$, finito) tivermos uma cadeia estritamente crescente de ideais primos: $(0) \subset \wp_1 \subset \wp_2 \subset \ldots \subset \wp_v \neq R$ (onde $\wp_i \neq \wp_{i+1}$) então $r-1 \geq \dim. \wp_1 > \dim. \wp_2 > \ldots > \dim. \wp_v \geq 0$.

Definição 7 - Um ideal primo $\wp$, $\wp \neq (0)$, de um campo de integridade R é denominado ideal primo mínimal se o único ideal contido pròpriamente em $\wp$ for o ideal nulo.

Pela proposição 5 teremos:

6. Seja R um campo de integridade que contém um corpo k; seja gr.tr. $R/k = r$ (finito). Se dim. $\wp = 0$, onde $\wp$ é um ideal primo de R, então $\wp$ é um ideal máximal de R; se dim. $\wp = r-1$ então $\wp$ é um ideal primo mínimal de R.

No caso de um campo de integridade qualquer (mas que verifique as condições da proposição 6) não podemos, em geral, inverter as propriedades acima, isto é, se $\wp$ for máximal (mínimal) não podemos afirmar que dim. $\wp = 0$ (dim. $\wp = r-1$). O caso que nos interessa, neste trabalho, é aquele em que R é um campo finito de integridade (e, portanto, anel das coordenadas de uma variedade algébrica irredutível), para tais campos de integridade poderemos dar respostas afirmativas às duas questões acima. Se R for o anel de polinômios em n indeterminadas: $R = k[X_1, \ldots, X_n]$, poderemos resolver as questões anteriores por processos elementares. Em primeiro lugar demonstram-se os teoremas (ver [15], pp.264-265, ou, [5], p.42):

Teorema 4 - Se f, $f \neq 0$, for um polinômio irredutível do anel R_n, então o ideal principal $\wp = (f)$ será um ideal primo mínimal.

Teorema 5 - Se $\wp$ for um ideal primo mínimal do anel R_n então $\wp$ será um ideal principal.

Dêstes dois resultados decorrem, fàcilmente, o seguinte (ver [15], p.265):

Teorema 6 - Se $\wp$ for um ideal primo mínimal de R_n então $\dim._k \wp = n-1$.

Pela aplicação do lema 2 do capítulo II, teremos:

Teorema 7 - Se $\wp$ for um ideal máximal de R_n então $\dim. \wp = 0$.

Definição 8 - Seja V uma variedade algébrica irredutível do espaço linear S_n^k e seja $\wp = \mathfrak{J}(V) \subset R_n$; chamaremos dimensão (sôbre k) da variedade algébrica V à dimensão do ideal primo $\wp$.

Pelas definições dadas anteriormente podemos dizer que a dimensão de uma variedade algébrica V, não vazia, é igual ao grau de transcendência de $\mathfrak{R}[V]$ sôbre k, ou seja, é igual ao grau de transcendência do corpo $\mathfrak{F}(V)$ sôbre k. Se $V \neq \emptyset$ teremos $0 \leq \dim._k V \leq n$; ainda mais, pela prop.6 e pelo teorema 7, teremos, $\dim. V = 0$ quando, e sòmente quando, V for um ponto. Também temos $\dim. V = n$ quando, e sòmente quando, $V = S_n$. O teorema 6 nos mostra que tôda hiper-superfície algébrica irredutível (isto é, variedade algébrica de um ideal principal (f), onde $f \in R_n$, $f \neq 0$, e f é irredutível sôbre k) do espaço linear S_n tem dimensão n-1 e reciprocamente.

§2 - Dependência inteira.

Seja R um sub-anel de um anel Ω; então podemos considerar Ω como um R-módulo (ver [15], pp.285-286). Diremos que Ω é um R-módulo finito se existirem elementos $\omega_1, \ldots, \omega_n$ em Ω tais que $\Omega = R\omega_1 + \ldots + R\omega_n$. Daremos a seguinte

Definição 9 - Diremos que um elemento ω de um R-módulo Ω, onde R é um sub-anel do anel Ω e R tem elemento unidade, é inteiro sôbre R, se ω for raiz de um polinômio $f = X^n + a_1X^{n-1} + \ldots + a_n$, onde $a_i \in R$ $(i=1,\ldots,n)$.

Temos a seguinte proposição (ver [15], p.290):

7. Se $\omega \in \Omega$ for inteiro sôbre R e se Ω tiver elemento unidade, então $R[\omega]$ é um R-módulo finito.

Com efeito, por hipótese, ω satisfaz uma relação da forma $\omega^n + a_1\omega^{n-1} + \ldots + a_n = 0$ $(a_i \in R)$; portanto, tôda potência de ω, ω^m, com $m \geq n$, é combinação linear de $1, \omega, \ldots, \omega^{n-1}$ com coeficientes em R. Isto nos mostra que $R[\omega] = R.1 + R.\omega + \ldots + R.\omega^{n-1}$, ou seja, $R[\omega]$ é um R-módulo finito. (q.e.d.).

Da definição de R-módulo finito resulta, imediatamente, que

8. Seja R um sub-anel de um anel R_1 que, por sua vez, é um sub-anel de um anel R_2; suponhamos que R_1 seja um R-módulo finito e que R_2 seja um R_1-módulo finito. Nestas condições, R_2 é um R-módulo finito.

Demonstraremos o (cfr. [15], p.289):

Teorema 8 - Se o anel Ω for um R-módulo finito ($R \subset \Omega$ e R sub-anel de Ω, $1 \in R$) com elemento unidade, então todo elemento de Ω é inteiro sôbre R.

Com efeito, temos $\Omega = \sum_{i=1}^{n} R.\omega_i$, onde $\omega_i \in \Omega$. Seja α um elemento qualquer de Ω, teremos $\alpha\omega_i \in \Omega$, logo $\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$, de onde vem $\sum_{j=1}^{n} (a_{ij} - \delta_{ij}\alpha)\omega_j = 0$ $(i=1,\ldots,n;$ δ_{ij} símbolo de Kronecker) e então $\Delta.\omega_i = 0$ $(\Delta = |a_{ij} - \delta_{ij}\alpha|)$. Mas $1 = \sum_{i=1}^{n} b_i\omega_i$ $(b_i \in R)$, logo,

$\Delta = \sum_{i=1}^{n} b_i \Delta\omega_i = 0$, portanto, $|a_{ij} - \delta_{ij}\alpha| = 0$. Esta última relação nos mostra que α é inteiro sôbre R. (q.e.d.).

Seja R um sub-anel de um anel R' e suponhamos que R' tenha elemento unidade. Das proposições 7 e 8 e do teorema 8 resulta, imediatamente, que

Teorema 9 - O conjunto $\bar{R}$ de todos os elementos de R' que são inteiros sôbre R, é um sub-anel de R'.

Chamaremos $\bar{R}$ de fêcho inteiro de R em R'. Se $R = \bar{R}$ diremos que R é inteiramente fechado em R'. Se R for um campo de integridade e se R' for o corpo de quocientes de R, então diremos, simplesmente, que R é inteiramente fechado, se $R = \bar{R}$.

Seja R um campo de integridade inteiramente fechado no seu corpo de quocientes Ω; seja Σ uma extensão algébrica de Ω. Indiquemos por $\bar{R}$ o fêcho inteiro de R em Σ. Nestas condições temos (ver [15], p.294):

9. Σ é o corpo de quocientes de $\bar{R}$.

Com efeito, todo elemento α de Σ é raiz de uma equação $a_0\alpha^n + \ldots + a_n = 0$ com coeficientes em R. Multiplicando ambos os membros desta igualdade por a_0^{n-1} teremos $(a_0\alpha)^n + a_0a_1(a_0\alpha)^{n-1} + \ldots + a_0^{n-1}a_{n-1}(a_0\alpha) + a_0^n a_n = 0$, portanto, $a_0\alpha$ é inteiro sôbre R, logo, $a_0\alpha = b_0 \in \bar{R}$. D'aqui vem $\alpha = b_0/a_0$, o que completa a demonstração de 9.

10. Se $\bar{R}$ for um R-módulo finito, então Σ será uma extensão algébrica finita de Ω.

Com efeito, temos $\bar{R} = \sum_{i=1}^{s} R.\omega_i$, onde $\omega_i \in \bar{R}$. Mas, pela demonstração da prop.9, todo elemento de Σ é o quociente de um elemento de $\bar{R}$ por um elemento de R. Portanto, temos $\Sigma = \sum_{i=1}^{s} \Omega.\omega_i$, o que demonstra a proposição 10.

Notemos que se Σ for uma extensão algébrica finita de Ω, $\bar{R}$ não será, necessàriamente, um R-módulo finito. Um exemplo foi dado por F.K.Schmidt (ver "Über die Erhaltung der Kettensätze der Idealtheorie bei beliebigen endlichen Körperweiterungen", M.Z., vol.41(1936)). No entretanto, isto sempre acontece no caso em que R é um anel de polinômios com coeficientes num cor

po k. Precisamente, temos o teorema (devido a F.K.Schmidt; ver [15], pp.295-297):

Teorema 10 - Seja R um anel de polinômios em r indeterminadas $X_1,\ldots,X_r$ sôbre um corpo k; se Σ for uma extensão algébrica finita de Ω (corpo de quocientes de R) então o fêcho inteiro $\bar{R}$ de R em Σ será um R-módulo finito.

Só demonstraremos êste teorema no caso em que Σ é uma extensão algébrica separável de Ω. Para o caso geral ver o trabalho de F.K.Schmidt, citado acima. Pelo teorema do elemento primitivo temos $\Sigma = \Omega(\xi)$, onde podemos supôr que $\xi \in \bar{R}$. Como Σ é extensão separável de Ω, ξ é raiz de um polinômio separável $f = X^n + a_1X^{n-1}+\ldots+a_n$, onde $a_i \in R$ e $n=[\Sigma:\Omega]$. As raizes de f são tôdas distintas; indiquemo-las por $\xi_1=\xi$, $\xi_2,\ldots,\xi_n$ (onde $\xi_2,\ldots,\xi_n$ pertencem a $\bar{\Omega}$, extensão algébrica algèbricamente fechada de Ω). Todo elemento ω de Σ pode ser escrito sob a forma $\omega = A_0(X) + A_1(X)\,\xi + \ldots + A_{n-1}(X)\,\xi^{n-1}$, onde $A_i(X)\in\Omega$. Introduziremos os conjugados de ω: $\omega_i = A_0(X) + A_1(X)\,\xi_i + \ldots + A_{n-1}(X)\,\xi_i^{n-1}$ $(i=1,\ldots,n;$ $\omega_1 = \omega)$. Dêste sistema de equações tiramos $\Delta . A_j(X) = \sum_{i=1}^{n} B_{ij}\,\omega_i$ $(j=0,1,\ldots,n-1)$, onde Δ é o determinante de Vandermonde $\begin{vmatrix} 1 & \xi_i & \xi_i^2 & \ldots & \xi_i^{n-1} \end{vmatrix}$ $(i=1,\ldots,n)$, que, certamente, é diferente de zero e B_{ij} é o complemento algébrico do elemento ξ_i^j. Notemos que $\Delta^2 = \prod_{i<j}(\xi_i-\xi_j)^2$ é uma função simétrica de $\xi_1,\ldots,\xi_n$, portanto, é uma função racional dos coeficientes $a_1,\ldots,a_n$, isto é, $\Delta^2\in\Omega$; mas, por outro lado, Δ^2 é inteiro sôbre R, logo, $\Delta^2\in R$. Suponhamos agora que ω seja inteiro sôbre R, então, $A_j(X).\Delta$ é inteiro sôbre R (pois B_{ij} é inteiro sôbre R), logo, $A_j(X).\Delta^2$ é também inteiro sôbre R. Mas $A_j(X)\,\Delta^2\in\Omega$, portanto, $A_j(X)\,\Delta^2 = P_j(X)\in R$. D'aqui tiramos $A_j(X)=P_j(X)/\Delta^2$, portanto, $\omega = \sum_{j=0}^{n-1}\frac{P_j(X)}{\Delta^2}\,\xi^j$. Esta relação nos mostra que $\bar{R} \subset R.\frac{1}{\Delta^2} + R.\frac{\xi}{\Delta^2} + \ldots + R.\frac{\xi^{n-1}}{\Delta^2}$, isto é, $\bar{R}$ é

um sub-módulo de um R-módulo finito, portanto, $\bar{R}$ é um R-módulo finito, pois R é um anel noetheriano (ver [14], vol.II, § 99).

Seja R um sub-anel de um campo de integridade R' e suponhamos que R contenha um corpo k. Seja r = gr.tr. R/k. Suporemos ainda que todo elemento de R' seja inteiro sôbre R (neste caso diremos que R' depende inteiramente de R, ou, que R e R' estão ligados pela relação de dependência inteira). Nestas condições demonstraremos o (Cfr. [15], pp.298-300):

Teorema 11 - Sejam $\mathfrak{p}$ e $\mathfrak{p}'$ dois ideais primos de R e R', respectivamente, ligados pela relação $\mathfrak{p} = \mathfrak{p}' \cap R$; então temos $\dim._k \mathfrak{p} = \dim._k \mathfrak{p}'$.

Demonstração - Se $\mathfrak{p} = R$ (ou $\mathfrak{p}' = R'$) o teorema é imediato. Suponhamos $\mathfrak{p} \neq R$ (e, portanto, $\mathfrak{p}' \neq R'$); podemos considerar $R/\mathfrak{p}$ como um sub-anel de $R'/\mathfrak{p}'$. Para chegarmos à tese do teorema basta demonstrar que todo elemento ω' de $R'/\mathfrak{p}'$ é algébrico sôbre $R/\mathfrak{p}$ (ver teorema 1). Seja ω um elemento de R' cujo $\mathfrak{p}'$-resíduo é ω'; como R' depende inteiramente de R teremos $\omega^n + a_1\omega^{n-1} + \ldots + a_n = 0$, onde $a_i \in R$. Indicando por a_i' o $\mathfrak{p}$-resíduo de a_i virá $\omega'^n + a_1'\omega'^{n-1} + \ldots + a_n' = 0$, onde $a_i' \in R/\mathfrak{p}$, isto é, ω' é algébrico sôbre $R/\mathfrak{p}$. (q.e.d.).

Observemos que na demonstração anterior provámos que $R'/\mathfrak{p}'$ depende inteiramente de $R/\mathfrak{p}$.

Terminaremos êste parágrafo dando o enunciado do teorema de normalização de Emmy Noether; a sua demonstração poderá ser encontrada em [15], pp.301-316, ou, [5], pp.41-42.

Teorema de normalização - Seja $R = k[\xi_1, \ldots, \xi_n]$ um campo finito de integridade e indiquemos por r o seu grau de transcendência sôbre k. Então existem r elementos $x_1, \ldots, x_r$ em R tais que R dependa inteiramente de $R_0 = k[x_1, \ldots, x_r]$; ainda mais, se k for um corpo infinito, podemos escolher $x_1, \ldots, x_r$ como combinações lineares, com coeficientes em k, dos geradores $\xi_1, \ldots, \xi_n$ de R sôbre k.

§ 3 - Relações entre os ideais primos de dois campos de integridade ligados pela relação de dependência inteira.

Sejam R e R' dois campos de integridade, sendo R um sub-anel de R'; suponhamos que R e R' tenham o mesmo elemento unidade e que todo elemento de R' seja inteiro sôbre R. Neste parágrafo, quando considerarmos um ideal primo $\mathfrak{p}$ de R (ou de R'º estará subentendido que $\mathfrak{p} \neq R$ (ou $\mathfrak{p} \neq R'$).

Lema 1 - R' é um corpo quando, e sòmente quando, R é um corpo.

Demonstração - E' imediato que se R for um corpo, R' será também um corpo. Vejamos a recíproca. Seja ω um elemento de R, $\omega \neq 0$; o seu inverso $1/\omega$ pertence a R', portanto, satisfaz uma relação da forma $(1/\omega)^n + a_1(1/\omega)^{n-1} + \ldots + a_n = 0$, onde $a_i \in R$ $(i=1,\ldots,n)$. D'aqui tiramos $1/\omega = -a_1 - a_2\omega - \ldots - a_n\omega^{n-1}$ e, portanto, $1/\omega \in R$. Isto nos mostra que R é um corpo. (q.e.d.).

Lema 2 - Seja $\mathfrak{p}$ um ideal primo de R e consideremos o conjunto $S = R - \mathfrak{p}$ que é um sistema multiplicativo tanto em R como em R'. O anel R'_S é então inteiramente dependente do anel $R_{\mathfrak{p}}$.

Com efeito, um elemento de R'_S é da forma ω/s, onde $\omega \in R'$ e $s \in S$. O elemento ω é inteiro sôbre R, portanto, satisfaz uma relação da forma $\omega^n + a_1\omega^{n-1} + \ldots + a_n = 0$ $(a_i \in R)$. D'aqui tiramos $(\omega/s)^n + (a_1/s)(\omega/s)^{n-1} + \ldots + a_n/s^n = 0$ onde $a_i/s^i \in R_{\mathfrak{p}}$, logo, ω/s é inteiro sôbre $R_{\mathfrak{p}}$. (q.e.d.).

Lema 3 - Se R tiver um único ideal máximal $\mathfrak{p}$, existirá um ideal máximal $\mathfrak{p}'$ de R' cuja projeção sôbre R é $\mathfrak{p}$: $\mathfrak{p}' \cap R = \mathfrak{p}$.

Com efeito, pelo lema 1, R' não é um corpo, portanto, existe em R' pelo menos um ideal máximal $\mathfrak{p}'$. Evidentemente, temos $\mathfrak{p}' \cap R = \mathfrak{p}$. (q.e.d.).

Teorema 12 - Para todo ideal primo $\mathfrak{p}$ de R existe um ideal primo $\mathfrak{p}'$ de R' que se projeta em $\mathfrak{p}$.

Demonstração - Consideremos o conjunto $S = R - \mathfrak{p}$ e construamos os aneis de quocientes $R_{\mathfrak{p}}$ e R'_S. Seja $\mathfrak{P} = \mathfrak{p}.R_{\mathfrak{p}}$ o único ideal máximal de R (I,prop.28); temos $\mathfrak{P} \cap R = \mathfrak{p}$ (I, prop.27). Pelo lema 2 o anel R'_S depende inteiramente de $R_{\mathfrak{p}}$, portanto, pelo lema 3, existe um ideal máximal $\mathfrak{P}'$ de R'_S que se projeta em $\mathfrak{P}$: $\mathfrak{P}' \cap R_{\mathfrak{p}} = \mathfrak{P}$. Pondo $\mathfrak{p}' = \mathfrak{P}' \cap R'$, teremos $\mathfrak{p}' \cap R = \mathfrak{P}' \cap R \cap R' = \mathfrak{P}' \cap R = \mathfrak{P}' \cap R_{\mathfrak{p}} \cap R = \mathfrak{P} \cap R = \mathfrak{p}$ e, além disso, $\mathfrak{p}'$ é um ideal primo de R'. (q.e.d.).

No que se segue manteremos as mesmas hipóteses sôbre os aneis R e R'.

Teorema 13 - Sejam $\mathfrak{p}_1$ e $\mathfrak{p}_2$ dois ideais primos de R e suponhamos que $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Seja $\mathfrak{p}'_1$ um ideal primo de R' cuja projeção sôbre R é $\mathfrak{p}_1$. Então existe um ideal primo $\mathfrak{p}'_2$ de R' cuja projeção é $\mathfrak{p}_2$ e que contém pròpriamente o ideal $\mathfrak{p}'_1$.

Demonstração - Consideremos os aneis resíduos $R/\mathfrak{p}_1 = \bar{R}$ e $R'/\mathfrak{p}_1' = \bar{R}'$; podemos dizer que $\bar{R}$ é um sub-anel de $\bar{R}'$, pois, $\mathfrak{p}_1 = \mathfrak{p}_1' \cap R$. O anel $\bar{R}'$ depende inteiramente de $\bar{R}$ (observação dada logo a seguir do teorema 11). Seja $\bar{\mathfrak{p}}_2 = \mathfrak{p}_2/\mathfrak{p}_1$; pelo teorema 12 existe um ideal primo $\bar{\mathfrak{p}}_2'$ de $\bar{R}'$ tal que $\bar{\mathfrak{p}}_2' \cap \bar{R} = \bar{\mathfrak{p}}_2$ e é imediato que $\bar{\mathfrak{p}}_2' \neq (0)$. Seja $\mathfrak{p}_2'$ o ideal primo de R' tal que $\bar{\mathfrak{p}}_2' = \mathfrak{p}_2'/\mathfrak{p}_1'$; teremos $\mathfrak{p}_2' \supset \mathfrak{p}_1'$, $\mathfrak{p}_2' \neq \mathfrak{p}_1'$ e $\mathfrak{p}_2' \cap R = \mathfrak{p}_2$. Isto demonstra o teorema 13.

Teorema 14 - *Sejam $\mathfrak{p}_1'$ e $\mathfrak{p}_2'$ dois ideais primos de R' e suponhamos que $\mathfrak{p}_1' \subset \mathfrak{p}_2'$, $\mathfrak{p}_1' \neq \mathfrak{p}_2'$. Então temos $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$, onde $\mathfrak{p}_1 = \mathfrak{p}_1' \cap R$ e $\mathfrak{p}_2 = \mathfrak{p}_2' \cap R$.*

Demonstração - Só precisamos demonstrar que $\mathfrak{p}_1 \neq \mathfrak{p}_2$ pois já temos $\mathfrak{p}_1 \subset \mathfrak{p}_2$. Consideremos os aneis resíduos $\bar{R} = R/\mathfrak{p}_1$ e $\bar{R}' = R'/\mathfrak{p}_1'$; temos $\bar{R} \subset \bar{R}'$ e $\bar{R}'$ é inteiramente dependente de $\bar{R}$. Seja $\bar{\mathfrak{p}}_2' = \mathfrak{p}_2'/\mathfrak{p}_1'$ que, certamente, é um ideal primo não nulo. Se demonstrarmos que $\bar{\mathfrak{p}}_2' \cap \bar{R} \neq (0)$ resultará que $\mathfrak{p}_2' \cap R = \mathfrak{p}_2 \neq \mathfrak{p}_1$. Portanto, precisamos demonstrar, que se $\mathfrak{p}'$ for um ideal primo não nulo de um campo de integridade R' (que depende inteiramente de um seu sub-anel R) então $\mathfrak{p}' \cap R$ não é o ideal nulo de R. Ora, sendo $\mathfrak{p}' \neq (0)$ existe um elemento ω, $\omega \neq 0$, em $\mathfrak{p}'$. Temos $\omega^n + a_1 \omega^{n-1} + \ldots + a_n = 0$ $(a_i \in R)$ e podemos supôr que $a_n \neq 0$. Desta relação vem $a_n \in \mathfrak{p}' \cap R = \mathfrak{p}$, portanto, $\mathfrak{p} \neq (0)$. Isto completa a demonstração do teorema 14.

Corolário - *Seja $\mathfrak{p}$ um ideal primo mínimal de R e seja $\mathfrak{p}'$ um ideal primo de R' tal que $\mathfrak{p}' \cap R = \mathfrak{p}$. Então $\mathfrak{p}'$ é um ideal primo mínimal de R'.*

Definição 10 - *Seja R um anel e seja $\mathfrak{a}$ um ideal não unitário de R. Um ideal primo $\mathfrak{p}$ de R é denominado ideal primo isolado de $\mathfrak{a}$ se $\mathfrak{p}$ verificar as condições: 1) $\mathfrak{a} \subset \mathfrak{p}$ e 2) se $\mathfrak{a} \subset \mathfrak{p}_1 \subset \mathfrak{p}$ onde $\mathfrak{p}_1$ é um ideal primo de R então $\mathfrak{p}_1 = \mathfrak{p}$.*

E' imediato que quando R é um anel noetheriano, esta definição coincide com a definição dada no cap.I, p.5.

Lema 4 - Seja R um sub-anel (com elemento unidade) de um campo de integridade R' e suponhamos que R' dependa inteiramente de R. Então um ideal primo $\mathfrak{P}'$ de R' que se projeta num ideal primo isolado de $\mathfrak{a}$ (ideal de R) é um ideal primo isolado de $R'.\mathfrak{a}$.

Demonstração - Seja $\mathfrak{P} = \mathfrak{P}' \cap R$; temos $\mathfrak{a} \subset \mathfrak{P}$, logo, $\mathfrak{a} \subset \mathfrak{P}'$ e então $R'\mathfrak{a} \subset \mathfrak{P}'$ o que verifica a condição 1). Seja $\mathfrak{P}_1'$ um ideal primo de R' tal que $R'\mathfrak{a} \subset \mathfrak{P}_1' \subset \mathfrak{P}'$ e seja $\mathfrak{P}_1 = \mathfrak{P}_1' \cap R$. Teremos $\mathfrak{a} \subset \mathfrak{P}_1 \subset \mathfrak{P}$, logo, $\mathfrak{P}_1 = \mathfrak{P}$; então, pelo teorema 14, virá $\mathfrak{P}_1' = \mathfrak{P}'$, o que verifica a condição 2).

Não é válida, em geral, a recíproca do lema 4, isto é, podem existir ideais primos isolados de $R'\mathfrak{a}$ que não se projetam em ideais primos isolados de $\mathfrak{a}$ (ver [15], pp.320-321). Interessa-nos saber em que condições todo ideal primo isolado de $R'\mathfrak{a}$ se projeta num ideal primo isolado de $\mathfrak{a}$. A êste respeito demonstra-se o seguinte teorema ([15], pp.321-325):

Teorema 15 - Seja R um sub-anel (com elemento unidade) de um campo de integridade R' e suponhamos que R' dependa inteiramente de R. Ainda mais, suporemos que R seja inteiramente fechado e que R' seja um anel noetheriano. Nestas condições todo ideal primo isolado de $R'\mathfrak{a}$ (onde $\mathfrak{a}$ é um ideal de R, $\mathfrak{a} \neq R$) projeta-se num ideal primo isolado de $\mathfrak{a}$.

Teorema 16 - Seja R um sub-anel (com elemento unidade) de um campo de integridade noetheriano R'; suponhamos que R' seja inteiramente dependente de R e que R seja inteiramente fechado. Sejam $\mathfrak{P}_1$ e $\mathfrak{P}_2$ dois ideais primos

de R, com $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$; seja $\mathfrak{p}_2'$ um ideal primo de R' cuja projeção sôbre R é $\mathfrak{p}_2$. Nestas condições, existe um ideal primo $\mathfrak{p}_1'$ pròpriamente contido em $\mathfrak{p}_2'$, tal que $\mathfrak{p}_1' \cap R = \mathfrak{p}_1$.

Demonstração - Consideremos o ideal $R'.\mathfrak{p}_1$ que está pròpriamente contido em $\mathfrak{p}_2'$. Como R' é noetheriano, de $R'.\mathfrak{p}_1 \subset \mathfrak{p}_2'$ vem que $\mathfrak{p}_2'$ contém, pelo menos, um ideal primo isolado $\mathfrak{p}'$ de $R'\mathfrak{p}_1$. Pelo teorema 15, $\mathfrak{p}_1'$ se projeta num ideal primo isolado de $\mathfrak{p}_1$, portanto, $\mathfrak{p}_1'$ se projeta sôbre $\mathfrak{p}_1$: $\mathfrak{p}_1' \cap R = \mathfrak{p}_1$. (q.e.d.).

Do teorema anterior resulta, imediatamente, o

Corolário - Se $\mathfrak{p}'$ for um ideal primo mínimal de R' então a sua projeção $\mathfrak{p} = \mathfrak{p}' \cap R$ será um ideal primo mínimal de R.

Demonstraremos agora um resultado fundamental para a teoria da dimensão de variedades algébricas. E' o seguinte (ver [15], p.326)

Teorema 17 - Todo ideal primo mínimal de um campo finito de integridade $R = k[\xi_1, \ldots, \xi_n]$, de grau de transcendência r, tem dimensão r-1.

Demonstração - Pelo teorema de normalização de E. Noether, existem r elementos $x_1, \ldots, x_r$ em R tais que R depende inteiramente de $R_o = k[x_1, \ldots, x_r]$. Sendo gr.tr. $R/k = r$ resulta que R_o é um anel de polinômios de r indeterminadas $x_1, \ldots, x_r$ sôbre k e então R_o é inteiramente fechado. Seja $\mathfrak{p}$ um ideal primo mínimal de R e consideremos o ideal $\mathfrak{p}_o = \mathfrak{p} \cap R_o$. Pelo corolário do teorema 16, $\mathfrak{p}_o$ é um ideal primo mínimal de R_o, então $\dim._k \mathfrak{p}_o = r-1$ (teorema 6), portanto, pelo teorema 11, $\dim._k \mathfrak{p} = r-1$. (q.e.d.).

§ 4 - Teorema dos ideais principais e teorema de F. K. Schmidt.

Teorema dos ideais principais - *Os ideais primos de um ideal principal não unitário* $R.\omega$ $(\omega \neq 0)$, *onde* R *é um campo de integridade noetheriano e inteiramente fechado, são ideais primos mínimais de* R.

Demonstração - Seja $\mathfrak{p}$ um ideal primo de $R.\omega$. Consideremos o anel de quocientes $R_{\mathfrak{p}} = R'$ de R em relação a $S = R - \mathfrak{p}$; seja $\mathfrak{p}' = \mathfrak{p}.R_{\mathfrak{p}}$. O ideal $\mathfrak{p}'$ é o único ideal máximal de R' (I, prop.28); ainda mais, se $\mathfrak{q}$ indicar a componente primária de $R.\omega$ que pertence a $\mathfrak{p}$, teremos que a decomposição de $R'.\omega$ tem $\mathfrak{q}' = R'.\mathfrak{q}$ como componente primária e qualquer outro ideal primo de $R'.\omega$ está contido em $\mathfrak{p}'$. Se demonstrarmos que $\mathfrak{p}'$ é um ideal primo mínimal de $R'.\omega$ virá, imediatamente, que $\mathfrak{p} = \mathfrak{p}' \cap R$ é um ideal primo mínimal de $R.\omega$. Notando que R' é inteiramente fechado (pois R é inteiramente fechado), vemos que as hipóteses do teorema se transportam para o anel R', sendo que agora $\mathfrak{p}$ é um ideal máximal de $R'.\omega$. Portanto, podemos supôr, desde o início, que $\mathfrak{p}$ é um ideal primo máximal de $R.\omega$; temos que demonstrar que $\mathfrak{p}$ é um ideal primo mínimal de R. Consideremos o conjunto $\mathfrak{p}^{-1}$ de todos os elementos ω de Ω (corpo de quocientes de R) tais que $\omega\mathfrak{p} \subset R$. Demonstra-se (ver [15], p.328 ou [13], 2ª vol., p.99) que $\mathfrak{p}^{-1} \supset R$, $\mathfrak{p}^{-1} \neq R$ e também que $\mathfrak{p}.\mathfrak{p}^{-1} = R$. Seja agora $\mathfrak{p}_1$, $\mathfrak{p}_1 \neq (0)$, um ideal primo de R contido em $\mathfrak{p}$: $(0) \neq \mathfrak{p}_1 \subset \mathfrak{p}$; devemos demonstrar que $\mathfrak{p}_1 = \mathfrak{p}$. De $\mathfrak{p}_1 \subset \mathfrak{p}$ vem $\mathfrak{p}^{-1} \supset \mathfrak{p}_1^{-1}$, de onde, $\mathfrak{p}_1\mathfrak{p}^{-1} \subset \subset \mathfrak{p}_1\mathfrak{p}_1^{-1} \subset R$, logo, $\mathfrak{p}_1\mathfrak{p}^{-1} = \mathfrak{m}$ é um ideal de R. De $\mathfrak{p}_1\mathfrak{p}^{-1} = \mathfrak{m}$ tiramos $\mathfrak{m}\mathfrak{p} = \mathfrak{p}_1$. Se $\mathfrak{m} \subset \mathfrak{p}_1$ teríamos $\mathfrak{p}_1 \subset \mathfrak{p}_1\mathfrak{p} \subset \mathfrak{p}_1$, logo, $\mathfrak{p}_1\mathfrak{p} = \mathfrak{p}_1$ e deveríamos ter $\mathfrak{p}_1 = (0)$, ou, $\mathfrak{p} = (1)$, o que é absurdo; logo $\mathfrak{m} \not\subset \mathfrak{p}_1$. Existe então um elemento a de $\mathfrak{m}$ não pertencente a $\mathfrak{p}_1$; de $\mathfrak{m}\mathfrak{p} = \mathfrak{p}_1$, virá, $a\mathfrak{p} \subset \mathfrak{p}_1$, de onde concluimos que $\mathfrak{p} \subset \mathfrak{p}_1$ (pois $a \notin \mathfrak{p}_1$). Mas, por hipótese, tínhamos $\mathfrak{p}_1 \subset \mathfrak{p}$, logo, $\mathfrak{p}_1 = \mathfrak{p}$. (q.e.d.).

Corolário - Seja $R = k[\xi_1, \ldots, \xi_n]$ um campo finito de integridade inteiramente fechado. Então todo ideal primo de um ideal principal $R.\omega$ (onde $\omega \in R$, $\omega \neq 0$ e $R.\omega \neq R$) tem dimensão r-1 (onde r = gr.tr. R/k).

E' uma consequência imediata do teorema anterior e do teorema 17.

Teorema 19 - Os ideais primos isolados de um ideal principal não nnitário $R.\omega$, onde $R=k[\xi_1, \ldots, \xi_n]$ é um campo finito de integridade e $\omega \neq 0$, são ideais primos mínimais de R.

Demonstração - Seja $\bar{R}$ o fêcho inteiro de R em $\Omega = k(\xi_1, \ldots, \xi_n)$, corpo de quocientes de R. Pelo teorema de E. Noether existem r elementos $x_1, \ldots, x_r$ em R tais que R depende inteiramente de $k[x_1, \ldots, x_r] = R_o$. Então $\bar{R}$ é também o fêcho inteiro de R_o em Ω. Pelo teorema 10 resulta que $\bar{R}$ é um R_o-módulo finito, portanto, $\bar{R}$ é um campo finito de integridade sôbre k (e, então $\bar{R}$ é noetheriano); além disso, $\bar{R}$ é inteiramente fechado. Seja agora $\mathfrak{p}$ um ideal primo isolado de $R.\omega$ e consideremos o ideal $\bar{R}.\omega \neq \bar{R}$. Pelo teorema 12 existe um ideal primo $\bar{\mathfrak{p}}$ de $\bar{R}$ que se projeta em $\mathfrak{p}$: $\bar{\mathfrak{p}} \cap R = \mathfrak{p}$, portanto, $\bar{\mathfrak{p}}$ é um ideal primo isolado de $\bar{R}.\omega$ (teorema 15). Logo, pelo teorema dos ideais principais, $\bar{\mathfrak{p}}$ é um ideal primo mínimal de $\bar{R}$ e, então, dim. $\bar{\mathfrak{p}}$ = r-1. Mas dim. $\mathfrak{p}$ = dim. $\bar{\mathfrak{p}}$ (teorema 11), logo, $\mathfrak{p}$ é um ideal primo mínimal de R. (q.e.d.).

Lema 5 - Seja $R = k[\xi_1, \ldots, \xi_n]$ um campo finito de integridade de grau de transcendência $r > 0$. Sejam $\mathfrak{p}_s$ e $\mathfrak{p}_t$ dois ideais primos de R de dimensões s e t, respectivamente; suponhamos que $\mathfrak{p}_s \subset \mathfrak{p}_t$ e que $s > t+1$. Nestas condições existe um ideal primo $\mathfrak{p}_{s-1}$, de dimensão s-1, compreendido entre $\mathfrak{p}_s$ e $\mathfrak{p}_t$: $\mathfrak{p}_s \subset \mathfrak{p}_{s-1} \subset \mathfrak{p}_t$.

Com efeito, consideremos o campo finito de integri-

dade $\bar{R} = R/\mathfrak{p}_s$; seja τ o homomorfismo canônico de R sôbre $\bar{R}$ e seja $\tau\mathfrak{p}_t = \bar{\mathfrak{p}}_t \neq (0)$. Temos gr.tr. $\bar{R}/k = s$ e dim. $\bar{\mathfrak{p}}_t = t$. Tomemos um elemento $\bar{\omega}$, $\bar{\omega} \neq 0$, de $\bar{\mathfrak{p}}_t$ e consideremos o ideal principal $\bar{R}.\bar{\omega}$; temos $\bar{R}.\bar{\omega} \subset \bar{\mathfrak{p}}_t$, portanto, $\bar{\mathfrak{p}}_t$ conterá um ideal primo isolado $\bar{\mathfrak{p}}_{s-1}$ de $\bar{R}.\bar{\omega}$. Pelos teoremas 17 e 19 teremos dim. $\bar{\mathfrak{p}}_{s-1} = s-1$. Seja $\mathfrak{p}_{s-1} = \tau^{-1}(\bar{\mathfrak{p}}_{s-1})$, então de $(0) \subset \bar{\mathfrak{p}}_{s-1} \subset \bar{\mathfrak{p}}_t$ vem $\mathfrak{p}_s \subset \mathfrak{p}_{s-1} \subset \mathfrak{p}_t$, o que demonstra o lema 5.

Notando que todo ideal máximal de R tem dimensão zero (o que resulta do teorema 7, ou, então, é uma consequência imediata do teorema de normalização) e que todo ideal primo mínimal de R tem dimensão $r-1$ (teorema 19), podemos, pelo que foi demonstrado no lema 5, enunciar o teorema fundamental da teoria da dimensão ([5], p.43):

Teorema 20 - Seja $R = k[\xi_1, \ldots, \xi_n]$ um campo finito de integridade de grau de transcendência r. Então todo ideal máximal de R tem dimensão zero e todo ideal primo mínimal de R tem dimensão $r-1$. Ainda mais, se $\mathfrak{p}_s$ e $\mathfrak{p}_t$ forem dois ideais primos de R, com $\mathfrak{p}_s \subset \mathfrak{p}_t$ e dim. $\mathfrak{p}_s = s$ dim. $\mathfrak{p}_t = t$, então existe uma cadeia máxima de ideais primos compreendidos entre $\mathfrak{p}_s$ e $\mathfrak{p}_t$ e esta cadeia tem $s-t-1$ têrmos.

Teorema de F.K. Schmidt - Seja $R = k[\xi_1, \ldots, \xi_n]$ um campo finito de integridade de grau de transcendência r e consideremos um ideal $\mathfrak{a} = (\omega_1, \ldots, \omega_s)$ de R, onde $s \leq r$ e $\mathfrak{a} \neq R$. Nestas condições, todo ideal primo isolado de $\mathfrak{a}$ tem dimensão maior ou igual a $r-s$.

Demonstração - O teorema já está demonstrado para $s = 1$ (teorema 19); suponhamo-lo verdadeiro para ideais cujas bases têm $s-1$ geradores. Consideremos o ideal $\mathfrak{a}_1 = (\omega_1, \ldots, \omega_{s-1})$ e seja $\mathfrak{p}$ um ideal primo isolado de $\mathfrak{a}$. De $\mathfrak{p} \supset \mathfrak{a} \supset \mathfrak{a}_1$ resulta que $\mathfrak{p}$ contém, pelo menos, um ideal primo isolado $\mathfrak{p}_1$

de $\mathfrak{a}_1$. Temos dim. $\mathfrak{p}_1 \geq r-s+1$. Consideremos o anel resíduo $R/\mathfrak{p}_1 = \bar{R}$ e seja τ o homomorfismo canônico de R sôbre $\bar{R}$; teremos $\tau\,\mathfrak{a}_1 = (0)$, logo, $\tau\,\omega_i = 0$ $(i=1,\ldots,s-1)$ e $\tau\,\mathfrak{a} = \bar{\mathfrak{a}} = \bar{R}.\bar{\omega}_s \neq \bar{R}$. Se $\bar{\omega}_s = \tau\,\omega_s = 0$, virá, $\bar{\mathfrak{a}} = (0)$; mas, neste caso, teremos $\mathfrak{p}_1 = \mathfrak{p}$, portanto, dim. $\mathfrak{p}_1 \geq r-s+1 > r-s$, e o teorema está demonstrado. Se $\bar{\omega}_s \neq 0$, teremos, $\bar{\mathfrak{a}} = \bar{R}.\bar{\omega}_s$ e $\bar{\mathfrak{p}}$ será um ideal primo isolado de $\bar{R}.\bar{\omega}_s$, logo, dim. $\bar{\mathfrak{p}}$ = = gr. tr. $\bar{R}/k$ -1 = dim. $\mathfrak{p}_1 - 1 \geq r-s+1-1 = r-s$; mas dim. $\mathfrak{p}$ = = dim. $\bar{\mathfrak{p}}$, então, dim. $\mathfrak{p} \geq r-s$. Isto completa a demonstração do teorema de F.K.Schmidt.

CAPITULO IV.

Derivações.

§1 - Derivações de primeira ordem.

1.1 - Definições.

Sejam I e I' dois campos de integridade com $I \subset I'$ e suponhamos que I e I' tenham o mesmo elemento unidade 1.

Definição - Chama-se derivação de primeira ordem de I (ou, simplesmente, derivação de I) a uma aplicação D de I em I' tal que

a)- $D(x + y) = Dx + Dy$ $\quad (x,y \in I)$;

b)- $D(xy) = xDy + yDx$ $\quad (x,y \in I)$.

Para cada x de I o elemento Dx, de I', é denominado primeira derivada de x (ou, simplesmente, derivada de x) em relação à derivação D. Se Dx=0 para todo x de um sub-conjunto I_o de I então diremos que D é uma derivação sôbre I_o. Se D for uma derivação sôbre I então D será denominada derivação trivial de I. Os elementos c de I tais que Dc=0 são denominados constantes em relação à derivação D. E' imediata a proposição (ver [8], p.8):

1. Tôda derivação de I é uma derivação sôbre o campo de integridade primo de I; além disso, as constantes em relação à D formam um sub-anel I_o de I.

Temos também (ver [8], pp.9-10):

Teorema 1 - Seja D uma derivação de um campo de integridade I num corpo I' $(I \subset I')$. Então D pode ser prolongada, de um único modo, a uma derivação do corpo de quocientes de I, Q(I), em I'.

Seja k um corpo e consideremos o conjunto $\mathfrak{D}(k)$ de tôdas as derivações de k em k. Se $c \in k$, $D \in \mathfrak{D}(k)$, $D_1 \in \mathfrak{D}(k)$ e $D_2 \in \mathfrak{D}(k)$, então as aplicações:

$$cD: \quad x \in k \longrightarrow c.(Dx) \in k$$

e

$$D_1 + D_2: \quad x \in k \longrightarrow D_1x + D_2x \in k,$$

são derivações de k em k. Podemos assim definir sôbre $\mathfrak{D}(k)$ uma estrutura de espaço vectorial sôbre o corpo k; $\mathfrak{D}(k)$ é denominado <u>espaço vectorial das derivações de k</u>. Indicaremos por $\mathfrak{D}(k/k_o)$, onde k_o é um sub-conjunto de k, o sub-espaço de $\mathfrak{D}(k)$ formado por tôdas as derivações de k sôbre k_o.

1.2 - <u>Derivações do corpo de funções racionais</u>.

Seja $K = k(X_1,\ldots,X_n)$ um corpo de funções racionais de n indeterminadas sôbre k e consideremos os aneis $R_n = k[X_1,\ldots,X_n]$ e $R = R_n[u_1,\ldots,u_n]$, onde $u_1,\ldots,u_n$ são indeterminadas sôbre K. Para todo elemento $f(X_1,\ldots,X_n)$ de R_n consideremos o elemento $f(X_1+u_1,\ldots,X_n+u_n)$ de R; temos:

$$f(X_1+u_1,\ldots,X_n+u_n) = f(X_1,\ldots,X_n) + f_1(X_1,\ldots,X_n)u_1 +$$

$$+ \ldots + f_n(X_1,\ldots,X_n)u_n + F(u_1,\ldots,u_n),$$

onde $F(u_1,\ldots,u_n)$ é um polinômio em $u_1,\ldots,u_n$, com coeficientes em R e de grau não inferior a 2. Indicaremos por D_i $(1 \leq i \leq n)$ a aplicação: $f(X) \in R_n \longrightarrow f_i(X) \in R_n$. Obteremos assim n derivações de R_n em K e sôbre k; pelo teorema 1 estas derivações podem ser prolongadas (de modo único) a derivações de K, que ainda indicaremos pelas mesmas notações. As seguintes propriedades são imediatas:

1. $D_i c = 0$ para todo $c \in k$;
2. $D_i X_i = 1$ e $D_i X_j = 0$ $(j \neq i)$;
3. O corpo das constantes de D_i é $k(X_1,\ldots,X_{i-1},X_{i+1},\ldots,X_n)$.
4. Se uma derivação D de K em K satisfizer as condições 1., 2. e 3. então $D = D_i$.

Por causa da propriedade 2 é que dizemos que D_i é uma derivação em relação a X_i; também indicaremos D_i por $\frac{\partial}{\partial X_i}$ e a denominaremos <u>derivação parcial em relação a</u> X_i e sôbre k. Temos ([8], p.12):

2. dim. $\mathfrak{D}(K/k) = n$.

Seja K uma extensão de k e consideremos n elementos $x_1,\ldots,x_n$ de K. Para um elemento qualquer $f(x_1,\ldots,x_n)$ de K consideremos a função racional $f(X_1,\ldots,X_n)$; indicaremos por $\partial f/\partial x_i$ o resultado da substituição de X_i por x_i $(i=1,..,n)$ em $\partial f/\partial X_i$. Com esta notação podemos estabelecer a relação:

$$(1) \qquad Df(x_1,\ldots,x_n) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} Dx_i,$$

onde D é uma derivação de K sôbre k.

1.3 - Prolongamento de uma derivação.

Seja K uma extensão de um corpo k.

Definição 2 - Diremos que K é uma extensão transcendente separável de k se existir uma base de transcendência X de K sôbre k tal que K seja extensão algébrica separável de k(X). Neste caso X é denominado base de transcendência separadora de K sôbre k.

Definição 3 - Diremos que K é uma extensão finitamente gerada sôbre k se existir um número finito de elementos $x_1,\ldots,x_n$ de K tais que $K = k(x_1,\ldots,x_n)$. Neste caso temos gr.tr. $K/k = r \leq n$; se $r > 0$ diremos também que K é um corpo de funções algébricas de r variáveis sôbre k. Se K for também extensão transcendente separável de k, diremos que K é separàvelmente gerado sôbre k.

Seja K um corpo finitamente gerado sôbre k: $K = k(x_1,\ldots,x_n)$; consideremos o anel de polinômios $R_n = k[X_1,\ldots,X_n]$. Indicaremos por $\mathfrak{A}$ o conjunto de todos os polinômios f de R_n tais que $f(x_1,\ldots,x_n) = 0$. E' imediato que $\mathfrak{A}$ é um ideal primo de R_n. Seja D uma derivação de k; suponhamos que D possa ser prolongada a uma derivação D' de K (em K). A derivada de um polinômio $F(x) \in k[x]$ é dada por (aplicando a (1)): $D'F(x) = F^D(x) + \sum_{i=1}^{n} \frac{\partial F}{\partial x_i} D'x_i$, onde $F^D(x)$ é

o polinômio, em $x_1,\ldots,x_n$, obtido aplicando-se aos coeficientes de $F(x)$ a derivação D', ou seja, D. Notemos que se $F(X) \in \mathfrak{A}$ teremos $F^D(x) + \sum_{i=1}^{n} \frac{\partial F}{\partial x_i} D'x_i = 0$. Consideremos agora uma base $\{F_1(X),\ldots,F_s(X)\}$ de $\mathfrak{A}$. Demonstra-se o seguinte teorema (ver [14],p.12, ou, [8],pp.14-16):

Teorema 2 - A condição necessária e suficiente para que uma derivação D de k (em k) possa ser prolongada a uma derivação D' de $K = k(x_1,\ldots,x_n)$ (em K) é que o sistema linear nos $Y_1,\ldots,Y_n$:

$$F_i^D(x) + \sum_{j=1}^{n} \frac{\partial F_i}{\partial x_j} Y_j = 0 \quad (i=1,\ldots,s), \tag{2}$$

tenha solução. Além disso, se $\alpha_1,\ldots,\alpha_n$ for uma solução dêste sistema, então só existirá um único prolongamento D' de D a K tal que $D'x_i = \alpha_i$ $(i=1,\ldots,n)$.

Dêste teorema tiramos os seguintes corolários (ver [14],p.13, ou, [8],pp.16-18):

Corolário 1 - Seja $K = k(X)$ uma extensão transcendente simples de k, então tôda derivação D de k pode ser prolongada a uma derivação D' de K; ainda mais, se fixarmos o valor de $D'X$, D' será o único prolongamento de D a K.

Corolário 2 - Seja K uma extensão algébrica, separável e finita de k; então tôda derivação D de k pode ser prolongada, de um único modo, a uma derivação D' de K. Em particular, se $D = 0$ então $D' = 0$.

Corolário 3 - Seja $K = k(x)$ uma extensão algébrica puramente inseparável de k; indiquemos por $F(X) = X^{p^e} - a$ (p característica de k, $a \in k$) o polinômio irredutível de k. Nestas condições, uma derivação D de k pode ser prolongada a uma derivação D' de K quando, e sòmente quando, $Da = 0$. Em particular, se $D = 0$ só existe uma única derivação D' de K que é prolongamento de D e tal que $D'x = 1$.

Consideremos agora o caso em que D é a derivação trivial de k; o sistema (2) se reduz a

$$(3) \qquad \sum_{j=1}^{n} \frac{\partial F_i}{\partial x_j} Y_j = 0 \qquad (i=1,\ldots,s).$$

Indicaremos a matriz $\left\| \frac{\partial F_i}{\partial x_j} \right\|$ por M e por $n-\mu$ a sua característica. Então μ nos dá o número de soluções linearmente independentes (sôbre K) de (3), portanto, temos:

5. dim. $\mathfrak{D}(K/k) = \mu$.

Suponhamos agora que $\mu = 0$, neste caso, o sistema (3) só admite a solução trivial $Y_j = 0$ $(j=1,\ldots,n)$, isto nos mostra que a única derivação de $K = k(x_1,\ldots,x_n)$ sôbre k, é a derivação trivial de K. Podemos então afirmar que K é uma extensão algébrica separável de k. Com efeito, seja X uma base de transcendência de K sôbre k e seja K_o a maior extensão separável de $k(X)$ contida em K; temos $k \subset k(X) \subset K_o \subset K$. Se $K_o \neq K$ teríamos $K = K_o(z_1,\ldots,z_t)$, onde z_i é puramente inseparável sôbre K_o; consideremos o corpo $K' = K_o(z_2,\ldots,z_t)$. Temos $K = K'(z_1)$ e K é uma extensão puramente inseparável e simples de K'; pelo corolário 3 existe, então, uma derivação não trivial de K sôbre K', portanto, existe uma derivação não trivial de K sôbre k, o que é absurdo. Em consequência devemos ter $K_o = K$. Agora se $X \neq \emptyset$, existiria, pelo corolário 1, uma derivação não trivial de $k(X)$ sôbre k, que, pelo corolário 2, poderia ser prolongada a uma derivação (evidentemente não trivial) de K sôbre k. Temos assim um

absurdo, logo, $X = \emptyset$ e, portanto, K é extensão algébrica separável de k. Do que demonstrámos acima e pelo corolário 2, podemos enunciar os seguintes teoremas (ver [8], pp.20-21; [19], pp.26-29):

Teorema 3 - A condição necessária e suficiente para que $K = k(x_1,\ldots,x_n)$ seja uma extensão algébrica separável de k é que a única derivação de K sôbre k seja a derivação trivial de K.

Teorema 4 - A condição necessária e suficiente para que $K = k(x_1,\ldots,x_n)$ seja uma extensão algébrica separável de k, é que a matriz M tenha característica n.

Demonstraremos a proposição:

6. $\mu \geq r = \text{gr.tr. } K/k$.

Com efeito, por hipótese, existe em M um menor de ordem $n-\mu$ não nulo; usando uma notação conveniente podemos supôr que $\left|\frac{\partial F_i}{\partial x_j}\right| \neq 0$ $(i=1,\ldots,n-\mu$ e $j=\mu+1,\ldots,n)$. Pelo teorema 4 resulta que $x_{\mu+1},\ldots,x_n$ são algébricos sôbre $k(x_1,\ldots,x_\mu)$, portanto, $r \leq \mu$. (q.e.d.).

Teorema 5 - μ é o menor número de elementos $u_1,\ldots,u_\mu$ de K tais que K seja extensão algébrica e separável de $k(u_1,\ldots,u_\mu)$.

Demonstração - Seja $u_1,\ldots,u_t$ um sistema mínimo de elementos de K tais que K seja extensão algébrica e separável de $k(u_1,\ldots,u_t)$; então cada u_i ou é inseparável, ou, é transcendente sôbre k. Consideremos o corpo $k_i = k(u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_t)$; temos $k(u_1,\ldots,u_t) = k_i(u_i)$. Pelos corolários 1 e 3 existe uma derivação $\frac{\partial}{\partial u_i}$ de $k(u_1,\ldots,u_t)$ sôbre k tal que $\frac{\partial}{\partial u_i} u_i = 1$; esta derivação pode ser prolongada, de um único modo, a uma derivação de K (corolário 2) que ainda indicaremos por $\frac{\partial}{\partial u_i}$. E' fácil ver que as derivações $\frac{\partial}{\partial u_1},\ldots,\frac{\partial}{\partial u_t}$ são linearmente independentes sôbre K. Seja agora

D uma derivação de K sôbre k e ponhamos $Du_i = \alpha_i \in K$ $(i=1,\ldots,t)$. Nêste caso, a derivação $\bar{D} = D - \sum_{i=1}^{t} \alpha_i \frac{\partial}{\partial u_i}$ é uma derivação sôbre $k(u_1,\ldots,u_t)$, portanto, pelo corolário 2, $\bar{D} = 0$, logo, $D = \sum_{i=1}^{t} \alpha_i \frac{\partial}{\partial u_i}$. Isto nos mostra que dim. $\mathfrak{D}(K/k) = t$; mas por outro lado temos (prop.5) dim. $\mathfrak{D}(K/k) = \mu$, logo, $\mu = t$. (q.e.d.).

Teorema 6 - Seja $K = k(x_1,\ldots,x_n)$ uma extensão não separàvelmente gerada sôbre k. Então K é uma extensão μ-ésima de k (1) mas não é uma extensão $(\mu-1)$-ésima de k.

Demonstração - Pelo teorema anterior existe um sistema mínimo de μ elementos $u_1,\ldots,u_\mu$ tais que K seja extensão algébrica e separável de $k(u_1,\ldots,u_\mu) = K_o$. Como K não é separàvelmente gerado sôbre k teremos $\mu > r = gr.tr.\ K/k$, portanto, existe, pelo menos, um elemento u_i, p.ex., u_1, que é inseparável sôbre $k(u_2,\ldots,u_\mu) = k_1$. Pelo teorema do elemento primitivo (ver [13], vol.I, §40) existe um elemento ξ de K tal que $K = K_o(\xi)$, portanto, $K = k_1(u_1,\xi)$. Pela demonstração usual do teorema do elemento primitivo (ver [13], vol.I, §40) podemos substituir os elementos ξ e u_1 por um único elemento u_1' de K e então teremos $K = k_1(u_1') = k(u_1',u_2,\ldots,u_\mu)$. Isto prova que K é extensão μ-ésima de k; pelo teorema anterior K não pode ser extensão $(\mu-1)$-ésima de k. (q.e.d.).

Demonstraremos agora o teorema (ver [19], p.14, ou [8], p.22):

Teorema 7 - A condição necessária e suficiente para que $K = k(x_1,\ldots,x_n)$ seja uma extensão transcendente separável de k, é que a matriz M tenha característica n-r, onde r = gr.tr.K/k.

(1) Diremos que K é uma extensão μ-ésima de k quando existirem elementos $u_1,\ldots,u_\mu$ de K tais que $K = k(u_1,\ldots,u_\mu)$.

Com efeito, suponhamos que a matriz M tenha característica n-r. Pela demonstração da proposição 6, resultará que (usando uma notação conveniente) $x_{r+1},\ldots,x_n$ são algébricos separáveis sôbre $k(x_1,\ldots,x_r)$, portanto, $\{x_1,\ldots,x_r\}$ é uma base de transcendência separadora de K sôbre k. Isto demonstra a condição suficiente. Suponhamos agora que K seja uma extensão transcendente separável de k; então existem r elementos $u_1,\ldots,u_r$ de K tais que K seja uma extensão algébrica separável de $k(u_1,\ldots,u_r)$. Ainda mais, r é o menor número de elementos com esta propriedade, pois, gr.tr. K/k = r. Portanto, pela demonstração do teorema 5, temos $\mu = r$ e, então, a característica de M é n-r. (q.e.d.).

Teorema 8 - Se $K = k(x_1,\ldots,x_n)$ for uma extensão transcendente separàvelmente gerada sôbre k, então existirá uma base de transcendência separadora de K sôbre k entre os geradores $x_1,\ldots,x_n$.

E' uma consequência imediata da condição suficiente do teorema anterior e da demonstração da condição necessária do mesmo teorema.

O teorema 8 é devido a S.Mac-Lane (ver [7], p.384); em [8],p.36 e em [19],pp.18-19, podem ser encontradas outras demonstrações do teorema de Mac-Lane.

§2 - Derivações em relação aos elementos de uma p-base.

2.1 - Conjuntos p-independentes.

Seja k um corpo de característica $p > 0$ e consideremos uma extensão K de k. Daremos a seguinte definição (ver [7],p.376):

Definição 4 - Diremos que um sub-conjunto X de K é relativamente p-independente se tivermos $L(X') \neq L(X)$ (onde $L=k(K^p)$) para todo sub-conjunto próprio X' de X. Um sub-conjunto B de K é denominado p-base relativa (sôbre k) se B for relativamente p-independente e se $K = L(B)$.

Demonstram-se as seguintes proposições:

8. Tôda extensão K de k tem uma p-base relativa sôbre k.
9. Todo conjunto relativamente p-independente de K pode ser imerso numa p-base relativa de K sôbre k.
10. Tôdas as p-bases relativas de K têm a mesma potência.

Quando o número de elementos de uma p-base de K sôbre k for finito, êle é denominado grau de imperfeição relativo de K (sôbre k). Demonstra-se fàcilmente que $[K:L] = p^m$, onde $L = k(K^p)$ e m é o grau de imperfeição relativo de K.

Definição 5 - Diremos que um sub-conjunto X de um corpo K é p-independente (ou absolutamente p-independente) se para todo sub-conjunto próprio X' de X tivermos $K^p(X') \neq K^p(X)$. Um sub-conjunto B de K é denominado p-base de K se B for p-independente e se $K = K^p(B)$.

Estas definições coincidem com as anteriores no caso em que o corpo base k (da definição 4) é perfeito, pois temos $L = k(K^p) = k^p(K^p) = K^p$. Valem então as proposições 8, 9 e 10 para os conjuntos p-independentes. Em particular, se o número de elementos de uma p-base de K for finito então tôda p-base de K terá o mesmo número de elementos. Êste número é denominado grau de imperfeição (absoluto) de K. Demonstra-se que $[K:K^p] = p^m$, onde m é o grau de imperfeição de K.

2.2 - Derivações em relação aos elementos de uma p-base relativa.

Seja K uma extensão de um corpo k de característica $p > 0$ e consideremos uma p-base relativa $B = (z_\alpha)_{\alpha \in A}$ de K sôbre k. Para cada z_α temos $z_\alpha \notin L(B-\{z_\alpha\})$, $z_\alpha^p \in L(B-\{z_\alpha\})$ e $L(B-\{z_\alpha\})(z_\alpha) = L(B) = K$ (onde $L = k(K^p)$), portanto, pelo corolário 3, a derivação trivial de L pode ser prolongada (de um único modo) a uma derivação D_α de K tal que $D_\alpha z_\alpha = 1$. Eviden-

tenente temos $D_\alpha z_\beta = 0$ para $\beta \in A$, $\beta \neq \alpha$ e $D_\alpha c = 0$ para todo $c \in k$. Obtemos assim uma família $(D_\alpha)_{\alpha \in A}$ de derivações de K sôbre k e em relação aos elementos da p-base relativa B. Diremos que estas são as derivações em relação aos elementos da p-base relativa B. Observemos que para todo $x \in K$ temos $D_\alpha x = 0$ exceto para um número finito de índices α de A, portanto, tem sentido escrever $\sum_{\alpha \in \Lambda} D_\alpha x . a_\alpha$, onde $(a_\alpha)_{\alpha \in \Lambda}$ é uma família de elementos de K. Seja agora D uma derivação de K sôbre k; é imediato que D é então uma derivação de K sôbre $L=k(K^p)$. Ainda mais temos (Cfr. fórmula (1)): $Dx = \sum_{\alpha \in \Lambda} D_\alpha x . Dz_\alpha$, onde x é um elemento de K. Vemos assim que uma derivação D de K sôbre k fica determinada pelas derivações em relação aos elementos de uma p-base relativa de K sôbre k e pelos elementos Dz_α ($\alpha \in A$). Reciprocamente, seja $(a_\alpha)_{\alpha \in \Lambda}$ uma família de elementos de K e consideremos a aplicação D que a $x \in K$ faz corresponder o elemento $Dx = \sum_{\alpha \in \Lambda} D_\alpha x . a_\alpha$. E' fácil ver que D é uma derivação de K sôbre k (portanto, sôbre L).

O que dissemos acima também se aplica para o caso de uma p-base (absoluta) de K.

§ 3 - Aneis locais.

3.1 - Completação de um anel local.

Definição 6 - Diremos que $\mathfrak{o}$ é um anel local quando: a) $\mathfrak{o}$ é um anel noetheriano; b) $\mathfrak{o}$ tem elemento unidade; c) $\mathfrak{o}$ tem um único ideal máximal $\mathfrak{m}$. O corpo $\Delta = \mathfrak{o}/\mathfrak{m}$ é denominado corpo resíduo de $\mathfrak{o}$.

Consideremos, para cada inteiro r, $r \geq 1$, o anel $\mathfrak{M}_r = \mathfrak{m}^r/\mathfrak{m}^{r+1}$. Podemos considerar $\mathfrak{M}_r$ como um espaço vectorial sôbre Δ; para isto precisamos definir o produto de um elemento $\bar{\delta}$ de Δ por um elemento ω^* de $\mathfrak{M}_r$. Seja δ um elemento de $\mathfrak{o}$ tal que $\bar{\delta}$ = $\mathfrak{m}$-resíduo de δ e seja $\omega \in \mathfrak{m}^r$ tal que $\omega^* = \mathfrak{m}^{r+1}$-resíduo de ω; então, definiremos $\bar{\delta}\omega^*$ como a classe resídua, módulo $\mathfrak{m}^{r+1}$, determinada por $\delta\omega$. E' fácil veri-

ficar que esta definição não depende dos elementos δ e ω escolhidos nas classes $\overline{\delta}$ e ω^*, respectivamente; e, também, que $\mathfrak{M}_r$ passa a ser um espaço vectorial sôbre Δ. Temos o teorema (Cfr. [16], p.19):

Teorema 9 - A condição necessária e suficiente para que g elementos $\omega_1, \ldots, \omega_g$ formem uma base minimal de $\mathfrak{m}^r$ é que os correspondentes vectores $\omega_1^*, \ldots, \omega_g^*$ de $\mathfrak{M}_r$ formem uma base de $\mathfrak{M}_r$.

Demonstração - Seja $\{\omega_1, \ldots, \omega_g\}$ uma base mínimal de $\mathfrak{m}^r$ e suponhamos que os vectores $\omega_1^*, \ldots, \omega_g^*$ não sejam linearmente independentes sôbre Δ (é imediato que $\omega_1^*, \ldots, \omega_g^*$ geram $\mathfrak{M}_r$ sôbre Δ). Teremos, usando uma notação conveniente, uma relação da forma $\omega_1^* = \overline{\delta}_2 \omega_2^* + \ldots + \overline{\delta}_g \omega_g^*$; voltando ao anel $\mathfrak{m}^r$ virá $\omega_1 \equiv \delta_2 \omega_2 + \ldots + \delta_g \omega_g \pmod{\mathfrak{m}^{r+1}}$, portanto, $\mathfrak{m}^r = ((\omega_2, \ldots, \omega_g), \mathfrak{m}^{r+1})$. Seja $\Omega = \mathfrak{o}.(\omega_2, \ldots, \omega_g)$; temos $\mathfrak{m}^r = (\Omega, \mathfrak{m}^{r+1})$, de onde, $\mathfrak{m}^{r+1} = (\Omega, \mathfrak{m}^{r+1})\mathfrak{m} = (\Omega\mathfrak{m}, \mathfrak{m}^{r+2})$ e então $\mathfrak{m}^r = (\Omega, \Omega\mathfrak{m}, \mathfrak{m}^{r+2})$. Repetindo o mesmo processo obteremos $\mathfrak{m}^r = (\Omega, \mathfrak{m}^{r+j})$ para $j \geq 1$. Mas pelo teorema 18 do capítulo I, temos $\bigcap_{j=1}^{\infty} (\Omega, \mathfrak{m}^{r+j}) = \bigcap_{\ell=1}^{\infty} (\Omega, \mathfrak{m}^{\ell}) = \Omega$ e então $\Omega = \mathfrak{m}^r$, isto é, $\mathfrak{m}^r = (\omega_2, \ldots, \omega_g)$, contra a hipótese. Isto demonstra a condição necessária. Seja agora $\{\omega_1^*, \ldots, \omega_g^*\}$ uma base de $\mathfrak{M}_r$; então, para todo ω de $\mathfrak{m}^r$ temos uma relação da forma $\omega \equiv \delta_1 \omega_1 + \ldots + \delta_g \omega_g \pmod{\mathfrak{m}^{r+1}}$, de onde podemos concluir que $\mathfrak{m}^r = ((\omega_1, \ldots, \omega_g), \mathfrak{m}^{r+1})$. Pelo mesmo processo da demonstração anterior teremos $\mathfrak{m}^r = (\omega_1, \ldots, \omega_g)$. E' imediato que $\{\omega_1, \ldots, \omega_g\}$ é uma base mínimal de $\mathfrak{m}^r$ pois, caso contrário, $\omega_1^*, \ldots, \omega_g^*$ não seriam linearmente independentes sôbre Δ. Isto completa a demonstração do teorema 9.

Dêste teorema vêm os seguintes corolários:

Corolário 4 - O número de elementos de uma base mínimal de $\mathfrak{m}^r$ é igual à dimensão de $\mathfrak{M}_r$ sôbre Δ.

Corolário 5 - Tôdas as bases mínimais de $\mathfrak{m}^r$ têm o mesmo número de elementos.

Corolário 6 - Se $\varsigma_i = \sum_{j=1}^{g} a_{ij}\omega_j$ $(i=1,\ldots,g; a_{ij}\in\mathfrak{o})$ então $\varsigma_1,\ldots,\varsigma_g$ é uma base de $\mathfrak{m}^r$ quando, e sòmente quando, $|a_{ij}| \notin \mathfrak{m}$.

Os corolários 4 e 5 são imediatos. Vejamos o corolário 6. De $\varsigma_i = \sum_{j=1}^{g} a_{ij}\omega_j$ vem $\varsigma_i^* = \sum_{j=1}^{g} \bar{a}_{ij}\omega_j^*$, portanto, os vectores $\{\varsigma_1^*,\ldots,\varsigma_g^*\}$ serão linearmente independentes quando, e sòmente quando $|\bar{a}_{ij}| \neq 0$, ou seja, quando, e sòmente quando, $|a_{ij}| \notin \mathfrak{m}$. (q.e.d.).

Se $r = 1$, no corolário 4, teremos que a dimensão de $\mathfrak{M}_1$ nos dá o número de elementos de uma base mínimal de $\mathfrak{m}$; indicaremos êste número por s: dim. $\mathfrak{M}_1 = s$.

Introduziremos agora uma topologia (natural) sôbre o anel $\mathfrak{o}$ tomando $\mathfrak{m}^0 = \mathfrak{o}, \mathfrak{m}, \mathfrak{m}^2, \mathfrak{m}^3, \ldots$, como o sistema fundamental de vizinhanças da orígem. E' imediato que $\mathfrak{o}$ será, então, um anel topológico; como $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = (0)$ (ver cap.I, teorema 17) o espaço topológico $\mathfrak{o}$ é um espaço de Hausdorff. Podemos também definir u'a métrica sôbre $\mathfrak{o}$ do seguinte modo: se $x,y \in \mathfrak{o}$, $x \neq y$ então existe um expoente j tal que $x-y \in \mathfrak{m}^j$, $x-y \notin \mathfrak{m}^{j+1}$; neste caso poremos $d(x,y) = \rho^{-j}$ (onde ρ é um número real maior do que 1); ainda mais, se $x=y$ então poremos $d(x,y) = 0$. E' imediato que estão verificadas as condições: a) $d(x,y)=0 \longleftrightarrow x=y$; b) $d(x,y) = d(y,x)$; c) $d(x,y) \leq \max.(d(x,z),d(y,z))$; portanto, d é uma pseudo-métrica. Notemos que a topologia introduzida em $\mathfrak{o}$ por meio desta pseudo-métrica é equivalente à topologia natural de $\mathfrak{o}$.

Diremos que uma sucessão $(x_n)_{n\in N}$ (N conjunto dos números naturais) de elementos de $\mathfrak{o}$ é uma sucessão de Cauchy quando dado $\varepsilon>0$ e arbitrário existe um índice k tal que $d(x_m,x_n) < \varepsilon$ para todo $m > k$, $n > k$. Como d é uma pseudo-métrica temos: a condição necessária e suficiente para que (x_n) seja uma sucessão de Cauchy, é que $d(x_n,x_{n+1}) \longrightarrow 0$ quando $n \longrightarrow \infty$. Diremos que um anel local $\mathfrak{o}$ é completo se tôda su-

cessão de Cauchy for convergente. Num anel completo $\mathcal{O}$, a condição necessária e suficiente para que uma série $\sum_{n=0}^{\infty} x_n$ $(x_n \in \mathcal{O})$ seja convergente é que $x_n \longrightarrow 0$ quando $n \longrightarrow \infty$.

Sendo $\mathcal{O}$ um espaço métrico podemos passar ao espaço completo $\mathcal{O}^*$, em relação à métrica d e, também, podemos definir sôbre $\mathcal{O}^*$ uma estrutura de anel. Temos o seguinte teorema (ver [2], p.59):

Teorema 10 - Seja $\mathcal{O}$ um anel local e $\mathcal{O}^*$ o seu completo em relação à topologia natural de $\mathcal{O}$. Então: a) $\mathcal{O}^*$ é um anel topológico; b) $\mathcal{O}$ é um sub-espaço e um sub-anel de $\mathcal{O}^*$; c) se $\mathcal{O}_1^*$ satisfizer às condições a), b) e c) então $\mathcal{O}_1^*$ é isomorfo (sôbre $\mathcal{O}$) a $\mathcal{O}^*$.

« c) $\mathcal{O}$ é denso em $\mathcal{O}^*$;

O anel $\mathcal{O}^*$ é denominado anel completo do anel local $\mathcal{O}$, em relação à topologia natural de $\mathcal{O}$.

Demonstra-se o seguinte teorema (ver [2], pp.59-62):

Teorema 11 - Seja $\mathcal{O}^*$ o anel completo de um anel local $\mathcal{O}$. Então temos: a) $\mathcal{O}^*$ é um anel local e a topologia de $\mathcal{O}^*$ é equivalente à sua topologia natural; b) $m^* = \mathcal{O}^* m$ e $m^{*h} = \mathcal{O}^* . m^h$, $m^{*h} \cap \mathcal{O} = m^h$ $(h \in N)$; c) $\Delta = \mathcal{O}/m \cong \Delta^* = \mathcal{O}/m$; d) uma base mínimal de m é também uma base mínimal de m^*; e) se $\mathfrak{a}$ for um ideal qualquer de $\mathcal{O}$ então $\mathcal{O}^* \mathfrak{a} \cap \mathcal{O} = \mathfrak{a}$.

3.2 - Aneis locais regulares.

Seja $\mathcal{O}$ um anel local e consideremos o espaço vectorial $\mathfrak{M}_\nu$ sôbre $\Delta = \mathcal{O}/m$. Indicaremos por s a dimensão do espaço vectorial $\mathfrak{M}_1$, portanto, pelo corolário 4, o ideal m tem uma base mínimal $\{t_1, \ldots, t_s\}$ $(t_i \in \mathcal{O})$ com s elementos. Uma base de m^ν é dada pelos produtos $T_{(\alpha_1, \ldots, \alpha_s)} = t_1^{\alpha_1} \ldots t_s^{\alpha_s}$, onde $\alpha_1 + \ldots + \alpha_s = \nu$ e $\alpha_i \geqslant 0$, portanto, temos

$\dim. \mathfrak{M}_r \leq \binom{r+s-1}{r}$. Nesta relação só vale o sinal de igualdade se a base $T_{(\alpha)}$ de $\mathfrak{m}^r$ for mínimal; neste caso diremos que o anel local $\mathfrak{o}$ é regular. Precisamente, daremos a

Definição 7 - Diremos que um anel local $\mathfrak{o}$ é regular se $\dim. \mathfrak{M}_r = \binom{r+s-1}{r}$, onde $s = \dim. \mathfrak{M}_1$ e r é um número natural qualquer, $r \geq 1$.

Temos, imediatamente, que

11. Seja $\mathfrak{o}$ um anel local e seja $\varphi_r(t_1,\ldots,t_s) = \sum a_{(\alpha_1,\ldots,\alpha_s)} t_1^{\alpha_1} \ldots t_s^{\alpha_s}$ (onde $a_{(\alpha)} \in \mathfrak{o}$ e a somatória está extendida a tôdas as soluções inteiras não negativas da equação $\alpha_1 + \ldots + \alpha_s = r$) uma forma em $t_1,\ldots,t_s$ pertencente a $\mathfrak{m}^r$. Então o anel local $\mathfrak{o}$ é regular quando de $\sum a_{(\alpha)} t_1^{\alpha_1} \ldots t_s^{\alpha_s} \equiv 0 \ (\mathfrak{m}^{r+1})$ vem $a_{(\alpha)} \in \mathfrak{m}$, para tôda forma $\varphi_r(t_1,\ldots,t_s)$ de $\mathfrak{o}$ e para todo inteiro $r \geq 1$.

12. Uma condição suficiente para que um anel local seja regular é que de tôda relação da forma $\sum a_{(\alpha)} t_1^{\alpha_1} \ldots t_s^{\alpha_s} = 0$ venha $a_{(\alpha)} \in \mathfrak{m}$.

Do teorema 11, parte b), vem, imediatamente, que

13. O anel completo $\mathfrak{o}^*$ de um anel local regular é também um anel local regular.

Consideremos agora o anel de polinômios $\Delta[z_1,\ldots,z_s]$ onde $\Delta = \mathfrak{o}/\mathfrak{m}$; seja ς, $\varsigma \neq 0$, um elemento de $\mathfrak{o}$. Existe então um expoente r tal que $\varsigma \in \mathfrak{m}^r$, $\varsigma \notin \mathfrak{m}^{r+1}$, portanto, ς pode ser escrito sob a forma $\varsigma = \sum a_{(\alpha)} t_1^{\alpha_1} \ldots t_s^{\alpha_s}$. Ao elemento ς faremos corresponder a forma $\bar{\varsigma} = \sum \bar{a}_{(\alpha)} z_1^{\alpha_1} \ldots z_s^{\alpha_s}$ de $\Delta[z]$. E' imediato que $\bar{\varsigma} \neq 0$ pois nem todos os coeficientes $a_{(\alpha)}$ estão em $\mathfrak{m}$. Mostraremos que se $\mathfrak{o}$ for um anel local regular, então a forma $\bar{\varsigma}$ associada ao elemento ς é única. Com efeito, seja

$\zeta = \sum b_{(\alpha)} t_1^{\alpha_1} \ldots t_s^{\alpha_s}$ uma outra representação de ζ ; teremos $\sum [a_{(\alpha)} - b_{(\alpha)}] t_1^{\alpha_1} \ldots t_s^{\alpha_s} = 0$, portanto, pela proposição 8, $a_{(\alpha)} - b_{(\alpha)} \in \mathfrak{m}$, logo, $\bar{a}_{(\alpha)} = \bar{b}_{(\alpha)}$, como queríamos demonstrar. A forma $\bar{\zeta}$ correspondente ao elemento ζ é denominada <u>forma inicial</u> do elemento ζ . Sejam ζ e η dois elementos de $\mathfrak{o}$ e suponhamos que $\zeta \in \mathfrak{m}^{\mu}$, $\zeta \notin \mathfrak{m}^{\mu+1}$ e $\eta \in \mathfrak{m}^{\nu}$, $\eta \notin \mathfrak{m}^{\nu+1}$; d'aqui podemos concluir que $\zeta\eta \in \mathfrak{m}^{\mu+\nu}$, $\zeta\eta \notin \mathfrak{m}^{\mu+\nu+1}$ (pois $\mathfrak{o}$ é regular). Desta observação resultam as proposições:

14. <u>Todo anel local regular é um campo de integridade</u>.

15. $\overline{\zeta\eta} = \bar{\zeta}\bar{\eta}$, onde $\zeta \neq 0$ e $\eta \neq 0$.

Demonstraremos o teorema (cfr. [16], pp.34-37, ou, [2], pp.86-87):

<u>Teorema 12</u> - <u>Seja</u> $\mathfrak{o}$ <u>um anel local regular e seja</u> $\{t_1, \ldots, t_s\}$ <u>uma base mínimal de</u> $\mathfrak{m}$. <u>Então o ideal</u> $\mathfrak{p}_i = (t_1, \ldots, t_i)$ $(i \leq s)$ <u>é primo e</u> $\mathfrak{p}_i \subset \mathfrak{p}_{i+1}$, $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$.

<u>Demonstração</u> - A segunda parte do teorema é imediata pois $\{t_1, \ldots, t_s\}$ é uma base mínimal de $\mathfrak{m}$. Faremos a demonstração da primeira parte por indução sôbre i. Suponhamos que i=1 e consideremos o anel resíduo $\mathfrak{o}' = \mathfrak{o}/\mathfrak{p}_1$ que tem um único ideal máximal $\mathfrak{m}' = \mathfrak{o}'(t_2', \ldots, t_s') = \mathfrak{m}/\mathfrak{p}_1$, onde $t_j' = \tau t_j$ (j=2,..,s) e τ é o homomorfismo canônico de $\mathfrak{o}$ sôbre $\mathfrak{o}'$; notemos que $\{t_2', \ldots, t_s'\}$ é uma base mínimal de $\mathfrak{m}'$. Afirmamos que $\mathfrak{o}'$ é um anel local regular; d'aqui, pela proposição 11, resultará que $\mathfrak{p}_1$ é um ideal primo. Consideremos, então uma relação da forma $\sum a'_{(\alpha)} t_2'^{\alpha_2} \ldots t_s'^{\alpha_s} = 0$, onde $\sum_{i=2}^{s} \alpha_i = \nu$, $a'_{(\alpha)} \in \mathfrak{o}'$ e nem todos os $a'_{(\alpha)}$ são nulos; desta relação tiramos $\sum a_{(\alpha)} t_2^{\alpha_2} \ldots t_s^{\alpha_s} = a t_1$, onde $\tau a_{(\alpha)} = a'_{(\alpha)}$ e $a \in \mathfrak{o}$. O elemento a pertence exatamente a uma potência $\mathfrak{m}^h$ de $\mathfrak{m}$, isto é, $a \in \mathfrak{m}^h$, $a \notin \mathfrak{m}^{h+1}$. Se $h \geq \nu$, teremos, $a = \varphi_h(t_1, \ldots, t_s)$, portanto, $\sum a_{(\alpha)} t_2^{\alpha_2} \ldots t_s^{\alpha_s} - t_1 \varphi_h(t_1, \ldots, t_s) = 0$; mas $\mathfrak{o}$ é um anel local regular, logo,

devemos ter $a_{(\alpha)} \in \mathfrak{m}$ e, então, $a'_{(\alpha)} \in \mathfrak{m}'$. Provaremos que não podemos ter $h < r$, o que completará a demonstração do teorema para i=1. Se $h = r-1$, teríamos uma relação da forma $\sum a_{(\alpha)} t_2^{\alpha_2} \ldots t_s^{\alpha_s} - t_1 \varphi_{r-1}(t_1,\ldots,t_s) = 0$; d'aqui viria que todos os coeficientes da forma do primeiro membro estariam em $\mathfrak{m}$, o que não é possível, pois $a \in \mathfrak{m}^{r-1}$, $a \notin \mathfrak{m}^r$. Se $h < r-1$ teríamos $t_1 \varphi_h(t_1,\ldots,t_s) \in \mathfrak{m}^r$, em particular, $t_1 \varphi_h(t_1,\ldots,t_s) \in \mathfrak{m}^{h+2}$, portanto, todos os coeficientes de φ_h devem estar em $\mathfrak{m}$; logo, $a \in \mathfrak{m}^{h+1}$, contra a hipótese. Suponhamos agora que o teorema seja verdadeiro para i-1 e consideremos o ideal $\mathfrak{p}_i = \mathfrak{o}.(t_1,\ldots,t_i)$. No anel local regular $\mathfrak{o}' = \mathfrak{o}/\mathfrak{p}_1$ o ideal $\mathfrak{p}'_i = \tau\,\mathfrak{p}_i = \mathfrak{o}'.(t'_2,\ldots,t'_s)$ é primo, logo, o ideal $\mathfrak{p}_i = \bar{\tau}^{-1}\mathfrak{p}'_i$ é também um ideal primo. (q.e.d.).

Corolário 7 - Seja $\mathfrak{o}$ um anel local regular e sejam $u_1,\ldots,u_i$ $(i \leq s)$ i elementos de $\mathfrak{o}$. Se os vectores $u_1^*,\ldots,u_i^*$ de $\mathfrak{M}_1$ forem linearmente independentes sôbre Δ, então o ideal $\mathfrak{o}.(u_1,\ldots,u_i)$ será primo.

E' bastante notar que os vectores $u_1^*,\ldots,u_i^*$ sendo linearmente independentes sôbre Δ, fazem parte de uma base de $\mathfrak{M}_1$ sôbre Δ.

Corolário 8 - O anel resíduo $\mathfrak{o}/\mathfrak{p}_i$ é um anel local regular.

Com efeito, já sabemos que isto é verificado para i=1; suponhamos, então, que o corolário 8 seja verdadeiro para i-1 $(i > 1)$. Temos $\mathfrak{o}/\mathfrak{p}_i \cong (\mathfrak{o}/\mathfrak{p}_{i-1}) \big/ (\mathfrak{p}_i/\mathfrak{p}_{i-1})$, onde $\mathfrak{o}' = \mathfrak{o}/\mathfrak{p}_{i-1}$ é regular e $\mathfrak{p}_i/\mathfrak{p}_{i-1} = \mathfrak{o}'.(t'_i)$, portanto, $\mathfrak{o}/\mathfrak{p}_i$ é um anel local regular. (q.e.d.).

3.3 - Anel de séries de potências.

Seja $\mathfrak{R} = k[X_1,\ldots,X_n]$ um anel de polinômios de n indeterminadas $X_1,\ldots,X_n$ sôbre o corpo k e consideremos o ideal máximal $\mathfrak{m}_o = \mathfrak{R}.(X_1,\ldots,X_n)$. O anel de quocientes $\mathfrak{o} = \mathfrak{R}_{\mathfrak{m}_o}$ é noetheriano e tem um único ideal máximal $\mathfrak{m} = \mathfrak{o}.(X_1,\ldots,X_n)$, portanto, $\mathfrak{o}$ é um anel local. E' fácil provar que $\mathfrak{o}$ é um anel local regular. Seja $\mathfrak{o}^*$ o anel completo de $\mathfrak{o}$ em relação à topo-

logia natural de $\mathfrak{o}$; já sabemos que $\mathfrak{o}^*$ é um anel local com $\mathfrak{m}^* = \mathfrak{o}^*\mathfrak{m} = \mathfrak{o}^*.(X_1,\ldots,X_n)$ como único ideal máximal e, ainda mais, $\mathfrak{o}^*$ é um anel local regular (prop.13). Pela parte c) do teorema 11 temos $\mathfrak{o}/\mathfrak{m} \cong \mathfrak{o}^*/\mathfrak{m}^*$, mas $\mathfrak{o}/\mathfrak{m} \cong k$, portanto, os corpos resíduos de $\mathfrak{o}$ e de $\mathfrak{o}^*$ são isomorfos a k; no que se segue identificaremos $\mathfrak{o}/\mathfrak{m}$ e $\mathfrak{o}^*/\mathfrak{m}^*$ com o corpo k.

Lema 1 - Seja x^* um elemento de $\mathfrak{o}^*$; então existe para cada inteiro $r \geq 0$, um único conjunto de $r+1$ formas em $X_1,\ldots,X_n$: $\varphi_0(X),\ldots,\varphi_r(X)$, com coeficientes em k e de graus $0,1,\ldots,r$, respectivamente, tais que $x^* - \sum_{i=0}^{r} \varphi_i(X) \in \mathfrak{m}^{*r+1}$.

Demonstração - Faremos a demonstração por indução sôbre o número r. De $\mathfrak{o}^*/\mathfrak{m}^* = k$ tiramos $x^* \equiv \varphi_0 \pmod{\mathfrak{m}^*}$, onde $\varphi_0 \in k$, e é imediato que φ_0 é determinado de modo único; isto demonstra o lema para $r = 0$. Suponhamos que o lema seja verdadeiro para $r-1$ $(r \geq 1)$, portanto, existe um único conjunto de formas $\varphi_0(X), \varphi_1(X),\ldots,\varphi_{r-1}(X)$ (pertencentes a $\mathfrak{R}_0$ e de graus $0,1,\ldots, r-1$, respectivamente), tais que $x^* - \sum_{i=0}^{r-1} \varphi_i(X) \in \mathfrak{m}^{*r}$, logo, $x^* - \sum_{i=0}^{r-1} \varphi_i(X) = \Phi_r(X_1,\ldots,X_n)$, onde Φ_r é uma forma de grau r em $X_1,\ldots,X_n$ e com coeficientes em $\mathfrak{o}$: $\Phi_r(X_1,\ldots,X_n) = \sum a^*_{(\alpha)} X_1^{\alpha_1}\ldots X_n^{\alpha_n}$ $(a^*_{(\alpha)} \in \mathfrak{o}^*$ e a somatória está extendida a tôdas as soluções inteiras não negativas da equação $\alpha_1+\ldots+\alpha_n = r)$. Mas $a^*_{(\alpha)} \equiv a_{(\alpha)} \pmod{\mathfrak{m}^*}$, onde $a_{(\alpha)} \in k$, portanto, podemos escrever Φ_r sob a forma $\Phi_r(X) = \sum a_{(\alpha)} X_1^{\alpha_1}\ldots X_n^{\alpha_n} + \Phi_{r+1}(X)$, onde $\Phi_{r+1}(X) \in \mathfrak{m}^{*r+1}$. Indicando por $\varphi_r(X)$ a forma $\sum a_{(\alpha)} X_1^{\alpha_1}\ldots X_n^{\alpha_n}$, teremos $x^* - \sum_{i=0}^{r} \varphi_i(X) \in \mathfrak{m}^{*r+1}$. Falta demonstrar que (X) é determinada de modo único. Ora, se tivéssemos uma outra forma $\varphi'_r(X)$ (pertencente a $\mathfrak{m}^r$) tal que $x^* - \sum_{i=0}^{r-1} \varphi_i(X) - \varphi'_r(X) \in \mathfrak{m}^{*r+1}$, viria, $\varphi_r(X) - \varphi'_r(X) \in \mathfrak{m}^{*r+1}$ e, então, pela parte b) do teorema 11, $\varphi_r(X) - \varphi'_r(X) \in \mathfrak{m}^{r+1}$. Mas $\mathfrak{o}$ é um anel local regular, portanto, desta última relação tiramos $a_{(\alpha)} - a'_{(\alpha)} \in \mathfrak{m}$; como $a_{(\alpha)}$ e $a'_{(\alpha)}$

pertencem a k e $m \neq \sigma$ deveremos ter $a_{(\alpha)} = a'_{(\alpha)}$, isto é, $\varphi_r(X) = \varphi'_r(X)$. (q.e.d.).

Ponhamos $s_r = \varphi_0(X) + \varphi_1(X) + \ldots + \varphi_r(X)$, então a sucessão $(s_r)_{r\in N}$ (onde N é o conjunto dos números naturais) é uma sucessão de Cauchy e $\lim_{r\to\infty} s_r = x^*$. Portanto, o elemento x^* é a soma da série $\sum_{r=0}^{\infty} \varphi_r(X)$. E' imediato que tôda série da forma $\sum_{r=0}^{\infty} \varphi_r(X)$, onde $\varphi_r(X) \in \mathfrak{R}_0$ e $\varphi_r(X)$ é uma forma de grau r em $X_1,\ldots,X_n$ tem por soma um elemento x^* de σ^*. O anel σ^* é denominado <u>anel das séries de potências</u> em $X_1,\ldots,X_n$ e é indicado por $k\langle X_1,\ldots,X_n\rangle$. Observemos que dois elementos $\sum_{r=0}^{\infty} \varphi_r(X)$ e $\sum_{r=0}^{\infty} \varphi'_r(X)$ de σ^*, são iguais quando, e sòmente quando, $\varphi_r(X) = \varphi'_r(X)$ para todo $r \in N$. A soma e o produto de duas séries de potências $\sum_{r=0}^{\infty} \varphi_r(X)$ e $\sum_{r=0}^{\infty} \varphi'_r(X)$ de σ^*, são dados por $\sum_{r=0}^{\infty} \varphi_r(X) + \sum_{r=0}^{\infty} \varphi'_r(X) = \sum_{r=0}^{\infty} \left[\varphi_r(X) + \varphi'_r(X)\right]$ e $\sum_{r=0}^{\infty} \varphi_r(X) \cdot \sum_{r=0}^{\infty} \varphi'_r(X) = \sum_{r=0}^{\infty} \Phi_r(X)$, onde $\Phi_r(X) = \sum_{j=0}^{r} \varphi_j(X)\, \varphi'_{r-j}(X)$. Desta última relação resulta, imediatamente, que σ^* é um campo de integridade (o que também é consequência do fato que σ^* é um anel local regular).

<u>Teorema 13</u> - <u>Tôda série de potências</u> $x^* = \sum_{r=0}^{\infty} \varphi_r(X)$, <u>com</u> $\varphi_0(X) \neq 0$ <u>tem um único inverso em</u> σ^*.

<u>Demonstração</u> - Notemos incialmente que se existir o inverso de x^* êle é único pois σ^* é um campo de integridade. Seja $y^* = \sum_{r=0}^{\infty} \varphi'_r(X)$ um elemento de σ^*; y^* é inverso de x^* quando, e sòmente quando, estão verificadas as condições $\sum_{j=0}^{r} \varphi_j \varphi'_{r-j} = 0$, para todo $r > 0$, e $\varphi_0 \varphi'_0 = 1$. Estas equações determinam de modo único as formas $\varphi'_0(X), \varphi'_1(X), \ldots, \varphi'_r(X)$. Então se puzermos $y^* = \sum_{r=0}^{\infty} \varphi'_r(X)$, onde $\varphi'_r(X)$ verificam às condições acima, obteremos o inverso de x^*. (q.e.d.).

§ 4 - Derivações parciais.

Seja $K = k(X_1,\ldots,X_n)$ um corpo de funções racionais de n indeterminadas $X_1,\ldots,X_n$ sôbre o corpo k; consideremos o anel de polinômios $R = K[u_1,\ldots,u_n]$ de n indeterminadas $u_1,\ldots,u_n$ sôbre K. Seja $\mathfrak{o} = R_{\mathfrak{m}_o}$, onde $\mathfrak{m}_o = R.(u_1,\ldots,u_n)$; $\mathfrak{o}$ é um anel local regular com $\mathfrak{m} = \mathfrak{o}.\mathfrak{m}_o = \mathfrak{o}.(u_1,\ldots,u_n)$ como único ideal máximal. O anel completo $\mathfrak{o}^*$ de $\mathfrak{o}$ é o anel das séries de potências em $u_1,\ldots,u_n$, com coeficientes em K: $\mathfrak{o}^* = K\langle u_1,\ldots,u_n\rangle$. Seja $F(X) = f(X)/g(X)$, $f(X) \in k[X]$, $g(X) \in k[X]$, $g(X) \neq 0$, um elemento de K e consideremos o elemento $F(X+u) = f(X+u)/g(X+u)$. Como o têrmo independente de $u_1,\ldots,u_n$ em $g(X+u)$ é $g(X) \neq 0$, segue-se que $F(X+u) \in \mathfrak{o}$. Então o elemento $F(X+u)$ pode ser representado, de um único modo, como uma série de potências em $u_1,\ldots,u_n$ com coeficientes em K:

$$F(X+u) = F_0(u) + F_1(u) + \ldots + F_\nu(u) + \ldots, \tag{4}$$

onde $F_\nu(u)$ é uma forma de grau ν em $u_1,\ldots,u_n$ com coeficientes em K:

$$F_\nu(u) = \sum a_{(\alpha)} u_1^{\alpha_1}\ldots u_n^{\alpha_n},$$

sendo que $a_{(\alpha)} \in K$ e a somatória está extendida a tôdas as soluções (distintas) inteiras não negativas da equação $\alpha_1+\ldots+\alpha_n = \nu$. Observemos que $F(X+u) \equiv F(X) \pmod{\mathfrak{m}}$, portanto, teremos $F_0(u) = F(X)$. Diremos que (4) é o desenvolvimento em série do elemento $F(X)$. Notemos que se $F(X) \in k[X_1,\ldots,X_n]$ então o desenvolvimento em série de $F(X)$ é igual ao desenvolvimento do polinômio $F(X+u)$ em relação às potências crescentes de $u_1,\ldots,u_n$.

Podemos obter a série (4) aplicando o processo dado na demonstração do teorema 13 aos desenvolvimentos dos polinômios $f(X+u)$ e $g(X+u)$; vê-se, fàcilmente, que $F_\nu(u)$ pode então ser escrito do seguinte modo $F'_\nu(u)/[g(X)]^{\nu+1}$, onde $F'_\nu(u)$ é uma forma de grau ν em $u_1,\ldots,u_n$ e com coeficientes em $k[X]$.

Definição 8 - A aplicação D_i^{ν} $(1 \leq i \leq n,\ \nu \geq 1)$ que a cada elemento $F(X)$ de K faz corresponder o coeficiente $a_{(\alpha_1,\ldots,\alpha_n)}$ onde $\alpha_j = 0$ para $j \neq i$ e $\alpha_i = \nu$ do desenvolvimento em série de $F(X)$ é denominada derivação de ordem ν em relação a X_i e sôbre k.

Indicaremos por D_i^{0} a aplicação idêntica de K.

Teorema 14 - Sejam x e y dois elementos de K; então temos: a) $D_i^{\nu}(x+y) = D_i^{\nu}x + D_i^{\nu}y$, para $\nu \geq 0$; b) $D_i^{\nu}(xy) = \sum_{j=0}^{\nu} D_i^{j}x \cdot D_i^{\nu-j}y$ para $\nu \geq 0$; c) $D_i^{1}X_i = 1$, $D_i^{\nu}X_i = 0$ para $\nu > 1$; $D_i^{\nu}X_j = 0$ para $\nu \geq 1$ e $j \neq 1$; $D_i^{\nu}c = 0$, onde $c \in k$ e $\nu \geq 1$.

A demonstração é imediata. Por causa da propriedade c) é que dizemos que D_i^{ν} $(\nu \geq 1)$ é uma derivação em relação a X_i e sôbre k.

Teorema 15 - Seja $F(X)$ um elemento de K e consideremos o elemento $F(X_1+u_1,\ldots,X_\ell+u_\ell,X_{\ell+1},\ldots,X_n)$ (que também indicaremos por $F_{(\ell)}$) de $\mathfrak{S}$. Provaremos que a série de potências correspondente a $F_{(\ell)}$ só contém têrmos em $u_1,\ldots,u_\ell$: $F_{(\ell)} = \sum_{\nu=0}^{\infty} \bar{F}_\nu(u_1,\ldots,u_\ell)$, onde $\bar{F}_\nu(u_1,\ldots,u_\ell) = \sum \bar{a}_{(\alpha_1,\ldots,\alpha_\ell)} u_1^{\alpha_1}\ldots u_\ell^{\alpha_\ell}$, $\bar{a}_{(\alpha_1,\ldots,\alpha_\ell)} \in K$ e $\alpha_1+\ldots+\alpha_\ell = \nu$.

Ainda mais, se $F(X_1+u_1,\ldots,X_n+u_n) = \sum_{\nu=0}^{\infty} F_\nu(u_1,\ldots,u_n)$, onde $F_\nu(u_1,\ldots,u_n) = \sum a_{(\alpha)} u_1^{\alpha_1}\ldots u_n^{\alpha_n}$, $a_{(\alpha)} \in K$ e $\alpha_1+\ldots+\alpha_n = \nu$, então

$$\bar{a}_{(\alpha_1,\ldots,\alpha_\ell)} = a_{(\alpha_1,\ldots,\alpha_\ell,0,\ldots 0)}.$$

Demonstração - Seja $F(X) = f(X)/g(X)$, onde $f(X)$ e $g(X)$ pertencem ao anel $k[X_1,\ldots,X_n] = \mathfrak{R}$ e $g(X) \neq 0$. E' imediato que as séries correspondentes a $f_{(\ell)}$ e $g_{(\ell)}$ só contêm têrmos em $u_1,\ldots,u_\ell$. Isto demonstra a primeira parte do teorema. Seja $\mathfrak{p}_{n-\ell} = \mathfrak{O}.(u_{\ell+1},\ldots,u_n)$ que é um ideal primo de $\mathfrak{O}$ (teorema 12); para demonstrar a segunda parte do teorema basta provar que $F_\nu(u_1,\ldots,u_n) \equiv \bar{F}_\nu(u_1,\ldots,u_\ell) \pmod{\mathfrak{p}_{n-\ell}}$, pois $\mathfrak{O}/\mathfrak{p}_{n-\ell}$ é um anel local regular. Se $\nu = 0$ isto é imediato; suponhamos então que $F_j(u_1,\ldots,u_n) \equiv \bar{F}_j(u_1,\ldots,u_\ell) \pmod{\mathfrak{p}_{n-\ell}}$ para $j=0,1,\ldots,\nu-1$. Temos

$$F(X+u) - \sum_{j=0}^{\nu} F_j(u_1,\ldots,u_n) \in \mathfrak{m}^{\nu+1} \quad \text{e} \quad F_{(\ell)} - \sum_{j=0}^{\nu} \bar{F}_j(u_1,\ldots,u_\ell) \in \mathfrak{m}^{\nu+1},$$

portanto, $F(X+u) - F_{(\ell)} - \left(\sum_{j=0}^{\nu} F_j(u_1,\ldots,u_n) - \sum_{j=0}^{\nu} \bar{F}_j(u_1,\ldots,u_\ell)\right) =$

$= \sum b_{(\beta)} u_1^{\beta_1} \ldots u_n^{\beta_n}$, onde $b_{(\beta)} \in \mathfrak{O}$ e $\beta_1 + \ldots + \beta_n = \nu+1$. Tomando ambos os membros desta igualdade módulo $\mathfrak{p}_{n-\ell}$ virá

$$\sum \left[\bar{a}_{(\alpha_1,\ldots,\alpha_\ell)} - a_{(\alpha_1,\ldots,\alpha_\ell,0,\ldots,0)}\right] u_1'^{\alpha_1} \ldots u_\ell'^{\alpha_\ell} =$$

$$= \sum b'_{(\beta_1,\ldots,\beta_\ell,0,\ldots,0)} u_1'^{\beta_1} \ldots u_\ell'^{\beta_\ell}, \text{ onde } u_i' = \mathfrak{p}_{n-\ell}\text{-resíduo}$$

de u_i $(i=1,\ldots,\ell)$ e $b'_{(\beta_1,\ldots,\beta_\ell,0,\ldots,0)} = \mathfrak{p}_{n-\ell}$-resíduo de $b_{(\beta_1,\ldots,\beta_\ell,0,\ldots,0)}$. Mas $\mathfrak{O}/\mathfrak{p}_{n-\ell} = \mathfrak{O}'$ é um anel local regular, logo, $\bar{a}_{(\alpha_1,\ldots,\alpha_\ell)} - a_{(\alpha_1,\ldots,\alpha_\ell,0,\ldots,0)} \in \mathfrak{m}' = \mathfrak{m}/\mathfrak{p}_{n-\ell}$ e então $\bar{a}_{(\alpha_1,\ldots,\alpha_\ell)} = a_{(\alpha_1,\ldots,\alpha_\ell,0,\ldots,0)}$. Isto prova que

$\bar{F}_\nu(u_1,\ldots,u_\ell) \equiv F_\nu(u_1,\ldots,u_n) \pmod{\mathfrak{p}_{n-\ell}}$. (q.e.d.).

Corolário 9 - Seja $F(X_1,\ldots,X_n)$ um elemento de K, então temos $F(X_1,\ldots,X_{i-1},X_i+u_i,X_{i+1},\ldots,X_n) = \sum_{\nu=0}^{\infty} D_i^\nu F(X).u_i^\nu$.

Definição 9 - Um elemento x de K tal que $D_i^{\nu}x=0$ para $\nu=1,\ldots,\rho-1$ e $D_i^{\rho}x \neq 0$ é denominado constante de ordem ρ. Se $D_i^{\nu}x = 0$ para todo $\nu \geqslant 1$ então diremos que x é uma constante absoluta.

Do corolário 9 vem, imediatamente, que

Corolário 10 - O corpo $k(X_1,\ldots,X_{i-1},X_{i+1},\ldots,X_n)$ é o corpo das constantes absolutas das derivações D_i^{ν} $(\nu \geqslant 1)$.

Corolário 11 - O corpo $k(X_1^{p^e},\ldots,X_{i-1}^{p^e},X_{i+1}^{p^e},\ldots,X_n^{p^e})$, onde p é a característica de k, $p > 0$, e e é inteiro, $e \geqslant 1$, é o corpo das constantes de ordem pelo menos p^e das derivações D_i^{ν} $(\nu \geqslant 1)$.

Indicaremos por $D_1^{\alpha_1}\ldots D_{\ell}^{\alpha_{\ell}}$ $(1 \leqslant \ell \leqslant n)$ a aplicação composta de $D^{\alpha_{\ell}},\ldots,D_1^{\alpha_1}$ (nesta ordem), isto é, $D_1^{\alpha_1}D_2^{\alpha_2}\ldots D_{\ell}^{\alpha_{\ell}} = D_1^{\alpha_1} \circ D_2^{\alpha_2} \circ \ldots \circ D_{\ell}^{\alpha_{\ell}}$. Também indicaremos $D_i^{\alpha_i}$ por $\dfrac{\partial^{\alpha_i}}{\partial X_i^{\alpha_i}}$ e $D_1^{\alpha_1}\ldots D_{\ell}^{\alpha_{\ell}}$ por $\dfrac{\partial^{\alpha_1+\cdots+\alpha_{\ell}}}{\partial X_1^{\alpha_1}\ldots\partial X_{\ell}^{\alpha_{\ell}}}$. Estas aplicações compostas são denominadas derivações parciais de K, em relação às indeterminadas $X_1,\ldots,X_n$. Demonstraremos o

Teorema 16 - Se $F(X+u) = \sum_{\nu=0}^{\infty} F_{\nu}(u_1,\ldots,u_n)$ onde

$$F_{\nu}(u_1,\ldots,u_n) = \sum a_{(\alpha_1,\ldots,\alpha_n)} u_1^{\alpha_1}\ldots u_n^{\alpha_n},$$

$a_{(\alpha)} \in K$ e $\sum_{i=1}^{n} \alpha_i = \nu$, então

$$(D_1^{\alpha_1}\ldots D_{\ell}^{\alpha_{\ell}})F(X) = a_{(\alpha_1,\ldots,\alpha_{\ell},0,\ldots,0)}.$$

Demonstração - O corolário 9 nos mostra que o teorema é verdadeiro para $\ell = 1$; suponhamo-lo verdadeiro para $\ell - 1$ $(\ell > 1)$. Pelo teorema 15 e pela hipótese de indução temos

$$F(X_1,X_2+u_2,\ldots,X_{\ell}+u_{\ell},X_{\ell+1},\ldots,X_n) = \sum_{\nu=0}^{\infty} \bar{F}_{\nu}(u_2,\ldots,u_{\ell}), \text{ onde}$$

$$\bar{F}_{\nu}(u_2,\ldots,u_{\ell}) = \sum \bar{a}_{(\alpha_2,\ldots,\alpha_{\ell})} u_2^{\alpha_2}\ldots u_{\ell}^{\alpha_{\ell}},\ \bar{a}_{(\alpha_2,\ldots,\alpha_{\ell})} \in K,$$

$\alpha_2+\ldots+\alpha_\ell = \nu$ e $\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)} = (D_2^{\alpha_2}\ldots D_\ell^{\alpha_\ell})F(X)$. Temos

$$(5)\qquad F(X_1,X_2+u_2,\ldots,X_\ell+u_\ell,X_{\ell+1},\ldots,X_n) - \sum_{j=0}^{\nu}\bar{F}_j(u_2,\ldots,u_\ell) =$$

$$= \sum b_{(\beta)}u_1^{\beta_1}\ldots u_n^{\beta_n} \in \mathfrak{m}^{\nu+1},$$

onde $b_{(\beta)} \in \Theta$ e $\beta_1+\ldots+\beta_n = \nu+1$. Substituamos, nesta última relação, X_1 por X_1+u_1; no segundo membro ainda teremos um elemento de $\mathfrak{m}^{\nu+1}$. Pelo corolário 9 temos

$$\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}(X_1+u_1,X_2,\ldots,X_n) = \sum_{\mu=0}^{\infty} D_1^{\mu}\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}u_1^{\mu},$$

de onde vem

$$\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}(X_1+u_1,X_2,\ldots,X_n) - \sum_{\mu=0}^{\nu-j} D_1^{\mu}\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}u_1^{\mu} \in \mathfrak{m}^{\nu-j+1},$$

portanto,

$$\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}(X_1+u_1,X_2,\ldots,X_n)u_2^{\alpha_2}\ldots u_\ell^{\alpha_\ell} - \sum_{\mu=0}^{\nu-j} D_1^{\mu}\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}u_1^{\mu}u_2^{\alpha_2}\ldots u_\ell^{\alpha_\ell}$$

é um elemento de $\mathfrak{m}^{\nu+1}$ para $\alpha_2+\ldots+\alpha_\ell=j$. Levando êste resulado em (5), após a substituição de X_1 por X_1+u_1, virá:

$$F(X_1+u_1,\ldots,X_\ell+u_\ell,X_{\ell+1},\ldots,X_n) -$$

$$- \sum_{j=0}^{\nu}\sum_{\mu=0}^{\nu-j}\sum_{\alpha_2+\ldots+\alpha_\ell=j} D_1^{\mu}\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}u_1^{\mu}\ldots u_\ell^{\alpha_\ell} \in \mathfrak{m}^{\nu+1}$$

ou

$$F(X_1+u_1,\ldots,X_\ell+u_\ell,X_{\ell+1},\ldots,X_n) -$$

$$- \sum_{j=0}^{\nu}\Big(\sum_{\alpha_1+\ldots+\alpha_\ell=\nu} D_1^{\alpha_1}\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}u_1^{\alpha_1}\ldots u_\ell^{\alpha_\ell}\Big) \in \mathfrak{m}^{\nu+1},$$

portanto,

$$F(X_1+u_1,\ldots,X_\ell+u_\ell,X_{\ell+1},\ldots,X_n) = \sum_{\nu=0}^{\infty}\Big(\sum_{\alpha_1+\ldots+\alpha_\ell=\nu} D_1^{\alpha_1}\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)}u_1^{\alpha_1}\ldots u_\ell^{\alpha_\ell}\Big).$$

Aplicando o teorema 15 teremos $D_1^{\alpha_1}\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)} = a_{(\alpha_1,\ldots,\alpha_\ell,0,\ldots,0)}$; mas $\bar{a}_{(\alpha_2,\ldots,\alpha_\ell)} = (D_2^{\alpha_2}\ldots D_\ell^{\alpha_\ell})F(X)$, portanto

$$D_1^{\alpha_1}(D_2^{\alpha_2}\ldots D_\ell^{\alpha_\ell})F(X) = (D_1^{\alpha_1}\ldots D_\ell^{\alpha_\ell})F(X) = a_{(\alpha_1,\ldots,\alpha_\ell,0,\ldots,0)}.$$

(q.e.d.).

Corolário 12 - Seja $i_1,\ldots,i_n$ uma permutação dos números $1,2,\ldots,n$, então temos

$$D_{i_1}^{\alpha_{i_1}} \ldots D_{i_n}^{\alpha_{i_n}} = D_1^{\alpha_1} \ldots D_n^{\alpha_n}.$$

Demonstração - Basta provar que duas derivações quaisquer $D_i^{\alpha_i}$ e $D_j^{\alpha_j}$, com $i \neq j$, são permutáveis; para não dificultar as notações tomaremos $i=1$ e $j=2$. Pelo teorema 16 temos $(D_1^{\alpha_1} D_2^{\alpha_2})F(X) = a_{(\alpha_1,\alpha_2,0,\ldots,0)}$; agora, se considerássemos o elemento $F(X_1+u_1,X_2,\ldots,X_n)$ (ao envez de $F(X_1,X_2+u_2,X_3,\ldots,X_n)$ como foi feito na demonstração do teorema 15) teríamos $D_2^{\alpha_2}(D_1^{\alpha_1} F(X)) = a_{(\alpha_1,\alpha_2,0,\ldots,0)}$, portanto, $D_2^{\alpha_2} D_1^{\alpha_1} = D_1^{\alpha_1} D_2^{\alpha_2}$. (q.e.d.).

Após estas considerações poderemos escrever o desenvolvimento em série de um elemento $F(X)$ de K sob a forma

$$F(X+u) = F(X) + F_1(u) + \ldots + F_r(u) + \ldots, \tag{6}$$

onde

$$F_r(u_1,\ldots,u_n) = \sum_{\alpha_1+\ldots+\alpha_n=r} \frac{\partial^r F(X)}{\partial X_1^{\alpha_1} \ldots \partial X_n^{\alpha_n}} u_1^{\alpha_1} \ldots u_n^{\alpha_n}; \tag{7}$$

obtemos assim o chamado desenvolvimento de Taylor do elemento $F(X)$.

16. Se $f \in k[X_1,\ldots,X_n] = \mathfrak{R}$ então

$$\frac{\partial^r f}{\partial X_1^{\alpha_1} \ldots \partial X_n^{\alpha_n}} \in \mathfrak{R}, \text{ onde } r = \alpha_1+\ldots+\alpha_n.$$

Com efeito, o desenvolvimento em série de $f(X)$ coincide com o desenvolvimento segundo as potências crescentes de $u_1,\ldots,u_n$ do polinômio $f(X+u)$. A proposição 16 é então uma consequência imediata do desenvolvimento de Taylor.

17. Seja $\mathfrak{p}_0$ um ideal primo de $\mathfrak{R} = k[X_1,\ldots,X_n]$, $\mathfrak{p}_0 \neq \mathfrak{R}$ e consideremos o anel de quocientes $\mathfrak{o} = \mathfrak{R}_{\mathfrak{p}_0}$. Se $f \in \mathfrak{o}$ então $\frac{\partial^r f}{\partial X_1^{\alpha_1} \ldots \partial X_n^{\alpha_n}} \in \mathfrak{o}$ $(r = \alpha_1 + \ldots + \alpha_n)$.

Com efeito, de $f \in \mathfrak{o}$ vem $f = F/g$ onde $F \in \mathfrak{R}$, $g \in \mathfrak{R}$ e $g \notin \mathfrak{p}_0$. Pela observação dada antes da definição 6 te-

mos que o desenvolvimento em série de $f(X)$ é da forma

$$f(X+u) = f(X) + \frac{F_1(u)}{g^2} + \ldots + \frac{F_\nu(u)}{g^{\nu+1}} + \ldots,$$

onde $F_\nu(u)$ é uma forma de grau ν em $u_1,\ldots,u_n$ com coeficientes em $\mathfrak{o}$. A proposição 17 é então uma consequência imediata do desenvolvimento de Taylor.

18. Seja $f(X_1,\ldots,X_n) = f_0(X) + f_1(X) + \ldots + f_\nu(X)$ um polinômio de $\mathfrak{R} = k[X_1,\ldots,X_n]$, onde $f_j(X)$ $(j=0,\ldots,\nu)$ indica a componente homogênea de grau j de $f(X)$ e $f_\nu(X) \neq 0$ $(\nu \geq 1)$. Então nem tôdas as derivadas parciais de ordem ν do polinômio f são iguais a zero.

Com efeito, o desenvolvimento em série de $f(X)$ é da forma $f(X+u) = f(X) + F_1(u) + \ldots + F_\nu(u)$, onde $F_\nu(u) = f_\nu(u_1,\ldots,u_n) \neq 0$, portanto, nem tôdas as derivadas parciais de ordem ν de $f(X)$ são nulas. (q.e.d.).

19. Seja $\mathfrak{a}$ um ideal de $\mathfrak{R} = k[X_1,\ldots,X_n]$, $\mathfrak{a} \neq \mathfrak{R}$. Se $f \in \mathfrak{a}^{\rho+\nu}$ $(\rho \geq 1,\ \nu \geq 1)$ então

$$\frac{\partial^\nu f}{\partial X_1^{\alpha_1} \ldots \partial X_n^{\alpha_n}} \in \mathfrak{a}^\rho \text{, onde } \nu = \alpha_1 + \ldots + \alpha_n.$$

Demonstração - Em primeiro lugar demonstraremos que de $f \in \mathfrak{a}^{\rho+\nu}$ vem $\frac{\partial^\nu f}{\partial X_i^\nu} \in \mathfrak{a}^\rho$ $(1 \leq i \leq n)$. Suponhamos que $\nu = \rho = 1$. De $f \in \mathfrak{a}^2$ segue-se que $f = \sum_{j=1}^{s} f_j g_j$, onde $f_j \in \mathfrak{a}$ e $g_j \in \mathfrak{a}$, portanto $\frac{\partial f}{\partial X_i} = \sum_{j=1}^{s} (f_j \frac{\partial g_j}{\partial X_i} + g_j \frac{\partial f_j}{\partial X_i}) \in \mathfrak{a}$. Suponhamos agora que a propriedade seja verdadeira para $\rho = 1$ e para todo $\nu' \leq \nu - 1$. De $f \in \mathfrak{a}^{\nu+1} = \mathfrak{a} \cdot \mathfrak{a}^\nu$ segue-se que $f = \sum_{j=1}^{s} f_j g_j$, onde $f_j \in \mathfrak{a}$ e $g_j \in \mathfrak{a}^\nu$. D'aqui tiramos (pelo teorema 14):

$$\frac{\partial^\nu f}{\partial X_i^\nu} = \sum_{j=1}^{s} \Big(\sum_{m=0}^{\nu} \frac{\partial^m f_j}{\partial X_i^m} \frac{\partial^{\nu-m} g_j}{\partial X_i^{\nu-m}} \Big);$$

mas $\frac{\partial^{r-m} g_j}{\partial X_i^{r-m}} \in \mathfrak{o}$ para $1 \leq m \leq r$ e como também temos $f_j \frac{\partial^r g_j}{\partial X_i^r} \in \mathfrak{o}$, resultará $\frac{\partial^r f}{\partial X_i^r} \in \mathfrak{o}$. Suponhamos, finalmente, que a propriedade seja verdadeira para todo $r \geq 1$ e para todo $\rho' \leq \rho - 1$ $(\rho' \geq 1)$. Seja f um elemento de $\mathfrak{o}^{\rho+r} = \mathfrak{o}^{\rho-1+r} \cdot \mathfrak{o}$, portanto, $f = \sum_{j=1}^{s} f_j g_j$, $f_j \in \mathfrak{o}^{\rho-1+r}$ e $g_j \in \mathfrak{o}$. D'aqui tiramos

$\frac{\partial^r f}{\partial X_i^r} = \sum_{j=1}^{s} \left(\sum_{m=0}^{r} \frac{\partial^m f_j}{\partial X_i^m} \frac{\partial^{r-m} g_j}{\partial X_i^{r-m}} \right)$; mas, pela hipótese de indução, temos $\frac{\partial^m f_j}{\partial X_i^m} \in \mathfrak{o}$ para $1 \leq m \leq r$ e como $f_j \in \mathfrak{o}^{\rho-1+r}$ também temos $f_j \frac{\partial^r g_j}{\partial X_i^r} \in \mathfrak{o}^{\rho-1+r} \subset \mathfrak{o}^{\rho}$, logo, $\frac{\partial^r f}{\partial X_i^r} \in \mathfrak{o}^{\rho}$. Agora, se $f \in \mathfrak{o}^{\rho+r}$ e se $r = \alpha_1 + \ldots + \alpha_n$ teremos $\frac{\partial^{\alpha_1} f}{\partial X_1^{\alpha_1}} \in \mathfrak{o}^{\rho+r-\alpha_1}$; pelo corolário 12 virá $\frac{\partial^{\alpha_1+\alpha_2} f}{\partial X_1^{\alpha_1} \partial X_2^{\alpha_2}} \in \mathfrak{o}^{\rho+r-\alpha_1-\alpha_2}$. Assim por diante obteremos $\frac{\partial^r f}{\partial X_1^{\alpha_1} \ldots \partial X_n^{\alpha_n}} \in \mathfrak{o}^{\rho+r-\alpha_1-\ldots-\alpha_n} = \mathfrak{o}^{\rho}$. (q.e.d.).

20. Seja $\mathfrak{p}_0$ um ideal primo de $\mathfrak{R}_0$, $\mathfrak{p}_0 \neq \mathfrak{R}_0$, consideremos o anel de quocientes $\mathfrak{o} = \mathfrak{R}_{0\mathfrak{p}_0}$. Seja $\mathfrak{o}^*$ um ideal de $\mathfrak{o}$, $\mathfrak{o}^* \neq \mathfrak{o}$; então

$f \in \mathfrak{o}^{*\rho+r}$ $(\rho \geq 1,\ r \geq 1)$ vem $\frac{\partial^r f}{\partial X_1^{\alpha_1} \ldots \partial X_n^{\alpha_n}} \in \mathfrak{o}^{*\rho}$,

onde $r = \alpha_1 + \ldots + \alpha_n$.

A demonstração é análoga a da proposição 19.

§5 - Derivações parciais mistas.

5.1 - Derivações parciais de um corpo de funções racionais com infinitas indeterminadas.

Seja $K = k(X_\alpha)_{\alpha \in A}$ (onde A é um conjunto de índices, $A \neq \emptyset$) um corpo de funções racionais nas indeterminadas X_α. Consideremos um sub-conjunto finito A' de A e ponhamos

$A_1 = A - A'$, $K_1 = k(X_{\alpha_1})_{\alpha_1 \in A_1}$; então $K = K_1(X_{\alpha'})_{\alpha' \in A'}$, isto é, K é um corpo de funções racionais, com coeficientes em K_1, de um número finito de indeterminadas $X_{\alpha'}$ ($\alpha' \in A'$). No corpo K estão definidas as derivações $D_{\alpha'}^{\nu_{\alpha'}}$ ($\alpha' \in A'$) em relação às indeterminadas X_α; ainda mais, todo elemento de K_1 é uma constante absoluta em relação a estas derivações. E' imediato que a definição de $D_{\alpha'}^{\nu_{\alpha'}}$ não depende do sub-conjunto finito A' que contém o **índice** α'. Dêste modo, estão definidas em K as derivações $D_\alpha^{\nu_\alpha}$ ($\alpha \in A$) e também as compostas de um número finito delas. Observemos que um elemento x de K pertence a uma extensão K_0 de k, onde K_0 é obtido de k por meio da adjunção de um número finito de indeterminadas; portanto, temos $D_\alpha^{\nu_\alpha} x = 0$ ($\nu_\alpha \geq 1$) para todo α de A, exceto um número finito de índices α de A. Podemos então considerar o desenvolvimento de Taylor de um elemento qualquer x de K; obteremos as fórmulas (6) e (7), onde $X_1, \ldots, X_n$ são tôdas as indeterminadas que comparecem na expressão de x.

Indicaremos a aplicação composta das derivações $D_\alpha^{\nu_\alpha}$ ($\alpha \in A$), que satisfazem às condições: $\nu_\alpha \neq 0$ sòmente para um número finito de índices α de A, por $\prod_{\alpha \in A} D_\alpha^{\nu_\alpha}$.

5.2 - Derivações parciais mistas.

Seja k um corpo imperfeito de característica p, $p > 0$, e seja $Z = (z_\alpha)_{\alpha \in A}$ uma p-base de k. Consideremos o anel de polinômios $R = k^p[Y_\alpha]_{\alpha \in A}$ nas indeterminadas Y_α ($\alpha \in A$). Cada elemento z_α verifica uma relação da forma $z_\alpha^p - a_\alpha = 0$, onde $a_\alpha \in k^p$ e $a_\alpha \notin k^{p^2}$; portanto, cada polinômio $Y_\alpha^p - a_\alpha$ é irredutível sôbre k^p. Seja $\mathfrak{M} = R.(Y_\alpha^p - a_\alpha)_{\alpha \in A}$ o ideal de R gerado pelos polinômios $Y_\alpha^p - a_\alpha$.

21. O ideal $\mathfrak{M}$ é máximal.

Com efeito, seja $\bar{z}_\alpha$ = $\mathfrak{M}$-resíduo de Y_α; então é imediato que $\bar{z}_\alpha^p - a_\alpha = 0$, isto é, cada elemento $\bar{z}_\alpha$ é algébrico sôbre k^p. Como $R/\mathfrak{M} = k^p[\bar{z}_\alpha]_{\alpha \in A}$ resulta que $\mathfrak{M}$ é um ideal máximal, pois $k^p[\bar{z}_\alpha]_{\alpha \in A}$ é um corpo.

22. $R/\mathfrak{M} \cong k$.

Com efeito, estabelecemos acima a relação

$R/\mathfrak{N} = k^p(\bar{z}_\alpha)_{\alpha\in\Lambda}$ e é imediato que a aplicação

$\varphi : f(\bar{z}_\alpha)_{\alpha\in\Lambda} \longrightarrow f(z_\alpha)_{\alpha\in\Lambda}$ $(f \in R)$ é um isomorfismo de $R/\mathfrak{N}$ sôbre $k^p(z_\alpha)_{\alpha\in\Lambda} = k$.

No que se segue identificaremos os corpos $R/\mathfrak{N}$ e k.

Seja $K = k(X_1,\ldots,X_n)$ um corpo de funções racionais de n indeterminadas $X_1,\ldots,X_n$ sôbre k e consideremos o sub-corpo $K_o = k^p(X_1,\ldots,X_n)$. Seja $R = R_o[Y_\alpha]_{\alpha\in\Lambda}$, onde $(Y_\alpha)_{\alpha\in\Lambda}$ é uma família de indeterminadas sôbre K_o; temos $R \subset k^p(X_1,\ldots,X_n; (Y_\alpha)_{\alpha\in\Lambda}) = K'$. No corpo K' estão definidas as derivações $D_i^{\mu_i}$ e $D_\alpha^{\varsigma_\alpha}$ (sôbre k^p) em relação a X_i e a Y_α, respectivamente; além disso temos $D_i^{\mu_i} R \subset R$ e $D_\alpha^{\varsigma_\alpha} R \subset R$ $(i=1,\ldots,n; \alpha\in\Lambda)$, pela proposição 13. A proposição 22 nos mostra que $R/\mathfrak{N} = K$, onde $\mathfrak{N} = R.(Y_\alpha^p - a_\alpha)_{\alpha\in\Lambda}$.

Teorema 17 - Se $f \in \mathfrak{N}$ então $D_i^{\mu_i} f \in \mathfrak{N}$ $(i=1,\ldots,n)$ e $D_\alpha^{\varsigma_\alpha} f \in \mathfrak{N}$, para $0 \le \varsigma_\alpha \le p-1$ e $\alpha\in\Lambda$.

Com efeito, f é da forma $f = \sum_{\alpha\in\Lambda} \lambda_\alpha (Y_\alpha^p - a_\alpha)$, onde $\lambda_\alpha \in R$ e $\lambda_\alpha \neq 0$ sòmente para um número finito de índices α de Λ. D'aqui tiramos $D_i^{\mu_i} f = \sum_{\alpha\in\Lambda} \left(\sum_{m=o}^{\mu_i} D_i^m \lambda_\alpha D_i^{\mu_i - m}(Y_\alpha^p - a_\alpha)\right)$; mas $D_i^{\mu_i - m}(Y_\alpha^p - a_\alpha) = 0$ para $m < \mu_i$, portanto, $D_i^{\mu_i} f = \sum_{\alpha\in\Lambda} (D_i^{\mu_i} \lambda_\alpha)(Y_\alpha^p - a_\alpha) \in \mathfrak{N}$. Temos também: $D_\alpha^{\varsigma_\alpha} f = \sum_{\beta\in\Lambda} D_\alpha^{\varsigma_\alpha}\left[\lambda_\beta (Y_\beta^p - a_\beta)\right] = \sum_{\beta\in\Lambda} \left(\sum_{m=o}^{\varsigma_\alpha} D_\alpha^m \lambda_\beta D_\alpha^{\varsigma_\alpha - m}(Y_\beta^p - a_\beta)\right)$; mas $D_\alpha^{\varsigma_\alpha - m}(Y_\beta^p - a_\beta) = 0$ para $\beta \neq \alpha$ e $m < \varsigma_\alpha$, logo, $D_\alpha^{\varsigma_\alpha} f = \lambda_\alpha D_\alpha^{\varsigma_\alpha}(Y_\alpha^p - a_\alpha) + \sum_{\beta\in\Lambda} (D_\alpha^{\varsigma_\alpha} \lambda_\beta)(Y_\beta^p - a_\beta)$. Se $1 \le \varsigma_\alpha \le p-1$ temos $D_\alpha^{\varsigma_\alpha}(Y_\alpha^p - a_\alpha) = 0$, portanto, $D_\alpha^{\varsigma_\alpha} f = \sum_{\beta\in\Lambda} (D_\alpha^{\varsigma_\alpha} \lambda_\beta)(Y_\beta^p - a_\beta) \in \mathfrak{N}$.

Se $\varsigma_\alpha = 0$ o teorema 17 é imediato.

Observemos que a restrição $0 \le \varsigma_\alpha \le p-1$ é necessária pois, por exemplo, se $\varsigma_\alpha = p$ temos $Y_\alpha^p - a_\alpha \in \mathfrak{N}$ e, no en-

tretanto, $D_\alpha^p(Y_\alpha^p - a_\alpha) = 1 \notin \mathfrak{N}$; se $r_\alpha > p$ temos $Y_\alpha^{r_\alpha - p}(Y_\alpha^p - a_\alpha) \in \mathfrak{N}$ e, no entretanto, $D_\alpha^{r_\alpha}\left[Y_\alpha^{r_\alpha - p}(Y_\alpha^p - a_\alpha)\right] = 1 \notin \mathfrak{N}$.

Corolário 13 - Se $f \in \mathfrak{N}$ então $(D_1^{\mu_1} \dots D_n^{\mu_n})f \in \mathfrak{N}$ e $(\prod_{\alpha \in A} D_\alpha^{r_\alpha})f \in \mathfrak{N}$, onde $0 \leq r_\alpha \leq p-1$, e $r_\alpha \neq 0$ sòmente para um número finito de índices α.

Corolário 14 - Se $f \in \mathfrak{N}$ então $(\prod_{i;\alpha \in A} D_i^{\mu_i} D_\alpha^{r_\alpha})f \in \mathfrak{N}$, onde $1 \leq i \leq n$, e $r_\alpha \neq 0$ sòmente para um número finito de índices α de A.

Corolário 15 - Se $f \equiv g \pmod{\mathfrak{N}}$, $f \in R$ e $g \in R$, então $(\prod_{i;\alpha \in A} D_i^{\mu_i} D_\alpha^{r_\alpha})f \equiv (\prod_{i;\alpha \in A} D_i^{\mu_i} D_\alpha^{r_\alpha})g \pmod{\mathfrak{N}}$, onde $1 \leq i \leq n$, $0 \leq r_\alpha \leq p-1$ e $r_\alpha \neq 0$ sòmente para um número finito de índices α de A.

Êstes corolários são consequências imediatas do teorema 17.

Seja τ o homomorfismo canônico de R sôbre $R/\mathfrak{N} = K$; indicaremos por $\bar{x}$ a imágem por τ de um elemento x de R: $\bar{x} = \tau x$.

Definição 10 - $\bar{D}_i^{\mu_i}\bar{x} = \overline{D_i^{\mu_i}x}$ e $\bar{D}_\alpha^{r_\alpha}\bar{x} = \overline{D_\alpha^{r_\alpha}x}$ para $\bar{x} \in K$, $i=1,\dots,n$, $\alpha \in A$ e r_α vericando a condição $0 \leq r_\alpha \leq p-1$. A aplicação $\bar{D}_i^{\mu_i}$ $(i=1,\dots,n)$ é denominada derivação de ordem μ_i em relação a X_i (sôbre k); a aplicação $\bar{D}_\alpha^{r_\alpha}$ $(0 \leq r_\alpha \leq p-1)$ é denominada derivação de ordem r_α em relação a z_α (sôbre k^p).

E' fácil ver que estas aplicações $\bar{D}_i^{\mu_i}$ e $\bar{D}_\alpha^{r_\alpha}$ não dependem do elemento x de R tal que $\bar{x} = \tau x$; basta aplicar o

corolário 15.

Teorema 18 - Sejam $\bar{x}$ e $\bar{y}$ dois elementos de K. Temos: a) $\bar{D}_i^{\nu}(\bar{x}+\bar{y}) = \bar{D}_i^{\nu}\bar{x} + \bar{D}_i^{\nu}\bar{y}$ e $\bar{D}_\alpha^{\nu_\alpha}(\bar{x}+\bar{y}) = \bar{D}_\alpha^{\nu_\alpha}\bar{x} + \bar{D}_\alpha^{\nu_\alpha}\bar{y}$, onde $\nu \geq 0$ e $0 \leq \nu_\alpha \leq p-1$; b) $\bar{D}_i^{\nu}(\bar{x}\bar{y}) =$

$$= \sum_{j=0}^{\nu} \bar{D}_i^{j}\bar{x}.\bar{D}_i^{\nu-j}\bar{y} \quad \text{e} \quad \bar{D}_\alpha^{\nu_\alpha}(\bar{x}\,\bar{y}) =$$

$$= \sum_{j=0}^{\nu_\alpha} \bar{D}_\alpha^{j}\bar{x}.\bar{D}_\alpha^{\nu_\alpha-j}\bar{y}, \text{ onde } \nu \geq 0,$$

$i=1,\ldots,n$, $0 \leq \nu_\alpha \leq p-1$; c) $\bar{D}_i X_i = 1$, $\bar{D}_i^{\nu} X_i = 0$ para todo $\nu > 1$,

$\bar{D}_i^{\nu} X_j = 0$ para $j \neq i$ e $\nu \geq 1$;

$\bar{D}_i^{\nu} c = 0$ para todo $c \in k$ e $\nu \geq 1$;

$\bar{D}_\alpha^{\nu_\alpha} X_i = 0$ para $0 \leq \nu_\alpha \leq p-1$ e $\alpha \in \Lambda$,

$\bar{D}_\alpha z_\alpha = 1$, $\bar{D}_\alpha^{\nu_\alpha} z_\beta = 0$ para $\beta \in \Lambda$, $\beta \neq \alpha$ e $1 \leq \nu_\alpha \leq p-1$, $\bar{D}_\alpha^{\nu_\alpha} c = 0$ para todo $c \in k^p$ e $1 \leq \nu_\alpha \leq p-1$.

Estas propriedades resultam, imediatamente, da definição 10 e do teorema 14.

Observemos que a derivação $\bar{D}_i^{\nu}$ se comporta do mesmo modo que a derivação D_i^{ν}; por êste motivo indicaremos $\bar{D}_i^{\nu}$ por D_i^{ν}. Por causa da propriedade c) é que dizemos que D_i^{ν} é uma derivação em relação a X_i e sôbre k e que $\bar{D}_\alpha^{\nu_\alpha}$ ($1 \leq \nu_\alpha \leq p-1$, $\alpha \in \Lambda$) é uma derivação em relação a z_α e sôbre k^p.

Do corolário 10, vem

Corolário 16 - $D_i^{\nu} x = 0$ para todo $\nu \geq 1$ e i fixo quando, e sòmente quando, $x \in k(X_1,\ldots,X_{i-1},X_{i+1},\ldots,X_n)$;

$D_\alpha^{\nu_\alpha} x = 0$ ($\alpha \in \Lambda$, α fixo) para todo $\nu_\alpha \geq 1$ e $\nu_\alpha \leq p-1$ quando, e sòmente quando, $x \in k^p(Z-\{z_\alpha\};X_1,\ldots,X_n)$.

Podemos considerar em R a aplicação composta de um número finito de derivações $\bar{D}_{\alpha_1}^{\nu_{\alpha_1}},\ldots,\bar{D}_{\alpha_s}^{\nu_{\alpha_s}},D_1^{\mu_1},\ldots,D_n^{\mu_n}$ (onde $\alpha_j \neq \alpha_\ell$ para $j \neq \ell$). Pelos corolários 12 e 15 e pela definição 10 resulta que estas derivações são permutáveis. Podemos então usar a notação $\prod_{i;\alpha\in\Lambda} D_i^{\mu_i}\bar{D}_\alpha^{\nu_\alpha}$, onde $i=1,\ldots,n$, $0 \leq \nu_\alpha \leq p-1$ e $\nu_\alpha \neq 0$ sòmente para um número finito de índices α de Λ, $\mu_i \geq 0$, para a aplicação composta das aplicações $\bar{D}_\alpha^{\nu_\alpha}$ e $D_i^{\mu_i}$. A aplicação $\prod_{i;\alpha\in\Lambda} D_i^{\mu_i}\bar{D}_\alpha^{\nu_\alpha}$ é denominada <u>derivação parcial mista</u>. Pelo corolário 15 temos

23. $(\prod_{i;\alpha\in\Lambda} D_i^{\mu_i}\bar{D}_\alpha^{\nu_\alpha})\bar{x} = \overline{(\prod_{i;\alpha\in\Lambda} D_i^{\mu_i}D_\alpha^{\nu_\alpha})x}$, <u>onde</u> x <u>é tal que</u> $\tau x = \bar{x}$.

Daremos agora o desenvolvimento de Taylor de um elemento $\bar{x}$ de $K = k^p(X_1,\ldots,X_n;(z_\alpha)_{\alpha\in\Lambda})$. O elemento $\bar{x}$ pertence a uma extensão K_o' de $K_o = k^p(X_1,\ldots,X_n)$ que é gerada sôbre K_o por um número finito de elementos z_α; usando uma notação conveniente teremos $\bar{x} \in K_o' = K_o(z_1,\ldots,z_m) = k^p(X_1,\ldots,X_n;z_1,\ldots,z_m)$. Como K_o' é uma extensão algébrica de K_o segue-se que o elemento $\bar{x}$ pode ser escrito de um único modo como um polinômio em $z_1,\ldots,z_m$, com coeficientes em K_o e cada z_j comparece com expoentes no máximo iguais a $p-1$; indicaremos tal representação de $\bar{x}$ por $f(X_1,\ldots,X_n;z_1,\ldots,z_m)$. Consideremos o polinômio $f(X_1,\ldots,X_n;Y_1,\ldots,Y_m)$ em $Y_1,\ldots,Y_m$ com coeficientes em K_o; cada indeterminada Y_j comparece com expoentes no máximo iguais a $p-1$. Seja $K_1\langle u_1,\ldots,u_n;w_1,\ldots,w_m\rangle$ o anel de série de potências nas indeterminadas $u_1,\ldots,u_n,w_1,\ldots,w_m$ sôbre $K_1 = k^p(X_1,\ldots,X_n;Y_1,\ldots,Y_m)$. O desenvolvimento em série de $f(X_1,\ldots,X_n;Y_1,\ldots,Y_m)$ será da forma

(8) $f(X+u;Y+w) = f(X;Y) + f_1(u;w) + \ldots + f_\nu(u;w) + \ldots$

onde $f_\nu(u;w)$ é uma forma de grau ν em $u_1,\ldots,u_n,w_1,\ldots,w_m$ com coeficientes em $k^p(X)[Y]$:

$$f_\nu(u;w) = \sum a_{(\mu_1,\ldots,\mu_n;\nu_1,\ldots,\nu_m)} u_1^{\mu_1}\ldots u_n^{\mu_n} w_1^{\nu_1}\ldots w_m^{\nu_m}$$

sendo que a somatória está extendida a tôdas as soluções inteiras não negativas da equação $\mu_1 + \ldots + \mu_n + \nu_1 + \ldots + \nu_m = \nu$ tais que $0 \leq \nu_j \leq p-1$ para $j=1,\ldots,m$. Pelo teorema 16 temos

$$a_{(\mu_1,\ldots,\mu_n;\nu_1,\ldots,\nu_m)} = (D_1^{\mu_1}\ldots D_n^{\mu_n} D_{Y_1}^{\nu_1}\ldots D_{Y_m}^{\nu_m}) f(X;Y).$$

Tomando ambos os membros desta igualdade módulo $\mathfrak{A}$ teremos:

$$\bar{a}_{(\mu;\nu)} = (D_1^{\mu_1}\ldots D_n^{\mu_n} \bar{D}_1^{\nu_1}\ldots \bar{D}_m^{\nu_m}) f(X;z).$$

Fazendo o mesmo para todos os coeficientes de (8), e observando que o primeiro membro ficará $f(X+u;z+w)$, teremos:

$$(9) \qquad f(X+u;z+w) = f(X;z) + \bar{f}_1(u;w) + \ldots + \bar{f}_\nu(u;w) + \ldots$$

onde

$$(10) \qquad f_\nu(u;w) = \sum_{\substack{\mu_1+\ldots+\mu_n+\nu_1+\ldots+\nu_m=\nu \\ 0\leq\nu_j\leq p-1}} D_1^{\mu_1}\ldots D_n^{\mu_n} \bar{D}_1^{\nu_1}\ldots \bar{D}_m^{\nu_m} f(X;z) u_1^{\mu_1}\ldots u_n^{\mu_n} w_1^{\nu_1}\ldots w_m^{\nu_m}.$$

Diremos que (9), com as relações (10), é o <u>desenvolvimento de Taylor</u> do elemento $f(X;z)$.

24. <u>Se</u> $f \in \mathfrak{R} = k[X_1,\ldots,X_n] = k^p[X_1,\ldots,X_n;(z_\alpha)_{\alpha\in\Lambda}]$ <u>então</u> $(\prod_{i;\alpha\in\Lambda} D_i^{\mu_i} \bar{D}_\alpha^{\nu_\alpha}) f \in \mathfrak{R}$, <u>onde</u> $\mu_i \geq 0$, $0 \leq \nu_\alpha \leq p-1$ <u>e</u> $\nu_\alpha \neq 0$ <u>sòmente para um número finito de índices</u> α.

Com efeito, sejam $\bar{D}_1^{\nu_1},\ldots,\bar{D}_m^{\nu_m}$ as derivações que comparecem em $\prod_{i;\alpha\in\Lambda} D_i^{\mu_i} \bar{D}_\alpha^{\nu_\alpha}$ com expoentes $\nu_\alpha \neq 0$. O desenvolvimento em série do polinômio f coincide com o desenvolvimento do polinômio $f(X+u;z+w)$ em relação às potências crescentes de u e w. A proposição 24 é então uma consequência imediata do desenvolvimento de Taylor.

25. <u>Seja</u> $\mathfrak{p}_0$ <u>um ideal primo de</u> $\mathfrak{R} = k[X_1,\ldots,X_n]$ $\mathfrak{p}_0 \neq \mathfrak{R}$ <u>e consideremos o anel de quocientes</u> $\mathfrak{O} = \mathfrak{R}_{\mathfrak{p}_0}$. <u>Então se</u> $f \in \mathfrak{O}$, <u>teremos</u> $(\prod_{i;\alpha\in\Lambda} D_i^{\mu_i} \bar{D}_\alpha^{\nu_\alpha}) f \in \mathfrak{O}$, <u>onde</u> $\mu_i \geq 0$ $(i=1,\ldots,n)$, $0 \leq \nu_\alpha \leq p-1$ <u>e</u> $\nu_\alpha \neq 0$ <u>sòmente para um número finito de índices</u> α <u>de</u> Λ.

Demonstração - Se $\nu_\alpha = 0$ para todo $\alpha \in \Lambda$ a proposição já foi demonstrada (prop.14), pois $D_1^{\mu_1} \ldots D_n^{\mu_n} f \in \mathfrak{o}$. Precisamos sòmente demonstrar que se $f \notin \mathfrak{o}$ então $\bar{D}_\alpha^{\nu_\alpha} f \in \mathfrak{o}$ para $1 \leq \nu_\alpha \leq p-1$. Ora f é da forma $f = F/g$ onde $F \in \mathfrak{R}$, $g \in \mathfrak{R}$ e $g \notin \mathfrak{p}_o$; podemos supôr que todos os coeficientes de g pertençam a k^p, pois, caso contrário, multiplicaríamos ambos os têrmos de F/g por g^{p-1}. Portanto, f pode ser escrito como um polinômio em $z_1, \ldots, z_m$ cujos coeficientes são frações da forma f_j/g, onde $f_j \in k^p[X_1, \ldots, X_n]$, $g \in k^p[X_1, \ldots, X_n]$ e $g \notin \mathfrak{p}_o$. A proposição 26 é então uma consequência imediata do teorema 17.

26. *Seja* $\mathfrak{A}$ *um ideal de* $\mathfrak{R} = k[X_1, \ldots, X_n]$. *Se* $f \in \mathfrak{A}^{\rho+\nu}$, *onde* $\rho \geq 1$, $\nu \geq 1$, *então* $\left(\prod_{i;\alpha \in \Lambda} D_i \bar{D} \right) f \in \mathfrak{A}^{\rho}$, *onde* $\mu_i \geq 0$, $0 \leq \nu_\alpha \leq p-1$, $\nu_\alpha \neq 0$ *sòmente para um número finito de índices* α *de* Λ *e* $\mu_1 + \ldots + \mu_n + \sum_{\alpha \in \Lambda} \nu_\alpha = \nu$.

Esta proposição se demonstra do mesmo modo que a proposição 16. Também temos:

27. *Seja* $\mathfrak{p}_o$ *um ideal primo de* $\mathfrak{R} = k[X_1, \ldots, X_n]$, $\mathfrak{p}_o \neq \mathfrak{R}$ *e seja* $\mathfrak{A}^*$ *um ideal de* $\mathfrak{o} = \mathfrak{R}_{\mathfrak{p}_o}$. *Se* $f \in \mathfrak{A}^{*\rho+\nu}$ ($\rho \geq 1$, $\nu \geq 1$) *então* $\left(\prod_{i;\alpha \in \Lambda} D_i^{\mu_i} D_\alpha^{\nu_\alpha} \right) f \in \mathfrak{A}^{*\rho}$, *onde* $\mu_i \geq 0$ ($i=1, \ldots, n$), $0 \leq \nu_\alpha \leq p-1$, $\nu_\alpha \neq 0$ *sòmente para um número finito de índices* α *de* Λ *e* $\mu_1 + \ldots + \mu_n + \sum_{\alpha \in \Lambda} \nu_\alpha = \nu$.

C A P I T U L O V.

Pontos simples de uma variedade algébrica.

Neste capítulo desenvolveremos a teoria dos pontos (e sub-variedades) simples de uma variedade algébrica; faremos aqui uma exposição de alguns dos resultados que se encontram nos trabalhos de O.Zariski: "The Concept of a Simple Point of an Abstract Algebraic Variety", Transactions of the A.M.S., vol.62(1947), pp. 1-52 e "Aneis locais Generalizados e o Conceito de Ponto simples de uma Variedade Algébrica" (apostila feita dos seminários do prof. Zariski).

§1 - Teoria local.

Seja S_n o espaço linear de n dimensões sôbre um corpo k (II,§1) e seja V uma variedade algébrica irredutível do S_n. Consideremos o ideal $\mathfrak{J}(V)$, da variedade V, no anel de polinômios $R_n = k[X_1,\ldots,X_n]$; já sabemos que $\mathfrak{J}(V)$ é um ideal primo do anel R_n (II,teorema 1). O anel resíduo $R_n/\mathfrak{J}(V) = k[\xi_1,\ldots,\xi_n]$, onde ξ_i = $\mathfrak{J}(V)$-resíduo de X_i (i=1,...,n) é um campo finito de integridade e $(\xi_1,\ldots,\xi_n)$ é um ponto geral de V (cap.II,§3). Seja W uma sub-variedade irredutível de V; indicaremos por $\mathfrak{p}(W/V)$ o ideal primo de W no anel das coordenadas de V: $\mathfrak{R}[V] = k[\xi_1,\ldots,\xi_n]$ (cap.II, prop.10). Consideremos o anel de quocientes $Q(W/V) = \mathfrak{O}$ de $\mathfrak{R}[V]$ em relação ao ideal $\mathfrak{p}(W/V)$; indicaremos por $\mathfrak{m} = \mathfrak{m}(W/V)$ o único ideal máximal de $\mathfrak{O}$. Pela proposição 11, do capítulo II, podemos dizer que $\mathfrak{O}/\mathfrak{m}(W/V) = \mathfrak{F}(W)$, onde $\mathfrak{F}(W) = \Delta$ é o corpo das funções racionais sôbre W, isto é, $\mathfrak{F}(W) = k(\eta_1,\ldots,\eta_n)$, onde (η) é um ponto geral de W. O anel $\mathfrak{O}$ é um anel local (cap.IV, def.6); consideremos então o espaço vectorial $\mathfrak{M}_1 = \mathfrak{M}$ sôbre Δ (cap. IV,§3). Se $u_1,\ldots,u_s$ $(u_i \in \mathfrak{O})$ for uma base mínimal de $\mathfrak{m}$, teremos dim.$\mathfrak{M}_1 = s$ (cap.IV, corolário 4); temos $u_i = f_i(\xi)/g(\xi)$, onde $f_i(\xi) \in \mathfrak{R}[V]$, $g_i(\xi) \in \mathfrak{R}[V]$ e $g_i(\xi) \notin \mathfrak{p}(W/V)$, portanto, podemos supôr que $u_i \in \mathfrak{R}[V]$ (i=1,...,s).

Seja r = dim.V e ρ = dim.W. O campo finito de integridade $\mathfrak{R}[V] = R$ terá grau de transcendência r sôbre k; portanto, pelo teorema de F.K.Schmidt (cap.III,§4), todo ideal

primo isolado de $R.(u_1,\ldots,u_s)$ tem dimensão maior ou igual a r-s. Mas de $\mathfrak{m} = \mathfrak{o}.(u_1,\ldots,u_s) = \mathfrak{o} \cdot p(W/V)$ segue-se que $p(W/V)$ é um ideal primo isolado de $R.(u_1,\ldots,u_s)$ (cap.I,prop.29 e III, def.10) e como dim. $p(W/V)$ = gr.tr. $\mathfrak{R}[W] = \rho$ virá $\rho \geq r-s$, de onde tiramos $s \geq r-\rho$. Demonstrámos assim a proposição

1. dim. $\mathfrak{M} \geq$ dim.V - dim.W.

Em particular, se W for um ponto, teremos:

2. dim. $\mathfrak{M} \geq$ dim.V.

Definição 1 - Uma sub-variedade algébrica irredutível W de V é simples se, e sòmente se, dim. $\mathfrak{M} = r-\rho$, onde r=dim.V e ρ = dim.W. Diremos que W é singular se W não for simples.

Desta definição resulta que uma sub-variedade algébrica irredutível W de V é uma sub-variedade simples de V quando, e sòmente quando, o ideal $\mathfrak{m} = \mathfrak{m}(W/V)$ tem uma base mínimal com $s = r-\rho$ elementos $u_1,\ldots,u_s$, que serão denominados parâmetros uniformizadores de W.

Teorema 1 - Uma sub-variedade algébrica irredutível W de uma variedade irredutível V é simples quando, e sòmente quando, $\mathfrak{o} = Q(W/V)$ é um anel local regular.

Demonstração - Suponhamos que W seja uma sub-variedade simples de V e consideremos o anel $\mathfrak{o} = Q(W/V)$; então o ideal máximal $\mathfrak{m} = \mathfrak{m}(W/V)$ tem uma base mínimal com $s = r-\rho$ (r = dim.V e ρ = dim.W) elementos: $\mathfrak{m} = \mathfrak{o}.(t_1,\ldots,t_s)$. Precisamos demonstrar que dim. $\mathfrak{M}_\nu = \binom{\nu+s-1}{\nu}$ (cap.IV, def. 7). Uma base de $\mathfrak{m}^\nu$ é dada pelos produtos $T_{(\alpha_1,\ldots,\alpha_s)} = t_1^{\alpha_1} \ldots t_s^{\alpha_s}$, onde $\alpha_1 + \ldots + \alpha_s = \nu$; o número dêstes produtos é $\binom{\nu+s-1}{\nu}$ e os correspondentes vectores $\bar{T}_{(\alpha)}$ formam um sistema de geradores de $\mathfrak{M}_\nu$, portanto, dim. $\mathfrak{M}_\nu \leq \binom{\nu+s-1}{\nu}$. A condição necessária estará demonstrada se provarmos que os vectores $\bar{T}_{(\alpha)}$ são linearmente independentes sôbre $\Delta = \mathfrak{o}/\mathfrak{m} = \mathfrak{z}(W)$. Para isto basta demonstrar que de tôda relação da forma $\varphi_\nu(t) = \sum a_{(\alpha)} T_{(\alpha)} = 0$, onde

$a_{(\alpha)} \in \mathfrak{o}$, vem $a_{(\alpha)} \in \mathfrak{m}$ (cap.IV,prop.12). Consideremos uma transformação linear $t_i = \sum_{j=1}^{s} b_{ij} \tau_j$, onde $b_{ij} \in \mathfrak{o}$ e $|b_{ij}| \not\equiv 0$ (mod.$\mathfrak{m}$). Pelo corolário 6 do capítulo IV, sabemos que $\{\tau_1, \ldots, \tau_s\}$ é também uma base mínimal de $\mathfrak{m}$. A forma $\varphi_\nu(t)$ vem transformada numa forma $\Psi_\nu(\tau)$ de grau ν, nos parâmetros locais $\tau_1, \ldots, \tau_s$: $\varphi_\nu(t) = \Psi_\nu(t) = \sum c_{(\alpha)} \tau_1^{\alpha_1} \ldots \tau_s^{\alpha_s}$, onde $c_{(\alpha)} \in \mathfrak{o}$. Seja $\overline{\Psi}_\nu(Z) = \sum \bar{c}_{(\alpha)} Z_1^{\alpha_1} \ldots Z_s^{\alpha_s}$ a forma de grau ν, obtida de $\Psi_\nu(\tau)$ substituindo τ_i por Z_i (indeterminada sôbre Δ) e $c_{(\alpha)}$ pelo seu resíduo módulo $\mathfrak{m}$; consideremos também a forma $\overline{\varphi}_\nu(z) = \sum \bar{a}_{(\alpha)} z_1^{\alpha_1} \ldots z_s^{\alpha_s}$, onde $z_1, \ldots, z_s$ são indeterminadas sôbre Δ. A transformação $z_i = \sum_{j=1}^{s} \bar{b}_{ij} Z_j$ leva a forma $\overline{\varphi}_\nu(z)$ na forma $\overline{\Psi}_\nu(Z)$; ainda mais, o coeficientes de Z_1^ν nesta última forma é igual a $\overline{\varphi}_\nu(\bar{b}_{11}, \ldots, \bar{b}_{s1})$, portanto, $\overline{\Psi}_\nu(Z) = \bar{a} Z_1^\nu + \ldots$, onde $\bar{a} = \overline{\varphi}_\nu(\bar{b}_{11}, \ldots, \bar{b}_{s1})$. Suponhamos, por absurdo, que $\overline{\varphi}_\nu(z) \not\equiv 0$. Se Δ tiver infinitos elementos poderemos determinar s^2 elementos $\bar{b}_{ij}$ em Δ tais que $|\bar{b}_{ij}| \not\equiv 0$ e $\overline{\varphi}_\nu(\bar{b}_{11}, \ldots, \bar{b}_{s1}) \not\equiv 0$. Portanto por uma mudança de parâmetros locais obtemos uma forma que tem um têrmo que só depende de τ_1: $a\tau_1^\nu$, onde $a \notin \mathfrak{m}$. Podemos, então, desde o início, supôr que a forma $\varphi_\nu(t)$ verifique esta condição, isto é, $\varphi_\nu(t) = at_1^\nu + \ldots = 0$, onde $a \notin \mathfrak{m}$. Mas de $at_1^\nu + \ldots = 0$ tiramos $at_1^\nu \in \mathfrak{o}.(t_2, \ldots, t_s)$ e então $t_1^\nu \in \mathfrak{o}.(t_2, \ldots, t_s)$, isto é, $t_1 \in \text{Rad.}\,\mathfrak{o}(t_2, \ldots, t_s)$. Seja $\mathfrak{p}$ um ideal primo isolado de $\mathfrak{o}.(t_2, \ldots, t_s)$; teremos (pelo teorema de F.K.Schmidt, cap.III,§3) dim. $\mathfrak{p} \geq r-(s-1) = \rho+1$. Mas, por outro lado, $t_1 \in \mathfrak{p}$, portanto, $\mathfrak{p} \supset \mathfrak{o}.(t_2, \ldots, t_s)$ e então $\mathfrak{p} = \mathfrak{m}$. Chegámos assim a uma contradição pois dim.$\mathfrak{m} = \rho$. No caso em que Δ é finito a condição necessária do teorema 1 é verdadeira (ver a demonstração em [19], pp.21-22). Suponhamos agora que $\mathfrak{o} = Q(\mathbb{W}/V)$ seja um anel local regular e seja $\{t_1, \ldots, t_s\}$ uma base mínimal de $\mathfrak{m}$. Pela proposição 1 temos dim.$\mathfrak{m} = s \geq r-\rho$. Agora, pelo teorema 12 do capítulo IV temos $(0) \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_{s-1} \subset \mathfrak{p}_s = \mathfrak{m}$, $\mathfrak{p}_i = \mathfrak{o}.(t_1, \ldots, t_i)$ e $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$, $\mathfrak{p}_1 \neq (0)$, portanto, dim.$(0) >$ dim.$\mathfrak{p}_1 > \ldots >$ dim.$\mathfrak{p}_{s-1} >$ dim.$\mathfrak{p}_s =$ dim.$\mathfrak{m}$. Mas

dim. (O) = r e dim.$\mathfrak{m} = \rho$, logo, $s \leq r-\rho$ e então $s = r-\rho$. (q.e.d.).

Da demonstração da condição suficiente do teorema anterior tiramos, imediatamente, a proposição:

3. Seja W uma sub-variedade irredutível e simples de uma variedade irredutível V. Se $u_1,\ldots,u_i$ forem i elementos de $\mathfrak{m} = \mathfrak{m}(W/V)$ tais que $\tau u_1,\ldots,\tau u_i$ sejam linearmente independentes sôbre Δ (onde τ é o homomorfismo canônico de $\mathfrak{m}$ sôbre $\mathfrak{M}$) então o ideal $\mathfrak{p}_i = \mathfrak{o}.(u_1,\ldots,u_i)$ será primo e de dimensão r-i (r = dim.V).

Teorema 2 - Todo ponto P do espaço linear S_n é um ponto simples de S_n.

Demonstração - Sejam $\alpha_1,\ldots,\alpha_n$ $(\alpha_i \in \bar{k})$ as coordenadas do ponto P. O elemento α_1 é algébrico sôbre k; seja $f_1(X) \in k[X]$, o polinômio mínimal de α_1 e ponhamos $t_1 = f_1(X_1) \in R_n$. A coordenada α_2 é algébrica sôbre k, portanto, é também algébrica sôbre $k(\alpha_1)$; seja $f_2(X) \in k(\alpha_1)[X]$ (anel de polinômios de uma indeterminada X sôbre $k(\alpha_1)$) o polinômio mínimal de α_2 sôbre $k(\alpha_1)$. O coeficiente da mais alta potência X^{ν_2} de X em f_2 é igual à unidade e os outros coeficientes podem ser escritos como polinômios em α_1, com coeficientes em k e de graus no máximo iguais a ν_1-1, onde $\nu_1 = [k(\alpha_1):k] =$ $= gr.f_1$: $f_2(X) = X^{\nu_2} + (a_{11}\alpha_1^{\nu_1-1} + \ldots + a_{1\nu_1})X^{\nu_2-1} + \ldots +$ $+(a_{\nu_2,1}\alpha_1^{\nu_1-1} + \ldots + a_{\nu_2,\nu_1})$, onde $a_{ij} \in k$. Poremos $t_2 = f_2(X_1,X_2) =$ $= X_2^{\nu_2} + (a_{11}X_1^{\nu_1-1} + \ldots + a_{1\nu_1})X_2^{\nu_2-1} + \ldots + (a_{\nu_2,1}X_1^{\nu_1-1} +$ $+ \ldots + a_{\nu_2,\nu_1})$ que é um polinômio de R_n. Do mesmo modo podemos determinar um polinômio $t_3 = f_3(X_1,X_2,X_3)$ de grau $\nu_3 = [k(\alpha_1,\alpha_2,\alpha_3):k(\alpha_1,\alpha_2)]$ em relação a X_3 e de graus $\leq \nu_1-1$ e $\leq \nu_2-1$ em relação a X_1 e X_2, respectivamente. Assim por diante obteremos n polinômios $t_1,\ldots,t_n$ que têm as propriedades:

1. $t_i = f_i(X_1,\ldots,X_i) \in R_i = k[X_1,\ldots,X_i]$;
2. $gr._{X_i} t_i = \nu_i = [k(\alpha_1,\ldots,\alpha_i):k(\alpha_1,\ldots,\alpha_{i-1})]$ e o coeficiente de $X_i^{\nu_i}$ é igual a 1;
3. $gr._{X_j} t_i < \nu_j$ se $j < i$;
4. $f_i(\alpha_1,\ldots,\alpha_{i-1},X_i)$ é o polinômio mínimal de α_i sôbre $k(\alpha_1,\ldots,\alpha_{i-1})$.

Se provarmos que $\mathfrak{m} = \mathfrak{o}.(t_1,\ldots,t_n)$ onde $\mathfrak{o} = Q(P/S_n)$ e que $\{t_1,\ldots,t_n\}$ é uma base mínimal do ideal $\mathfrak{m} = \mathfrak{o}.\mathfrak{p}_o$ $(\mathfrak{p}_o = \mathfrak{J}(P))$ resultará que P é um ponto simples de S_n. Demonstraremos que $\mathfrak{p}_o = R_n.(t_1,\ldots,t_n)$ e que $\{t_1,\ldots,t_n\}$ é uma base mínimal de $\mathfrak{p}_o$ (d'aqui virá, evidentemente, o resultado anterior). Suponhamos que n=1; neste caso é imediato que $\mathfrak{p}_o = R_1.(t_1)$ e $\{t_1\}$ é uma base mínimal de $\mathfrak{p}_o$. Suponhamos a proposição acima verdadeira para n-1 e consideremos o anel resíduo $k[X_1,\ldots,X_n]/(t_1) = k[\alpha_1,X_2,\ldots,X_n] = k(\alpha_p)[X_2,\ldots,X_n]$. Temos assim um anel de polinômios em n-1 indeterminadas $X_2,\ldots,X_n$ sôbre o corpo $k'=k(\alpha_1)$. Ao ideal $\mathfrak{p}_o = R_n.(t_1,\ldots,t_n)$ corresponderá um ideal $\mathfrak{p}_o' = \tau\mathfrak{p}_o$, onde τ é o homomorfismo canônico de R_n sôbre $k(\alpha_1)[X_2,\ldots,X_n]$. Pela hipótese de indução segue-se que o ideal $\mathfrak{p}_o'$ tem $\{\tau t_2,\ldots \tau t_n\}$ como base mínimal; mas $\mathfrak{p}_o = \bar{\tau}^1\mathfrak{p}_o'$. portanto, $\{t_1,\ldots,t_n\}$ é uma base de $\mathfrak{p}_o$. Ainda mais, esta é uma base mínimal de $\mathfrak{p}_o$, pois, caso contrário, $\{t_2,\ldots,\tau t_n\}$ não seria uma base mínimal de $\mathfrak{p}_o'$. Isto completa a demonstração do teorema 1.

Os polinômios $f_1(X_1), f_2(X_1,X_2),\ldots,f_n(X_1,\ldots,X_n)$, construidos na demonstração do teorema 1, são denominados <u>parâmetros locais canônicos do ponto P</u>.

Seja W uma sub-variedade irredutível de uma variedade algébrica irredutível V; seja $(\xi_1,\ldots,\xi_n)$ e $(\eta_1,\ldots,\eta_n)$ os pontos gerais de W e V, respectivamente. Temos o seguinte homomorfismo (relativo a k):
$\tau: k[\xi_1,\ldots,\xi_n] \sim k[\eta_1,\ldots,\eta_n]$ que leva ξ_i sôbre η_i (i=1,...,n). Suponhamos que êste homomorfismo τ induza um isomorfismo entre os aneis $k[\xi_1,\ldots,\xi_\nu]$ e $k[\eta_1,\ldots,\eta_\nu]$ $(1 \leq \nu \leq n)$; é, então, possível identificar cada ξ_i com o correspondente η_i, para $i=1,\ldots,\nu$. Consideremos agora as variedades

algébricas W^* e V^* do espaço linear $S^{k^*}_{n-v}$, onde $k^* = k(\xi_1, \ldots, \xi_v)$, cujos pontos gerais são, respectivamente, $(\eta_{v+1}, \ldots, \eta_n)$ e $(\xi_{v+1}, \ldots, \xi_n)$. Demonstraremos a seguinte proposição:

4. $Q(W/V) = Q(W^*/V^*)$ e, portanto, $m(W/V) = m(W^*/V^*)$.

Com efeito, é imediato que $Q(W/V) \supset k^*$, pois $k[\xi_1, \ldots, \xi_v] \cap \wp = (0)$, onde $\wp = p(W/V)$. D'aqui tiramos que $Q(W/V) \subset Q(W^*/V^*)$. Mas todo elemento de $\mathfrak{R}[V^*]$ pode ser escrito como o quociente de um elemento de $\mathfrak{R}[V]$ por um elemento de $k[\xi_1, \ldots, \xi_v]$ e, também, todo elemento de $\wp^*$, $\wp^* = p(W^*/V^*)$ (notar que W^* é uma sub-variedade de V^*), pode ser escrito como o quociente de um elemento de $\wp$, $\wp = p(W/V)$, por um elemento de $k[\xi_1, \ldots, \xi_v]$. D'aqui resulta que todo elemento de $Q(W^*/V^*)$ é elemento de $Q(W/V)$, portanto, $Q(W/V) = Q(W^*/V^*)$.

A proposição 4 nos dá, num caso especial, a "redução à dimensão zero". Seja ρ a dimensão de W; então, usando uma notação conveniente podemos supôr que $\eta_1, \ldots, \eta_\rho$ são algébricamente independentes sôbre k e, portanto, também $\xi_1, \ldots, \xi_\rho$ são algèbricamente independentes sôbre k. Então é possível identificar ξ_i com η_i para $i=1, \ldots, \rho$. Neste caso, obteremos uma variedade algébrica V^* em $S^{k^*}_{n-\rho}$ de dimensão $r-\rho$ (sôbre k^*) e a variedade algébrica W^*, cujo ponto geral é $(\eta_{\rho+1}, \ldots, \eta_n)$ é então um ponto de V^* (pois $\eta_{\rho+1}, \ldots, \eta_n$ são algébricos sôbre k^*).

Teorema 3 - Tôda variedade algébrica irredutível W do espaço linear S_n é uma variedade simples do S_n.

Demonstração - Temos o homomorfismo $\tau: k[X_1, \ldots, X_n] \sim k[\eta_1, \ldots, \eta_n]$, onde $\tau X_i = \eta_i$ $(i=1, \ldots, n)$ e $(\eta_1, \ldots, \eta_n)$ é o ponto geral de W. Seja ρ a dimensão de W sôbre k; usando uma notação conveniente podemos supôr que $\eta_1, \ldots, \eta_\rho$ sejam algébricamente independentes sôbre k e, portanto, podemos pôr $\eta_i = X_i$ para $i=1, \ldots, \rho$. Consideremos o espaço linear $S^{k^*}_{n-\rho}$ sôbre $k^* = k(X_1, \ldots, X_\rho)$ e nele a variedade algébrica W^* cujo ponto geral é $(\eta_{\rho+1}, \ldots, \eta_n)$. W^* é um ponto de $S^{k^*}_{n-\rho}$ e já sabemos que $Q(W/S_n) = Q(W^*/S^{k^*}_{n-\rho})$ (prop.4); pelo teorema 2, W^* é um ponto simples de $S^{k^*}_{n-\rho}$, portanto, o ideal $m^* = m(W^*/S^{k^*}_{n-\rho})$ tem uma base mínimal com $n-\rho$ elementos. Mas $m = m(W/S_n) = m^*$,

logo, $\mathfrak{m}$ também tem uma base mínimal com $n-\rho$ elementos, isto é, W é uma variedade simples do S_n. (q.e.d.).

Sejam agora W, V' e V variedades algébricas irredutíveis do S_n, tais que $W \subset V' \subset V$. Consideremos os espaços vectoriais $\mathfrak{M} = \mathfrak{M}(W/V)$ e $\mathfrak{M}' = \mathfrak{M}(W/V')$ sôbre $\Delta = \mathfrak{F}(W)$. Seja $\mathfrak{o} = \mathfrak{Q}(W/V)$, $\mathfrak{m} = \mathfrak{m}(W/V)$, $\mathfrak{o}' = \mathfrak{Q}(W/V')$ e $\mathfrak{m}' = \mathfrak{m}(W/V')$. Temos as seguintes aplicações (cap.IV, §2.1)

τ: $u \in \mathfrak{m} \longrightarrow \bar{u} = \mathfrak{m}^2$-resíduo de u, $\bar{u} \in \mathfrak{M}$ e

τ': $u' \in \mathfrak{m}' \longrightarrow \bar{u}' = \mathfrak{m}'^2$-resíduo de u', $\bar{u}' \in \mathfrak{M}'$. Sejam $(\xi_1, \ldots, \xi_n)$ e $(\xi'_1, \ldots, \xi'_n)$ os pontos gerais de V e V', respectivamente, e ponhamos $R = \mathfrak{R}[V]$ e $R' = \mathfrak{R}[V']$. Sendo V' uma sub-variedade algébrica de V existe um homomorfismo Ψ de R sôbre R' que leva ξ_i sôbre ξ'_i $(i=1,\ldots,n)$; o núcleo de Ψ é o ideal $\mathfrak{P}_1 = \mathfrak{p}(V'/V)$ e, ainda mais, $\bar{\Psi}^{-1}(\mathfrak{P}') = \mathfrak{P}$, onde $\mathfrak{P} = \mathfrak{p}(W/V)$ e $\mathfrak{P}' = \mathfrak{p}(W/V')$. O homomorfismo Ψ pode ser prolongado, de um único modo, a um homomorfismo de $\mathfrak{o}$ sôbre $\mathfrak{o}'$; continuaremos a indicar êste prolongamento por Ψ. Notemos que $\Psi(\mathfrak{m}) = \mathfrak{m}'$. Seja $\mathfrak{P}_1 = \mathfrak{o}.\mathfrak{P}_1$; é fácil ver que $\mathfrak{P}_1$ é o núcleo do homomorfismo Ψ de $\mathfrak{o}$ sôbre $\mathfrak{o}'$. E' imediato que $\tau\mathfrak{P}_1$ é um sub-espaço vectorial de $\mathfrak{M}$; notemos que $\tau\mathfrak{P}_1$ é gerado pelos vectores pertencentes a $\tau\mathfrak{P}_1$. Nestas condições demonstraremos o seguinte (ver [19], p.9):

Teorema 4 - $\Phi = \tau'\Psi\bar{\tau}$ é uma aplicação linear de $\mathfrak{M}$ sôbre $\mathfrak{M}'$; ainda mais, $\bar{\Phi}(0) = \tau\mathfrak{P}_1$.

Demonstração - Sendo $\Psi(\mathfrak{m}) = \mathfrak{m}'$ segue-se que Φ leva $\mathfrak{M}$ sôbre $\mathfrak{M}'$. a) Φ é uma aplicação. Com efeito, se $\bar{u} = \bar{v}$ temos $\bar{\tau}'(\bar{u}) = \bar{\tau}'(\bar{v})$, ou, $u + \mathfrak{m}^2 = v + \mathfrak{m}^2$, onde $u \in \mathfrak{m}$, $v \in \mathfrak{m}$ e $\tau u = \bar{u}$, $\tau v = \bar{v}$; mas $\Psi(\mathfrak{m}^2) = \mathfrak{m}'^2$, logo, $\Psi(u) + \mathfrak{m}'^2 = \Psi(v) + \mathfrak{m}'^2$ e, portanto, $\tau'\Psi(u) = \tau'\Psi(v)$, isto é, $\Phi(\bar{u}) = \Phi(\bar{v})$. b) Φ é um homomorfismo do grupo aditivo de $\mathfrak{M}$ sôbre o grupo aditivo de $\mathfrak{M}'$. Isto é imediato pois τ, Ψ e τ' são homomorfismos (sôbre) entre grupos aditivos. c) Φ é linear, isto é, $\Phi(\bar{\delta}\,\bar{u}) = \bar{\delta}\,\Phi(\bar{u})$, onde $\bar{\delta} \in \Delta$. Com efeito, sejam u e δ elementos de $\mathfrak{m}$ e $\mathfrak{o}$, respectivamente, tais que $\tau u = \bar{u}$ e $\bar{\delta} = \mathfrak{m}$-resíduo de δ. Temos $\tau(\delta u) = \bar{\delta}\,\bar{u}$, portanto, $\Phi(\tau(\delta u)) = \Phi(\bar{\delta}\,\bar{u})$; mas $\bar{\delta} = \mathfrak{m}'$-resíduo de $\Psi(\delta)$, logo,

$(\tau'\Psi)\delta u = \tau'(\Psi(\delta)\Psi(u)) = \bar{\delta}.(\tau'\Phi)u$. Mas $\Phi\tau = \tau'\Psi$, logo, $\Phi(\bar{\delta}\bar{u}) = \bar{\delta}(\Phi\tau)u = \bar{\delta}.\Phi(\bar{u})$. d) $\bar{\Phi}(0) = \tau\mathfrak{P}_1$. Com efeito, temos $(\Phi\tau)u = \Phi(\bar{u})$ e $(\bar{\Phi}\tau)u = (\tau'\Psi)u$, portanto, teremos, $\Phi(\bar{u}) = 0$ quando, e sòmente quando, $(\tau'\Psi)u = 0$, isto é, quando, e sòmente quando $\Psi(u) \in \mathfrak{m}'^2$. Mas $\bar{\Psi}^{-1}(0) = \mathfrak{P}_1$, logo, $\bar{\Phi}(\bar{u}) = 0$ quando, e sòmente quando, $u \in \mathfrak{m}^2 + \mathfrak{P}_1$; d'aqui tiramos $\bar{\Phi}^{-1}(0) = \tau\mathfrak{P}_1$. (q.e.d.).

Teorema 5 - Seja V uma variedade algébrica irredutível do S_n e seja W uma sub-variedade irredutível de V; ponhamos r = dim.V e ρ = dim.W. Então W é uma sub-variedade simples de V quando, e sòmente quando, o ideal $\mathfrak{p} = \mathfrak{J}(V)$ contém n-r elementos $u_1,\ldots,u_{n-r}$ tais que os vectores $\tau u_1,\ldots,\tau u_{n-r}$ de $\mathfrak{M}(W/S_n)$ sejam linearmente independentes sôbre $\mathfrak{F}(W) = \Delta$.

Demonstração - Temos dim.$\mathfrak{M}(W/S_n) = n-\rho$ (teorema 3); pelo teorema 4 teremos dim.$\mathfrak{M}(W/V) = r-\rho$ quando, e sòmente quando, o núcleo da aplicação linear Φ, de $\mathfrak{M}(W/S_n)$ sôbre $\mathfrak{M}(W/V)$ tiver dimensão n-r. Mas, por outro lado, o núcleo de Φ é gerado pelos vectores pertencentes a $\tau\mathfrak{p}$ (τ: $\mathfrak{M}(W/S_n) \longrightarrow \mathfrak{M}(W/S_n)$), portanto, W é uma sub-variedade simples de V quando, e sòmente quando, $\mathfrak{p}$ contém n-r elementos $u_1,\ldots,u_{n-r}$ tais que os vectores $\tau u_1,\ldots,\tau u_{n-r}$ sejam linearmente independentes sôbre $\Delta = \mathfrak{F}(W)$. (q.e.d.).

Corolário 1 - Seja $\mathfrak{o} = \mathfrak{Q}(W/S_n)$, onde W é uma sub-variedade irredutível de uma variedade irredutível V do S_n. Então W é uma sub-variedade simples de V quando, e sòmente quando, o ideal $\mathfrak{o}.\mathfrak{p}$, $\mathfrak{p} = \mathfrak{J}(V)$, tem uma base $\{u_1,\ldots,u_s\}$ ($u_i \in \mathfrak{o}$) tal que os vectores $\tau u_1,\ldots,\tau u_s$ de $\mathfrak{M}(W/S_n)$ sejam linearmente independentes sôbre $\Delta = \mathfrak{F}(W)$.

Demonstração - Suponhamos que W seja uma sub-variedade simples de V; então, pelo teorema 5, existem $n-r$ elementos $u_1,\ldots,u_{n-r}$ de $\mathfrak{p}$ tais que $\tau u_1,\ldots,\tau u_{n-r}$ sejam linearmente independentes sôbre $\Delta = \mathfrak{F}(W)$. Temos $\mathfrak{o}.(u_1,\ldots,u_{n-r}) \subset \mathfrak{o}.\mathfrak{p}$ e dim. $\mathfrak{o}.\mathfrak{p} = r$; mas, pela proposição 3, dim. $\mathfrak{o}(u_1,\ldots,u_{n-r}) = n-(n-r) = r$. Sendo $\mathfrak{o}.\mathfrak{p}$ um ideal primo (cap.I, teorema 12) segue-se que $\mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(u_1,\ldots,u_{n-r})$ (cap.III, teorema 3). Está assim demonstrada a condição necessária. Suponhamos agora que $\mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(u_1,\ldots,u_s)$ onde os vectores $\tau u_1,\ldots,\tau u_s$ de $\mathfrak{M}(W/S_n)$ são linearmente independentes sôbre $\Delta = \mathfrak{F}(W)$. Pela proposição 3 virá dim. $\mathfrak{o}.\mathfrak{p}$ = dim. $V = n-s$, logo, $s = n-r$. Mas $\tau(\mathfrak{o}.\mathfrak{p})$ é o núcleo da aplicação linear Φ de $\mathfrak{M}(W/S_n)$ sôbre $\mathfrak{M}(W/V)$, logo, dim. $\mathfrak{M}(W/V) = r-\rho$, isto é, W é uma sub-variedade simples de V. (q.e.d.).

Corolário 2 - Os elementos $u_1,\ldots,u_{n-r}$ (determinados no teorema 5) formam uma base mínimal de $\mathfrak{o}.\mathfrak{p}$.

E' imediato, pois, caso contrário, teríamos dim.$V > r$ (pela proposição 3).

Corolário 3 - Seja W uma sub-variedade irredutível e simples de uma variedade algébrica irredutível V. Então tôda base mínimal de $\mathfrak{o}.\mathfrak{p}$ consiste de $n-r$ elementos $v_1,\ldots,v_{n-r}$ tais que os vectores $\tau v_1,\ldots,\tau v_{n-r}$ de $\mathfrak{M}(W/S_n)$ sejam linearmente independentes sôbre $\Delta = \mathfrak{F}(W)$.

Demonstração - Pelo teorema 5 existem $n-r$ elementos $u_1,\ldots,u_{n-r}$ em $\mathfrak{p}$ tais que os vectores $\tau u_1,\ldots,\tau u_{n-r}$ sejam linearmente independentes sôbre Δ; ainda mais $\mathfrak{O} = \mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(u_1,\ldots,u_{n-r})$. Temos $\mathfrak{O}\mathfrak{m} \subset \mathfrak{m}^2 \cap \mathfrak{O}$ (onde $\mathfrak{m} = \mathfrak{m}(W/S_n)$); se $\omega \in \mathfrak{m}^2 \cap \mathfrak{O}$ teremos $\omega = a_1u_1 + \ldots + a_{n-r}u_{n-r}$, onde $a_i \in \mathfrak{o}$ $(i=1,\ldots,n-r)$, então $\tau\omega = \bar{a}_1\tau u_1 + \ldots + \bar{a}_{n-r}\tau u_{n-r} = 0$, portanto, $a_i \in \mathfrak{m}$ e então $\omega \in \mathfrak{O}\mathfrak{m}$. Isto nos mostra que $\mathfrak{O}\mathfrak{m} = \mathfrak{O} \cap \mathfrak{m}^2$. Portanto, podemos considerar o espaço vectorial $\mathfrak{O}/\mathfrak{O}\mathfrak{m}$ (sôbre $\Delta = \mathfrak{F}(W)$ como um sub-espaço de $\mathfrak{M}(W/S_n)$. Seja $v_1,\ldots,v_s$ uma

uma base mínimal de $\mathfrak{o}.\mathfrak{p}$; do mesmo modo que na demonstração do teorema 9 do capítulo IV segue-se que os vectores $\bar{v}_1,\ldots,\bar{v}_s$ de $\mathfrak{N}/\mathfrak{N}\mathfrak{m}$ são linearmente independentes sôbre Δ. Em consequência também os vectores $\tau v_1,\ldots,\tau v_s$ de $\mathfrak{M}(V/S_n)$ são linearmente independentes sôbre Δ; pelo corolário 1 teremos dim.V = n-s e, portanto, s = n - r. (q.e.d.).

Corolário 4 - Seja P um ponto simples de uma variedade algébrica irredutível V. Então existe um sistema de parâmetros uniformizadores $u_1,\ldots,u_n$ de P, como ponto do S_n, tal que
$\mathfrak{o}.\mathfrak{p} = \mathfrak{O}.(u_1,\ldots,u_{n-r})$, onde
$\mathfrak{p} = \mathfrak{J}(V)$ e $\mathfrak{O} = \mathfrak{Q}(P/S_n)$.

Com efeito, pelo teorema 5 existem n-r elementos $u_1,\ldots,u_{n-r}$ em $\mathfrak{p}$ tais que os vectores $\tau u_1,\ldots,\tau u_{n-r}$ de $\mathfrak{M}(P/S_n)$ sejam linearmente independentes sôbre $\Delta = \mathfrak{J}(P)$. Pela demonstração do corolário 1 temos $\mathfrak{o}.\mathfrak{p} = \mathfrak{O}.(u_1,\ldots,u_{n-r})$. Mas os vectores $\tau u_1,\ldots,\tau u_{n-r}$ podem ser imersos numa base $\{\tau u_1,\ldots,\tau u_n\}$ de $\mathfrak{M}(P/S_n)$. Teremos então $\mathfrak{m}(P/S_n) = \mathfrak{O}.(u_1,\ldots,u_n)$ e $\mathfrak{o}.\mathfrak{p} = \mathfrak{O}.(u_1,\ldots,u_{n-r})$. (q.e.d.).

§ 2 - Critério das matrizes jacobianas.

Seja $R_n = k[X_1,\ldots,X_n]$ um anel de polinômios de n indeterminadas $X_1,\ldots,X_n$ sôbre o corpo k. A matriz $\|\partial f_i/\partial X_j\|$ (i=1,...,s; j=1,...,n e $f_i \in K = k(X_1,\ldots,X_n)$) é denominada matriz jacobiana de $f_1,\ldots,f_s$ em relação a $X_1,\ldots,X_n$; se s=n o determinante $|\partial f_i/\partial X_j|$ é denominado jacobiano de $f_1,\ldots,f_n$ em relação a $X_1,\ldots,X_n$. Indicaremos também u'a matriz jacobiana por $J(f_1,\ldots,f_s;X_1,\ldots,X_n)$, ou, simplesmente, por $J(f;X)$.

Seja $P(\alpha_1,\ldots,\alpha_n)$ um ponto do espaço linear S_n e sejam $t_1,\ldots,t_n$ os parâmetros locais canônicos do ponto P (ver demonstração do teorema 2); já sabemos que $\mathfrak{J}(P) = R_n.(t_1,\ldots,t_n)$ e, portanto, $R_n/\mathfrak{J}(P) = k[\alpha_1,\ldots,\alpha_n] = k(\alpha_1,\ldots,\alpha_n)$. Pelo teorema 4 do capítulo IV temos, imediatamente, que

Teorema 6 - A condição necessária e suficiente para que as coordenadas $\alpha_1,\ldots,\alpha_n$ do ponto P sejam separáveis sôbre k é que o jacobiano $|J(t;X)|$ seja diferente de zero no ponto P (ou, o que é o mesmo, $|J(t;X)| \not\equiv 0 \pmod{\mathfrak{m}}$, onde $\mathfrak{m} = \mathfrak{m}(P/S_n)$).

Por causa desta propriedade é que dizemos que quando $|J(t;X)|_{X=\alpha} \neq 0$, temos o caso separável.

Suponhamos que $J(t;X) \not\equiv 0 \pmod{\mathfrak{m}}$, isto é, que tenhamos o caso separáveis e sejam $u_1,\ldots,u_n$ um sistema de parâmetros uniformizadores do ponto P. Teremos $u_i = \sum_{\ell=1}^{n} a_{i\ell} t_\ell$ $(i=1,\ldots,n;\ a_i \in \mathfrak{o} = \mathfrak{o}(P/S_n))$, onde $|a_{ij}| \not\equiv 0 \pmod{\mathfrak{m}}$ (cap. III, corolário 6); destas relações vem $\frac{\partial u_i}{\partial X_j} = \sum_{\ell=1}^{n} a_{i\ell} \frac{\partial t_\ell}{\partial X_j}$, logo, $|J(u,X)|_{X=\alpha} = |a_{i\ell}|_{X=\alpha} |J(t;X)|_{X=\alpha}$. Como $|a_{i\ell}|_{X=\alpha} \neq 0$ e $|J(t;X)|_{X=\alpha} \neq 0$ teremos $|J(u;X)|_{X=\alpha} \neq 0$. Consideremos agora n elementos $u_1,\ldots,u_n$ de $\mathfrak{m} = \mathfrak{m}(P/S_n)$ tais que $|J(u;X)| \not\equiv 0 \pmod{\mathfrak{m}}$. Afirmamos que os elementos $u_1,\ldots,u_n$ são parâmetros uniformizadores do ponto P e que se trata do caso separável. Com efeito, basta demonstrar que os vectores $\tau u_1,\ldots,\tau u_n$ de $\mathfrak{M}(P/S_n)$ são linearmente independentes sôbre $\Delta = \mathfrak{z}(P)$. Se isto não acontecesse teríamos uma relação da forma (usando uma notação conveniente) $u_1 = \sum_{i=2}^{n} a_i u_i + u$, onde $a_i \in \mathfrak{o}$ e $u \in \mathfrak{m}^2$. D'aqui tiramos $\frac{\partial u_1}{\partial X_j} \equiv \sum_{i=2}^{n} a_i \frac{\partial u_i}{\partial X_j} \pmod{\mathfrak{m}}$ para $j=1,\ldots,n$ e então $|J(u;X)| \in \mathfrak{m}$, contra a hipótese. Demonstrámos assim o

Teorema 7 - Uma condição suficiente para que n elementos $u_1,\ldots,u_n$ de $\mathfrak{m} = \mathfrak{m}(P/S_n)$ sejam parâmetros uniformizadores do ponto P é que $|J(u;X)| \not\equiv 0 \pmod{\mathfrak{m}}$. Se tivermos o caso separável a condição acima é também necessária.

Seja V uma variedade irredutível, de dimensão r, do espaço linear S_n e seja $\{F_1(X),\ldots,F_s(X)\}$ uma base do ideal $\mathfrak{J}(V)$ de R_n. Consideremos um ponto $P(\alpha_1,\ldots,\alpha_n)$ de V. Demonstraremos o

Teorema 8 - Uma condição suficiente para que P seja um ponto simples de V é que a matriz jacobiana J(F;X) tenha característica n-r em P. Se tivermos o caso separável a condição acima é também necessária.

Demonstração - Suponhamos que a matriz J(F;X) tenha característica n-r no ponto P; usando uma notação conveniente podemos supôr que $\left|\frac{\partial F_i}{\partial X_j}\right|_{X=\alpha} \neq 0$, onde i=1,...,n-r e j=r+1,...,n. Afirmamos que os vectores $\tau F_1,\ldots,\tau F_{n-r}$ de $\mathfrak{M}(P/S_n)$ são linearmente independentes sôbre $\mathfrak{J}(P)$; d'aqui resultará, pelo teorema 5 (aplicado para o caso em que W=P), que P é um ponto simples de V. Ora, se aqueles vectores não fossem linearmente independentes teríamos uma relação da forma (usando uma notação conveniente):

$F_1 = \sum_{j=2}^{n} a_i F_i + u$, onde $a_i \in \mathfrak{o}$ e $u \in \mathfrak{m}^2$. D'aqui tiramos

$\frac{\partial F_1}{\partial X_j} \equiv \sum_{i=2}^{n-r} a_i \frac{\partial F_i}{\partial X_j}$ (mod. $\mathfrak{m}$), j=r+1,...,n e então

$\left|J(F_1,\ldots,F_{n-r};X_{r+1},\ldots,X_n)\right|_{X=\alpha} = 0$, contra a hipótese. Está assim demonstrada a condição suficiente do teorema 8. Passamos a demonstrar a segunda parte do teorema. Seja então P um ponto simples de V; temos $\mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(F_1,\ldots,F_s)$ (onde $\mathfrak{o} = \mathfrak{Q}(P/S_n)$), portanto, pelo teorema 5 e pelo corolário 3, virá (usando uma notação conveniente) $\mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(F_1,\ldots,F_{n-r})$ e os vectores $\tau F_1,\ldots,\tau F_{n-r}$ de $\mathfrak{M}(P/S_n)$ são linearmente independentes sôbre $\Delta = \mathfrak{J}(P)$. Por outro lado, temos $F_i = \sum_{\ell=1}^{n} a_{i\ell} t_\ell$, onde $t_1,\ldots,t_n$ são os parâmetros locais canônicos do ponto P e $a_{i\ell} \in \mathfrak{o}$ (i=1,...,n-r); d'aqui resulta que a matriz $\|a_{i\ell}\|$ (i=1,...,n-r; ℓ=1,...,n) tem característica n-r no ponto P e também que

$J(F_1,\ldots,F_{n-r};X_1,\ldots,X_n)_{X=\alpha} = \|a_{ij}\|_{X=\alpha}\, J(t_1,\ldots,t_n;X_1,\ldots,X_n)_{X=\alpha}$.

Mas, por hipótese, temos $\left|J(t;X)\right|_{X=\alpha} \neq 0$, portanto, a característica

de $J(F_1,\ldots,F_{n-r};X_1,\ldots,X_n)$ no ponto P é igual a n-r. Como cada F_j $(j=n-r+1,\ldots,s)$ é combinação linear, com coeficientes em $\mathfrak{o}$, de $F_1,\ldots,F_{n-r}$, segue-se que a característica da matriz jacobiana $J(F_1,\ldots,F_s;X_1,\ldots,X_n)$, no ponto P, é igual à n-r. (q.e.d.).

Corolário 5 - Suponhamos que k seja um corpo perfeito. Então a condição necessária e suficiente para que $P(\alpha)$ seja um ponto simples de V é que a matriz jacobiana J(F;X) tenha característi- n-r no ponto P.

Êste corolário é uma consequência imediata do teorema anterior e do seguinte resultado (ver [4],p.143): se k for um corpo perfeito, então tôda extensão algébrica de k será uma extensão algébrica separável de k.

Seja W uma variedade algébrica irredutível do espaço linear S_n e ponhamos $\rho = \dim.W$, $\mathfrak{o} = Q(W/S_n)$, $\mathfrak{m} = \mathfrak{m}(W/S_n)$, $\mathfrak{M} = \mathfrak{M}(W/S_n)$, $\tau : \mathfrak{m} \longrightarrow \mathfrak{M}$, $\Delta = \mathfrak{J}(W) = k(\eta_1,\ldots,\eta_n)$; onde $(\eta_1,\ldots,\eta_n)$ é um ponto geral de W. Seja $\mathfrak{p} = \mathfrak{J}(W) = R_n.(f_1,\ldots,f_s)$ o ideal da variedade W. Temos $\mathfrak{m} = \mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(f_1,\ldots,f_s)$, portanto, existe uma base mínimal de $\mathfrak{m}$ formada por $n-\rho$ dos polinômios f_i; usando uma notação conveniente teremos $\mathfrak{m} = \mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(f_1,\ldots,f_{n-\rho})$. Pela proposição 7 e pelo teorema 8 do capítulo IV temos o

Teorema 9 - Uma condição necessária e suficiente para que $\mathfrak{J}(W)$ seja uma extensão transcendente separável de k é que a matriz $J(f_1,\ldots,f_{n-\rho};X_1,\ldots,X_n)$ tenha característica $n-\rho$ para $X=\eta$.

Quando a matriz $J(f_1,\ldots,f_{n-\rho};X_1,\ldots,X_n)$ tiver característica $n-\rho$ para $X=\alpha$ diremos que se trata do caso separável. Neste caso é fácil verificar que a matriz jacobiana $J(t_1,\ldots,t_{n-\rho};X_1,\ldots,X_n)$ onde $t_1,\ldots,t_{n-\rho}$ é um sistema de parâmetros uniformizadores de W, também tem característica $n-\rho$ para $X=\eta$. Consideremos agora $n-\rho$ elementos $u_1,\ldots,u_{n-\rho}$ de $\mathfrak{m}$ tais que a matriz jacobiana $J(u_1,\ldots,u_{n-\rho};X_1,\ldots,X_n)$ tenha característi-

ca para $X=\eta$. D'aqui resulta que $u_1,\ldots,u_{n-\rho}$ são parâmetros uniformizadores de W e que se trata do caso separável (a demonstração é análoga a dada para pontos). Estabelecemos assim o

Teorema 10 - Uma condição suficiente para que $n-\rho$ elementos $u_1,\ldots,u_{n-\rho}$ de $\mathfrak{m}=\mathfrak{m}(W/S_n)$ sejam parâmetros uniformizadores de W é que a matriz jacobiana $J(u;X)$ tenha característica $n-\rho$ para $X=\eta$. Se tivermos o caso separável a condição acima será também necessária.

Seja V uma variedade algébrica irredutível, de dimensão r, do espaço linear S_n e seja $\{F_1(X),\ldots,F_s(X)\}$ uma base do ideal $\mathfrak{J}(V)$ de R_n. Consideremos uma sub-variedade irredutível W de V e seja $(\eta_1,\ldots,\eta_n)$ um ponto geral de W. Com demonstração análoga a do teorema 8 chegaremos ao

Teorema 11 - Uma condição suficiente para que W seja uma sub-variedade simples de V é que a matriz jacobiana $J(F;X)$ tenha característica $n-r$ para $X=\eta$. Se tivermos o caso separável a condição acima é também necessária.

Corolário 6 - Suponhamos que k seja um corpo perfeito. Então a condição necessária e suficiente para que W seja uma sub-variedade simples de V é que a matriz jacobiana $J(F;X)$ tenha característica $n-r$ para $X=\eta$.

Êste corolário é uma consequência imediata do teorema anterior e do seguinte resultado, devido a F.K.Schmidt (ver [8], corolário 9): se k for um corpo perfeito, então tôda extensão finitamente gerada sôbre k é uma extensão transcendente separável de k.

Se k for um corpo perfeito segue-se que a característica da matriz jacobiana $J(F;X)$ para $X=\xi$ ($\xi_1,\ldots,\xi_n$ ponto geral de V) é $n-r$. Desta observação e dos corolários 5 e 6 resulta imediatamente que

Corolário 7 - Se k for um corpo perfeito, então os pontos singulares de V formam uma sub-variedade algébrica própria de V.

Corolário 8 - Se k for um corpo perfeito, então uma sub-variedade irredutível W de V é singular quando, e sòmente quando, todos os pontos de W são pontos singulares de V.

§ 3 - Critério das matrizes jacobianas mistas.

Seja $K = k(X_1,\ldots,X_n)$ um corpo de funções racionais de n indeterminadas $X_1,\ldots,X_n$ sôbre o corpo k de característica $p > 0$ e imperfeito. Seja $Z = (z_\alpha)_{\alpha \in A}$ uma p-base de k. Consideremos s elementos $f_1(X),\ldots,f_s(X)$ de K; todos os coeficientes de $f_1,\ldots,f_s$ pertencem a uma mesma extensão finita k_1 de k^p. Usando uma notação conveniente poremos: $k_1 = k^p(z_1,\ldots,z_m)$. A matriz $\|\partial f_i/\partial X_j,\ \partial f_i/\partial z_\nu\|$ $(i=1,\ldots,s;\ j=1,\ldots,n)$ de s linhas e n+m colunas é denominada matriz jacobiana mista de $f_1,\ldots,f_s$ em relação a $X_1,\ldots,X_n,z_1,\ldots,z_m$ e a indicaremos, abreviadamente, por $J(f;X,z)$.

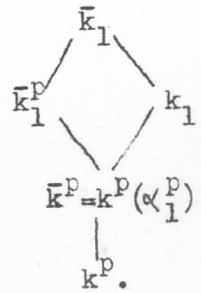
Seja $P(\alpha_1,\ldots,\alpha_n)$ um ponto do espaço linear S_n^k e consideremos os parâmetros locais canônicos $f_1(X_1)$, $f_2(X_1,X_2),\ldots,f_n(X_1,\ldots,X_n)$ do ponto $P(\alpha)$. Suponhamos que k_1 contenha todos os coeficientes dos polinômios f_i $(i=1,\ldots,n)$; o nosso objetivo é demonstrar que a matriz jacobiana mista $J(f;X,z)$ tem característica n no ponto P. Notemos que a característica desta matriz, no ponto P, não depende da extensão finita k_1 de k^p, que contém todos os coeficientes dos polinômios f_i (cap.IV, teorema 17). Em primeiro lugar consideraremos um caso especial, aquele em que os polinômios $f_1(X_1),\ldots,f_n(X_1,\ldots,X_n)$ só dependem de $X_1^p,\ldots,X_n^p$; neste caso temos $\partial f_i/\partial X_j = 0$ para $i,j = 1,\ldots,n$. Demonstraremos o

Teorema 12 - Se cada polinômio $f_i(X_1,\ldots,X_i)$ $(i=1,\ldots,n)$ só depender de $X_1^p,\ldots,X_i^p$ então a matriz jacobiana $J(f_1,\ldots,f_n;z_1,\ldots,z_m)$ terá característica n no ponto $P(\alpha)$ (isto é, para $X_i=\alpha_i$, $i=1,\ldots,n$).

Demonstração - Demonstraremos o teorema por indução sôbre n. Para $n=1$ o teorema afirma que nem tôdas as derivadas $\partial f_1/\partial z_j$, $j=1,\ldots,m$ são nulas no ponto $P(\alpha_1)$ de S_1. Suponhamos, por absurdo, que $\partial f_i/\partial z_j = 0$ para $X_1=\alpha_1$ e $j=1,\ldots,m$; então se $f_1(X_1) = X_1^{\varsigma_1 p} + a_1 X_1^{(\varsigma_1-1)p} + \ldots + a_{\varsigma_1-1}X_1^p + a_{\varsigma_1}$ $(a_i \in k_1)$

teremos $$\frac{\partial a_1}{\partial z_j}\alpha_1^{(\varsigma_1-1)p} + \ldots + \frac{\partial a_{\varsigma_1-1}}{\partial z_j}\alpha_1^p + \frac{\partial a_{\varsigma_1}}{\partial z_j} = 0, \quad j=1,\ldots,m.$$

Como $f_1(X_1)$ é o polinômio irredutível de α_1 sôbre k deveremos ter $\partial a_i/\partial z_j = 0$ para $i=1,\ldots,\varsigma_1$ e $j=1,\ldots,m$, portanto, teremos $\partial a_i/\partial z_\alpha = 0$ para $i=1,\ldots,\varsigma_1$ e para todo α de A. Pelo corolário 16 do capítulo IV virá $a_i \in k^p$ $(i=1,\ldots,\varsigma_1)$ e então o polinômio $f_1(X_1)$ não seria irredutível sôbre k. Isto prova o teorema para $n=1$; suponhamo-lo verificado para $n-1$. Ponhamos $\bar{k} = k(\alpha_1)$ e consideremos o espaço linear $S_{n-1}^{\bar{k}}$ e nele o ponto $\bar{P}(\alpha_2,\ldots,\alpha_n)$. Então os polinômios $\bar{\Phi}_i(X_2,\ldots,X_n) = f_i(\alpha_1,X_2,\ldots,X_n)$ $(i=2,\ldots,n)$ serão os parâmetros locais canônicos do ponto $\bar{P}$. Notemos que o corpo $\bar{k}_1 = k^p(\alpha_1^p,z_1,\ldots,z_m) = \bar{k}^p(z_1,\ldots,z_m)$ contém todos os coeficientes dos polinômios $\bar{\Phi}_i(X_2,\ldots,X_n)$ e que êstes polinômios só dependem de $X_2^p,\ldots,X_n^p$. Provaremos que o grau de imperfeição relativo de $\bar{k}_1$ sôbre $\bar{k}^p$ é igual a $m-1$; isto nos mostrará que existe uma p-base relativa de $\bar{k}_1$ sôbre $\bar{k}^p$ com $m-1$ dos elementos $z_1,\ldots,z_m$. Com efeito, temos as seguintes inclusões



D'aqui tiramos $[\bar{k}_1:k^p] = [\bar{k}_1:\bar{k}^p][\bar{k}^p:k^p] = [\bar{k}_1:k_1][k_1:k^p]$; mas

$[\bar{k}^p:k^p] = [\bar{k}:k]$, logo, $[\bar{k}_1:\bar{k}^p][\bar{k}:k] = [\bar{k}_1:k_1][k_1:k^p]$. Como $\bar{k}=k(\alpha_1)$ teremos $[\bar{k}:k] = \varsigma_1 = gr.f_1(X_1)$. Por hipótese temos $f_1(X_1) = \Phi_1(X_1^p)$, onde Φ_1 é irredutível sôbre k, portanto, Φ_1 é também irredutível sôbre k_1 ($\subset k$); mas $\bar{k}_1 = k_1(\sqrt[p]{\alpha_1})$ e $\Phi_1 \in k_1[X_1]$, logo, $[\bar{k}_1:k_1] = \varsigma_1/p = gr.\Phi_1$. Então teremos $[\bar{k}_1:\bar{k}^p]\varsigma_1 = \frac{\varsigma_1}{p}[k_1:k^p] = \frac{\varsigma_1}{p}.p^m$, de onde, $[\bar{k}_1:\bar{k}^p] = p^{m-1}$ o que prova a nossa afirmação. Podemos então supôr que, por exemplo, $\{z_2,\ldots,z_m\}$ seja uma p-base relativa de $\bar{k}_1$ sôbre $\bar{k}^p$. Em $\bar{k}_1$ estão definidas as derivações $\frac{\bar{\partial}}{\partial z_j}$ $(j=2,\ldots,m)$ sôbre $\bar{k}^p$ e tais que $\frac{\bar{\partial} z_i}{\partial z_j} = 0$ para $i,j = 2,\ldots,m$ e $j\neq i$ (cap.IV,§2.2). Notemos que se $x \in k_1$ então temos $\frac{\bar{\partial} x}{\partial z_j} = \frac{\partial x}{\partial z_j} + \frac{\partial x}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_j}$ $(j=2,\ldots,m)$ e como $f_1(\alpha_1) = 0$ também teremos $\left[\frac{\partial f_1}{\partial z_j} + \frac{\partial f_1}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_j}\right]_{X_1=\alpha_1} = 0$. Desta última relação e do primeiro caso examinado, n=1, resulta que $\frac{\partial f_1}{\partial z_1} \neq 0$ para $X_1 = \alpha_1$. A matriz $J(f;z)_{X=\alpha}$ tem a mesma característica que a matriz

$$\left\|\begin{array}{cccc} \frac{\partial f_1}{\partial z_1} & \frac{\partial f_1}{\partial z_2} + \frac{\partial f_1}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_2} & \cdots & \frac{\partial f_1}{\partial z_m} + \frac{\partial f_1}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_m} \\ \frac{\partial f_2}{\partial z_1} & \frac{\partial f_2}{\partial z_2} + \frac{\partial f_2}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_2} & & \frac{\partial f_2}{\partial z_m} + \frac{\partial f_2}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_m} \\ \cdots & \cdots\cdots & & \cdots\cdots \\ \frac{\partial f_n}{\partial z_1} & \frac{\partial f_n}{\partial z_2} + \frac{\partial f_n}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_2} & & \frac{\partial f_n}{\partial z_m} + \frac{\partial f_n}{\partial z_1}\frac{\bar{\partial} z_1}{\partial z_m} \end{array}\right\|_{X=\alpha}$$

ou, seja, que a matriz

$$\left\|\begin{array}{cccc} \frac{\partial f_1}{\partial z_1} & 0 & \cdots & 0 \\ \frac{\partial f_2}{\partial z_1} & \frac{\bar{\partial}\bar{\Phi}_2}{\partial z_2} & \cdots & \frac{\bar{\partial}\bar{\Phi}_2}{\partial z_m} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial f_n}{\partial z_1} & \frac{\bar{\partial}\bar{\Phi}_n}{\partial z_2} & \cdots & \frac{\bar{\partial}\bar{\Phi}_n}{\partial z_m} \end{array}\right\|_{X=\alpha}$$

Mas $\bar{J}(\overline{\Phi}_2,\ldots,\overline{\Phi}_n;z_2,\ldots,z_m)_{X=\alpha}$ tem característica n-1, pela hipótese de indução e como $\partial f_1/\partial z_1 \neq 0$ para $X_1=\alpha_1$, virá que $J(f;z)_{X=\alpha}$ tem característica n. (q.e.d.).

Teorema 13 - Sejam $f_1(X_1),\ldots,f_n(X_1,\ldots,X_n)$ os parâmetros locais canônicos de um ponto $P(\alpha_1,\ldots,\alpha_n)$ do espaço linear S_n sôbre k (k imperfeito). Então a matriz jacobiana mista $J(f_1,\ldots,f_n;X_1,\ldots,X_n,z_1,\ldots,z_m)$, onde $k_1=k^p(z_1,\ldots,z_m)$ contém todos os coeficientes dos polinômios $f_i(X_1,\ldots,X_i)$, tem característica n no ponto P.

Demonstração - Consideremos a matriz $J(f;X)$ e seja $n-\mu$ a sua característica no ponto $P(\alpha)$. Se $\mu = 0$ o teorema já está demonstrado; se $\mu = n$, segue-se que (pelas propriedades dos parâmetros locais canônicos) os polinômios $f_1,\ldots,f_n$ só dependem de $X_1^p,\ldots,X_n^p$ e d'aqui, pelo teorema anterior, resulta que $J(f;X,z)$ tem característica n no ponto P. Portanto, podemos supôr que $0 < \mu < n$. Usando uma notação conveniente (o que, possivelmente, acarretará uma mudança de nomes nas coordenadas de P, pois, os parâmetros locais canônicos foram introduzidos a partir de uma certa ordem nestas coordenadas) podemos supôr que a matriz $J(f_1,\ldots,f_n;X_{\mu+1},\ldots,X_n)$ tenha característica $n-\mu$ no ponto P. Como f_i é independente de $X_{i+1},\ldots,X_n$ teremos

$$(1) \qquad \left|J(f_{\mu+1},\ldots,f_n;X_{\mu+1},\ldots,X_n)\right|_{X=\alpha} \neq 0.$$

Mas

$$(2) \quad J(f_1,\ldots,f_n;X_1,\ldots,X_n) = \left\| \begin{matrix} J(f_1,\ldots,f_\mu;X_1,\ldots,X_n) & 0 \\ * & J(f_{\mu+1},\ldots,f_n;X) \end{matrix} \right\|$$

que tem característica $n-\mu$ no ponto P, portanto, pela (1), segue-se que $J(f_1,\ldots,f_\mu;X_1,\ldots,X_n)_{X=\alpha}$ deve ser a matriz nula, isto é, $\partial f_i/\partial X_j = 0$ $(i=1,\ldots,\mu;j=1,\ldots,n)$ no ponto P. Portanto, pelas propriedades 3) e 4) dos parâmetros locais canônicos do ponto P, teremos que f_i $(i=1,\ldots,\mu)$ depende sòmente de $X_1^p,\ldots,X_i^p$. Ora, os polinômios $f_1,\ldots,f_\mu$ são parâmetros locais canônicos do ponto $P_1(\alpha_1,\ldots,\alpha_\mu)$ de S_μ, portanto, pelo teorema 12, a matriz $J(f_1,\ldots,f_\mu;z_1,\ldots,z_m)$ tem característica μ para $X_j=\alpha_j$ $(j=1,\ldots,n)$.

Então teremos

$$J(f_1,\dots,f_m;X_1,\dots,X_m,z_1,\dots,z_m)=\left\|\begin{matrix} 0 & 0 & J(f_1,\dots,f_\mu;z_1,\dots,z_m) \\ * & J(f_{\mu+1},\dots,f_m;X_1,\dots,X_m) & J(f_{\mu+1},\dots,f_m;z_1,\dots,z_m)\end{matrix}\right\|$$

onde $\left|J(f_{\mu+1},\dots,f_n;X_1,\dots,X_n)\right|_{X=\alpha}\neq 0$ e

$J(f_1,\dots,f;z_1,\dots,z_m)_{X=\alpha}$ tem característica μ para $X=\alpha$. Isto nos mostra que a matriz $J(f_1,\dots,f_n;X_1,\dots,X_n,z_1,\dots,z_m)$ tem característica n no ponto $P(\alpha)$. (q.e.d.).

Corolário 9 - Seja $t_1,\dots,t_n$ $(t_i\in\Theta=Q(P/S_n))$ um sistema de parâmetros locais de um ponto P do espaço linear S_n. Então a matriz jacobiana mista $J(t;X,z)$ tem característica n no ponto P.

E' uma consequência imediata do teorema anterior e do fato que $t_i=\sum_{j=1}^{n}a_{ij}f_j$ $(i=1,\dots,n;a_{ij}\in\Theta)$, onde $|a_{ij}|\notin m(P/S_n)$ e $f_1,\dots,f_n$ são os parâmetros locais canônicos do ponto P.

Teorema 14 - Seja W uma variedade algébrica irredutível do espaço linear S_n e seja $t_1,\dots,t_{n-\rho}$ um sistema de parâmetros locais de W ($\rho=\dim.W$, $t_i\in\Theta=Q(W/S_n)$). Indiquemos por $k_1=k^p(z_1,\dots,z_m)$ o sub-corpo de k que se obtém de k^p acrescentando todos os coeficientes das funções racionais $t_1,\dots,t_{n-\rho}$. Nestas condições a matriz jacobiana mista $J(t_1,\dots,t_{n-\rho};X_1,\dots,X_n,z_1,\dots,z_m)$ tem característica $n-\rho$ em W (isto é, para $X_i=\eta_i$, onde (η) é o ponto geral de W).

Demonstração - Usando uma notação conveniente podemos supôr que $\eta_1,\dots,\eta_\rho$ sejam algèbricamente independentes sôbre k; identificaremos então η_i com X_i para $i=1,\dots,\rho$. Consideremos o espaço linear $S^{k^*}_{n-\rho}$ sôbre $k^*=k(X_1,\dots,X_\rho)$ e nele o ponto $W^*=(\eta_{\rho+1},\dots,\eta_n)$. Já sabemos que $\Theta=Q(W/S_n)=$ $=Q(W^*/S^{k^*}_{n-\rho})=\Theta^*$ e $m(W/S_n)=m(W^*/S^{k^*}_{n-\rho})=\Theta^*(t_1,\dots,t_{n-\rho})$.

Por um resultado de O.Teichmüller [1] temos que uma p-base de k é dada por $\{X_1,\ldots,X_\rho, Z=(z_\alpha)_{\alpha\in A}\}$, onde Z é a p-base de k que estamos considerando. Temos que o corpo $k_1=k^{*p}(X_1,..,X_\rho,z_1,\ldots,z_m)$ contém todos os coeficientes dos parâmetros locais $t_i^* = t_i^*(X_1,\ldots,X_\rho;X_{\rho+1},\ldots,X_n) = t_i$ $(i=1,\ldots,n-\rho)$ do ponto W^*. Portanto, pelo corolário 9, segue-se que a matriz jacobiana mista $J^*(t_1^*,\ldots,t_{n-\rho}^*;X_{\rho+1},\ldots,X_n,X_1,\ldots,X_\rho,z_1,\ldots,z_m)$ tem característica $n-\rho$ para $X_j=\eta_j$ $(j=\rho+1,\ldots,n)$, ou seja, a matriz jacobiana mista $J(t_1,\ldots,t_{n-\rho};X_1,\ldots,X_n,z_1,\ldots,z_m)$ tem característica $n-\rho$ em W. (q.e.d.).

Corolário 10 - Uma condição necessária e suficiente para que $n-\rho$ elementos $u_1,\ldots,u_{n-\rho}$ de $\mathfrak{m}=\mathfrak{m}(W/S_n)$ sejam parâmetros uniformizadores de W é que a matriz jacobiana mista $J(u;X,z)$ tenha característica $n-\rho$ em W (onde $k_1=k^p(z_1,\ldots,z_m)$ contém todos os coeficientes das funções racionais $u_1,\ldots,u_{n-\rho}$).

Demonstração - A condição necessária já foi demonstrada no teorema anterior. Demonstraremos que a condição é suficiente. Suponhamos, por absurdo, que $u_1,\ldots,u_{n-\rho}$ não sejam parâmetros uniformizadores de W; então existirá uma relação da forma $u_1 = \sum_{i=2}^{n-\rho} a_i u_i + u$, onde, $a_i \in \Theta$ e $u \in \mathfrak{m}^2$. D'aqui tiramos

$$\frac{\partial u_1}{\partial X_\varrho} \equiv \sum_{i=2}^{n-\rho} a_i \frac{\partial u_i}{\partial X_\varrho} \pmod{\mathfrak{m}} \quad \text{e} \quad \frac{\partial u_1}{\partial z_j} \equiv \sum_{i=2}^{n-\rho} a_i \frac{\partial u_i}{\partial z_j} \pmod{\mathfrak{m}}.$$ Mas

estas relações nos mostram que a matriz jacobiana mista $J(u;X,z)$ tem característica inferior a $n-\rho$ em W, contra a hipótese. (q.e.d.).

Pelo teorema 14 e pela demonstração da condição suficiente do corolário 10 resulta, imediatamente, que

---

(1) Se $K=k(X_1,\ldots,X_\rho)$ for uma extensão transcendente pura de k, uma p-base de K é dada por $Z \cup \{X_1,\ldots,X_\rho\}$ onde Z é uma p-base de k (ver [11]).

Corolário 11 - Uma condição necessária e suficiente para que s vectores $\tau u_1,\ldots,\tau u_s$ de $\mathfrak{M}(W/S_n)$ $(u_i \in \Theta = Q(W/S_n))$ sejam linearmente independentes sôbre $\Delta = \mathfrak{J}(W)$ é que a matriz jacobiana mista $J(u;X,z)$ tenha característica s em W (onde $k_1=k^p(z_1,\ldots,z_m)$ contém todos os coeficientes de $u_1,\ldots,u_s$).

Seja agora W uma sub-variedade algébrica irredutível de uma variedade algébrica irredutível V e consideremos uma base $\{F_1(X),\ldots,F_s(X)\}$ do ideal $\mathfrak{J}(V)$ de $R_n=k[X_1,\ldots,X_n]$. Seja $k_1=k^p(z_1,\ldots,z_m)$ o sub-corpo obtido de k^p acrescentando todos os coeficientes dos polinômios $F_1(X),\ldots,F_s(X)$, onde $\{z_1,\ldots,z_m\}$ é um sub-conjunto de uma p-base $Z=(z_\alpha)_{\alpha\in\Lambda}$ de k. Nestas condições demonstraremos o

Teorema 15 - Uma condição necessária e suficiente para que W seja uma sub-variedade simples de V é que a matriz jacobiana mista $J(F_1,\ldots,F_s;X_1,..,X_n,z_1,..,z_m)$ tenha característica n-r em W, onde r=dim.V.

Demonstração - Pelo teorema 5 resulta que W é simples quando, e sòmente quando, n-r dos vectores $\tau F_1,\ldots,\tau F_s$ (onde $\tau : \mathfrak{m}(W/S_n) \longrightarrow \mathfrak{M}(W/S_n)$) são linearmente independentes sôbre $\Delta = \mathfrak{J}(W)$. Indicaremos êstes vectores por $\tau F_1,\ldots,\tau F_{n-r}$; temos então que W é simples quando, e sòmente quando, $\tau F_1,\ldots,\tau F_{n-r}$ são linearmente independentes sôbre Δ e cada τF_j $(j=n-r+1,\ldots,s)$ depende linearmente de $\tau F_1,\ldots,\tau F_{n-r}$. Pelo corolário 11 resulta então que W é simples quando, e sòmente quando, a matriz jacobiana mista $J(F_1,\ldots,F_s;X_1,\ldots,X_n,z_1,\ldots,z_m)$ tem característica n-r em W. (q.e.d.).

Seja $(\xi_1,\ldots,\xi_n)$ o ponto geral de V, então a matriz jacobiana mista $J(F;X,z)$ tem característica n-r para $X=\xi$. Desta observação e do teorema 15 (aplicado para o caso em que W é um ponto) resultam os corolários:

Corolário 12 - O conjunto de todos os pontos singulares de V é uma sub-variedade algébrica própria de V.

Corolário 13 - Uma sub-variedade irredutível W de uma variedade algébrica irredutível V é uma sub-variedade singular de V quando, e sòmente quando, todos os pontos de W forem pontos singulares de V.

C A P I T U L O VI.

Sôbre as potências simbólicas de um ideal primo de um anel de polinômios.

§ 1 - Introdução.

Estudaremos neste capítulo o seguinte problema, sugerido pelo prof. O. Zariski: seja V uma variedade algébrica irredutível do espaço linear S_n^k; determinar o conjunto de todos os polinômios f de $R_n=k[X_1,\ldots,X_n]$ que verificam a condição: a) todo ponto de V é um ponto múltiplo de ordem pelo menos ρ, $\rho \geq 1$, da hipersuperfície algébrica $H = U(R_n.f)$. Se $\rho = 1$ o problema se reduzirá ao seguinte: dada uma variedade algébrica irredutível V, determinar o conjunto de todos os polinômios que se anulam sôbre V. O teorema dos zeros de Hilbert (cap.II,§2) nos diz que êste conjunto é o ideal primo que determina a variedade algébrica V. Se $\rho > 1$ demonstraremos o seguinte resultado: f satisfaz à condição a) quando, e sòmente quando, $f \in \mathfrak{p}^{(\rho)}$, onde $\mathfrak{p} = J(V)$. Portanto, o conjunto de todos os polinômios f de R_n que satisfazem à condição a) é a potência simbólica ρ-ésima de $\mathfrak{p}$, onde $\mathfrak{p} = J(V)$. Notando que $\mathfrak{p}^{(\rho)} \neq \mathfrak{p}^{(\rho+1)}$ (cap.I, teorema 19) seguir-se-á, em particular, o resultado: dada uma variedade algébrica irredutível V do espaço linear S_n existe, para cada inteiro ρ, $\rho \geq 1$, uma hipersuperfície algébrica H tal que a) H contém V; 2) todos os pontos de V são pontos múltiplos de ordem pelo menos ρ de V; c) existe, pelo menos, um ponto de V que é um ponto múltiplo de ordem ρ de H.

Como na teoria dos pontos simples de uma variedade algébrica (cap.V) distinguiremos dois casos: 1) o corpo base k é perfeito; 2) o corpo base k é imperfeito. O primeiro caso será estudado no §2 e o segundo no §3.

No §4 daremos uma nova demonstração de um teorema devido a O.Zariski, sôbre as funções de $J(V)$ (V variedade algébrica irredutível) que se anulam, com uma dada ordem, sôbre quasi todos os pontos de uma sub-variedade W de V.

Ainda neste parágrafo demonstraremos um lema que é

válido qualquer que seja o corpo base k. A situação de que trata êste lema é a seguinte: seja V uma variedade algébrica irredutível do espaço linear S_n^k ($V \neq \emptyset$) e seja $\mathfrak{p} = \mathfrak{J}(V)$ o ideal de V; consideremos um ponto simples P_o de V (cap.V, corolários 8 e 13) e ponhamos $\mathfrak{p}_o = \mathfrak{J}(P_o)$. O corolário 4 do capítulo V nos diz que existe um sistema de parâmetros uniformizadores $t_1,\ldots,t_n$ do ponto P_o, como ponto do espaço linear S_n, tal que $\mathfrak{m} = \mathfrak{o}.(t_1,\ldots,t_n)$ e $\mathfrak{o}.\mathfrak{p} = \mathfrak{o}.(t_1,\ldots,t_s)$, onde $\mathfrak{m} = \mathfrak{m}(P_o/S_n)$, $\mathfrak{o} = \mathfrak{Q}(P_o/S_n)$ e $s = n-r$, $r = \dim.V$. Nestas condições demonstraremos o

Lema 1 - Uma condição necessária e suficiente para que um elemento

$$\eta = \varphi_\nu(t_1,\ldots,t_s) = \sum_{\nu_1+\cdots+\nu_s=\nu} a_{(\nu_1,\ldots,\nu_s)} t_1^{\nu_1} \cdots t_s^{\nu_s}$$

de $\mathfrak{o}$, pertença exatamente à potência ν-ésima de $\mathfrak{p}^* = \mathfrak{o}.\mathfrak{p}$ é que nem todos os coeficientes $a_{(\nu)}$ de $\varphi_\nu(t)$ pertençam a $\mathfrak{p}^*$.

Demonstração - E' imediato que a condição é necessária. Suponhamos que nem todos os coeficientes $a_{(\nu)}$ de $\varphi_\nu(t)$ pertençam a $\mathfrak{p}^*$ mas que $\eta = \varphi_\nu(t)$ pertença a $\mathfrak{p}^{*\nu+1}$. Consideremos o anel de quocientes $\mathfrak{o}' = \mathfrak{o}_{\mathfrak{p}^*}$ (cap.I,§4); é fácil provar que $\mathfrak{o}' = \mathfrak{Q}(V/S_n)$. Temos $\mathfrak{o}'.\mathfrak{p}^* = \mathfrak{o}'.(t_1,\ldots,t_s) = \mathfrak{m}' = \mathfrak{m}(V/S_n)$ e $\mathfrak{o}'$ é um anel local regular (pelos teoremas 1 e 3 do capítulo V). De $\eta = \varphi_\nu(t) \in \mathfrak{p}^{*\nu+1}$ vem $\varphi_\nu(t) \in \mathfrak{m}'^{\nu+1}$, portanto, todos os coeficientes $a_{(\nu)}$ de $\varphi_\nu(t)$ estão em $\mathfrak{m}'$; mas $\mathfrak{m}' \cap \mathfrak{o} = \mathfrak{p}^*$ e $a_{(\nu)} \in \mathfrak{o}$, logo, todos os coeficientes $a_{(\nu)}$ de $\varphi_\nu(t)$ estão em $\mathfrak{p}^*$, contra a hipótese. Isto completa a demonstração do lema.

§2 - Resolução do problema quando o corpo base é perfeito.

2.1.

Seja V uma variedade algébrica irredutível do espaço linear S_n^k ($V \neq \emptyset$ e $V \neq S_n$). Neste parágrafo só consideraremos o caso em que o corpo base k é perfeito (isto é, ou k tem característica zero, ou, se a característica de k for p, $p > 0$, então

$k^p = k$). Seja P_o um ponto simples de V (já sabemos que existem pontos simples numa variedade algébrica - cap.V, corolário 8). Ponhamos $\mathfrak{p} = \mathfrak{J}(V)$, $\mathfrak{p}_o = \mathfrak{J}(P_o)$, $\mathfrak{o} = \mathfrak{Q}(P_o/S_n)$, $\mathfrak{m} = \mathfrak{m}(P_o/S_n)$, $r = \dim.V$, $s = n-r$ e $\mathfrak{p}^* = \mathfrak{o}.\mathfrak{p}$. Consideremos um sistema de parâmetros locais $t_1,\ldots,t_n$ do ponto P_o, como ponto do espaço linear S_n, tal que $\mathfrak{p}^* = \mathfrak{o}.(t_1,\ldots,t_s)$ (cap.V, corolário 4). No corpo $K = k(X_1,\ldots,X_n)$ estão definidas as derivações parciais em relação a $X_1,\ldots,X_n$ e sôbre k (cap.IV,§4); estas derivações deixam invariante o anel $\mathfrak{o}$ (cap.IV,prop.16). Consideremos um elemento ω de $\mathfrak{o}$, portanto, ω é uma função racional (cujo denominador não pertence a $\mathfrak{p}_o$) de $X_1,\ldots,X_n$, com coeficientes em k: $\omega = F(X_1,\ldots,X_n)$. Seja

$$F(X+u) = F(X) + F_1(u) + \ldots + F_\nu(u) + \ldots$$

o desenvolvimento de Taylor do elemento ω ; temos:

$$F_\nu(u) = \sum_{\nu_1+\ldots+\nu_m=\nu} \frac{\partial^\nu F(X)}{\partial X_1^{\nu_1}\ldots\partial X_n^{\nu_m}}\, u_1^{\nu_1}\ldots u_n^{\nu_m}.$$

Suponhamos que ω pertença à $\mathfrak{p}^{*\nu}$ ($\nu \geq 1$); pela proposição 19 do cap.IV teremos

$$\frac{\partial^i F(X)}{\partial X_1^{i_1}\ldots\partial X_n^{i_n}} \in \mathfrak{p}^*$$

para $i=1,\ldots,\nu-1$ e para tôdas as soluções inteiras não negativas da equação $i_1+\ldots+i_n=i$. Exprimiremos, abreviadamente, esta propriedade por

(1) $\qquad F_i(u) \equiv 0 \pmod{\mathfrak{p}^*}, \quad i=1,\ldots,\nu-1.$

Suponhamos agora que $F(X) = a(X)f(X)$ com $a(X) \in \mathfrak{o}$ e $f(X) \in \mathfrak{p}^{*\nu}$ ($\nu \geq 1$). Afirmamos que

$$F_\nu(u) \equiv a(X)\, f_\nu(u) \pmod{\mathfrak{p}^*},$$

onde $f_\nu(u)$ indica a forma de grau ν do desenvolvimento de Taylor do elemento $f(X)$. Com efeito, sejam $f(X+u) = f(X) + f_1(u) + \ldots + f_\nu(u) + \ldots$ e $a(X+u) = a(X) + a_1(u) + \ldots + a_\nu(u) + \ldots$ os desenvolvimentos de Taylor de $f(X)$ e $a(X)$, respectivamente. Temos:

$$F_\nu(u) = \sum_{j=0}^{\nu} a_j(u)\, f_{\nu-j}(u),$$

onde $a_0(u) = a(X)$ e $f_0(u) = f(X)$. Mas, pela relação (1), aplicada ao elemento $f_{\nu-j}(u)$, temos $f_{\nu-j}(u) \equiv 0 \pmod{\mathfrak{p}^*}$ para $j=1,\ldots,\nu$, logo

$$F_\nu(u) \equiv a(X)\, f_\nu(u) \pmod{\mathfrak{p}^*}.$$

Desta propriedade resulta a seguinte: seja

$$F(X) = \sum_{j_1+\cdots+j_s=\nu} a_{(j_1,\ldots,j_s)}(X)\, t_1^{j_1} \ldots t_s^{j_s}$$

um elemento de $\mathfrak{p}^{*\nu}$, onde $a_{(j)}(X) \in \mathfrak{o}$, então

$$(2)\quad F_\nu(u) \equiv \sum_{\nu_1+\cdots+\nu_m=\nu} \left(\sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X)\, \frac{\partial^\nu T_{(j)}}{\partial X_1^{\nu_1} \ldots \partial X_n^{\nu_m}} \right) u_1^{\nu_1} \ldots u_n^{\nu_m} \pmod{\mathfrak{p}^*}$$

onde $T_{(j)} = T_{(j_1,\ldots,j_s)} = t_1^{j_1} \ldots t_s^{j_s}$.

Temos

$$(3)\quad T_{(j)}(X+u) = T_{(j)}(X) + \sum_{i=1}^{n} \frac{\partial T_{(j)}}{\partial X_i}\, u_i + \ldots +$$

$$+ \sum_{\nu_1+\cdots+\nu_m=\nu} \frac{\partial^\nu T_{(j)}}{\partial X_1^{\nu_1} \ldots \partial X_n^{\nu_m}}\, u_1^{\nu_1} \ldots u_n^{\nu_m} + \ldots .$$

Multiplicando ambos os membros de (3) por $a_{(j)}(X)$ e somando as relações assim obtidas em relação a tôdas as soluções inteiras não negativas da equação $j_1+\ldots+j_s=\nu$ virá:

$$\sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X)\, T_{(j)}(X+u) = F(X) + \sum_{j_1+\cdots+j_s=\nu} \sum_{i=1}^{n} \left(a_{(j)}(X) \frac{\partial T_{(j)}}{\partial X_i}\, u_i \right) +$$

$$+ \ldots + \sum_{j_1+\cdots+j_s=\nu} \left(\sum_{\nu_1+\cdots+\nu_m=\nu} a_{(j)}(X)\, \frac{\partial^\nu T_{(j)}}{\partial X_1^{\nu_1} \ldots \partial X_n^{\nu_m}}\, u_1^{\nu_1} \ldots u_n^{\nu_m} \right) + \ldots .$$

Pondo $F(X) = H_\nu(t_1(X),\ldots,t_s(X))$, poderemos escrever esta última relação sob a forma

$$(4)\qquad H_\nu(t_1(X+u),\ldots,t_s(X+u)) = H_\nu(t) + \sum_{i=1}^{n}\Big(\sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X)\frac{\partial T_{(j)}}{\partial X_i}\Big)u_i +$$

$$+ \cdots + \sum_{\nu_1+\cdots+\nu_m=\nu}\Big(\sum_{j_1+\cdots+j_s=\nu} a_{(j)}\,\frac{\partial^\nu T_{(j)}}{\partial X_1^{\nu_1}\ldots\partial X_n^{\nu_m}}\Big)u_1^{\nu_1}\ldots u_n^{\nu_m} + \cdots .$$

Esta fórmula nos mostra que a forma de grau ν do desenvolvimento de $H_\nu(t_1(X+u),\ldots,t_s(X+u))$ (que é obtido de $H_\nu(t_1(X),\ldots,t_s(X))$ dando os "acréscimos" u sòmente às varíaveis X que comparecem em $t_1(X),\ldots,t_s(X)$ e deixando os coeficientes $a_{(j)}(X)$ "constantes") é igual à forma de grau ν que comparece no segundo membro da relação (2). Calcularemos, módulo $\wp^*$, a forma de grau ν de $H_\nu(t_1(X+u),\ldots,t_s(X+u))$ por um outro processo. Temos:

$$t_j(X+u) = t_j(X) + \sum_{i=1}^{n}\frac{\partial t_j}{\partial X_i}u_i + \cdots +$$

$$+ \sum_{i_1+\cdots+i_n=\nu}\frac{\partial^\nu t_j}{\partial X_1^{i_1}\ldots\partial X_n^{i_n}}u_1^{i_1}\ldots u_n^{i_n} + \cdots ;$$

pondo

$$V_j = \sum_{i=1}^{n}\frac{\partial t_j}{\partial X_i} + \cdots + \sum_{i_1+\cdots+i_n=\nu}\frac{\partial^\nu t_j}{X_1^{i_1}\ldots X_n^{i_n}}u_1^{i_1}\ldots u_n^{i_n} + \ldots;$$

virá

$$t_j(X+u) = t_j(X) + V_j$$

e teremos

$$(5)\qquad H_\nu(t_1(X+u),\ldots,t_s(X+u)) = H_\nu(t_1(X)+V_1,\ldots,t_s(X)+V_s).$$

Mas sendo $H_\nu(t_1,\ldots,t_s)$ um polinômio em $t_1,\ldots,t_s$ (com coeficientes em $\mathfrak{C}$) o desenvolvimento do segundo membro de (5) será da forma

$$H_\nu(t_1(X)+V_1,\ldots,t_s(X)+V_s) = H_\nu(t_1,\ldots,t_s) +$$

$$+ H_{\nu,1}(V_1,\ldots,V_s) + \cdots + H_{\nu,\nu}(V_1,\ldots,V_s),$$

onde $H_{\nu,j}(V_1,\ldots,V_s)$ $(1 \leq j \leq \nu)$ é uma forma de grau j em $V_1,\ldots,V_s$ com coeficientes em $\mathfrak{C}$. Consideremos o polinômio

$$H_\nu(Z_1,\ldots,Z_s) = \sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X)\, Z_1^{j_1} \ldots Z_s^{j_s}$$

nas indeterminadas $Z_1,\ldots,Z_s$, obtido de $H_\nu(t_1,\ldots,t_s)$ substituindo t_j por Z_j $(j=1,\ldots,s)$. Teremos

$$H_{\nu,j}(V_1,\ldots,V_s) = \sum_{\sigma_1+\cdots+\sigma_s=j} \left(\frac{H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}}\right)_{Z=t} V_1^{\sigma_1} \ldots V_s^{\sigma_s}.$$

Mas $H_\nu(t_1,\ldots,t_s) \in \mathfrak{p}^{*\nu}$ portanto

$$\left(\frac{\partial^j H(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}}\right)_{Z=t} \in \mathfrak{p}^* \quad \text{para} \quad \sigma_1+\ldots+\sigma_s=j < \nu.$$

Então a forma de grau ν do desenvolvimento de $H_\nu(t_1(X+u),\ldots,t_s(X+u))$ (ver (4)) é côngrua, módulo $\mathfrak{p}^*$, à forma

$$\sum_{\nu_1+\cdots+\nu_n=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}}\right)_{Z=t} \left(\sum_{i=1}^n \frac{\partial t_1}{\partial X_i} u_i\right)^{\sigma_1} \ldots \left(\sum_{i=1}^n \frac{\partial t_s}{\partial X_i} u_i\right)^{\sigma_s},$$

portanto, pondo $V'_j = \sum_{i=1}^n \frac{\partial t_j}{\partial X_i} u_i$ $(j=1,\ldots,s)$, teremos

$$\sum_{\nu_1+\cdots+\nu_m=\nu} \left(\sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X) \frac{\partial^\nu T_{(j)}}{\partial X_1^{\nu_1} \ldots \partial X_n^{\nu_m}}\right) u_1^{\nu_1} \ldots u_n^{\nu_m} \equiv$$

$$\equiv \sum_{\sigma_1+\cdots+\sigma_s=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}}\right)_{Z=t} V_1'^{\sigma_1} \ldots V_s'^{\sigma_s} \quad (\text{mod. } \mathfrak{p}^*).$$

Pela fórmula (2) virá:

$$(6) \qquad F_\nu(u) \equiv \sum_{\sigma_1+\cdots+\sigma_s=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}}\right)_{Z=t} V_1'^{\sigma_1} \ldots V_s'^{\sigma_s} \quad (\text{mod. } \mathfrak{p}^*),$$

onde

$$V'_j = \sum_{i=1}^n \frac{\partial t_j}{\partial X_i} u_i \quad (j=1,\ldots,s).$$

Observando que $\mathfrak{o}/\mathfrak{p}^* = Q(P/V)$, poderemos escrever a (6) sob a for-

ma

$$F_\nu(u)_{X=\xi} = \sum_{\sigma_1+\cdots+\sigma_s=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{\substack{Z=t \\ X=\xi}} (V_1'^{\sigma_1} \ldots V_s'^{\sigma_s})_{X=\xi}.$$

Mas

$$\left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{Z=t} = a_{(\sigma_1,\ldots,\sigma_s)}(X)$$

e pondo

$$U_j = (V_j')_{X=\xi} = \sum_{i=1}^{n} \left(\frac{\partial t_j}{\partial X_i}\right)_{X=\xi} u_i$$

teremos

$$(7) \qquad F_\nu(u)_{X=\xi} = \sum_{\sigma_1+\cdots+\sigma_s=\nu} a_{(\sigma_1,\ldots,\sigma_s)}(\xi)\, U_1^{\sigma_1} \ldots U_s^{\sigma_s}.$$

Portanto, a forma $F_\nu(u)_{X=\xi}$ é obtida da forma

$$\sum_{\sigma_1+\cdots+\sigma_s=\nu} a_{(\sigma)}(\xi)\, U_1^{\sigma_1} \ldots U_s^{\sigma_s}$$

pela transformação linear

$$(8) \qquad U_j = \sum_{i=1}^{n} \left(\frac{\partial t_j}{\partial X_i}\right)_{X=\xi} u_i \qquad (j=1,\ldots,s).$$

A matriz $\left\| \frac{\partial t_j}{\partial X_i} \right\|$ $(i,j=1,\ldots,n)$ tem característica n no ponto P_o (cap.V, teorema 7), portanto, a matriz $\left\| \frac{\partial t_j}{\partial X_i} \right\|$ $(i=1,\ldots,n;$ $j=1,\ldots,s)$ terá característica máxima s para $X=\xi$, logo a transformação linear (7) é não singular. D'aqui tiramos o seguinte resultado: se a forma (em $U_1,\ldots,U_s$) do segundo membro de (7) for diferente de zero também a sua transformada $F_\nu(u)_{X=\xi}$, pela transformação linear (8), será diferente de zero. Demonstraremos o seguinte lema:

Lema 2 - Seja

$$F(X_1,\ldots,X_n) = H_\nu(t_1,\ldots,t_s) = \sum_{j_1+\ldots+j_s=\nu} a_{(j)}(X)\, t_1^{j_1} \ldots t_s^{j_s}$$

uma forma de grau ν em $t_1,\ldots,t_s$, com coeficientes $a_{(j)}(X)$ em $\mathfrak{S} = Q(P_o/S_n)$, mas nem todos em $\mathfrak{p}^*$; então, nem tôdas as derivadas parciais de $F(X)$, de ordem ν, estão em $\mathfrak{p}^*$.

Demonstração - Usaremos as mesmas notações anteriores. Pela proposição 17 do capítulo IV segue-se que nem tôdas as derivadas parciais, de ordem ν, de $H_\nu(Z_1,\ldots,Z_s)$, em relação a $Z_1,\ldots,Z_s$, estão em $\mathfrak{p}^*$ (pois nem todos os coeficientes $a_{(j)}(X)$ estão em $\mathfrak{p}^*$ pela lema 1). Portanto a forma

$$\sum_{\sigma_1+\ldots+\sigma_s=\nu} a_{(\sigma)}(\xi)\, U_1^{\sigma_1} \ldots U_s^{\sigma_s}$$

é diferente de zero; então, pelo último resultado que estabelecemos acima, a sua transformada $F_\nu(u)_{X=\xi}$, pela transformação linear (8), não é nula. D'aqui resulta que nem tôdas as derivadas parciais, de ordem ν, de $F(X)$ estão em $\mathfrak{p}^*$. (q.e.d.).

2.2.

Seja S_n^k o espaço linear de n dimensões sôbre um corpo perfeito k. Consideremos um polinômio f, $f \neq 0$ e $gr.f > 0$, de $R_n = k[X_1,\ldots,X_n]$; a variedade algébrica do ideal $\mathfrak{a} = R_n.f$ é denominada hipersuperfície algébrica. Pelo teorema dos ideais principais segue-se que tôdas as componentes irredutíveis de $\mathfrak{V}(\mathfrak{a})$ têm dimensão n-1.

Daremos as seguintes definições

Definição 1 - Diremos que um ponto $P(\alpha)$, do espaço linear S_n, é um ponto múltiplo de ordem pelo menos ρ, $\rho \geq 1$, da hipersuperfície algébrica $H = \mathfrak{V}(R_n.f)$ quando, e sòmente quando, for verificada a condição: tôdas as derivadas par-

ciais de ordens $0,1,\ldots,\rho-1$ de f, em relação a $X_1,\ldots,X_n$, se anulam em P, isto é,

$$\left(\frac{\partial^i f}{\partial X_1^{i_1}\ldots\partial X_n^{i_n}}\right)_{X=\alpha} = 0,$$

para $i=0,1,\ldots,\rho-1$ e para tôdas as soluções inteiras não negativas da equação $i_1+\ldots+i_n=i$.

Definição 2 - Diremos que um ponto $P(\alpha)$, do espaço linear S_n, é um ponto múltiplo de ordem ρ, $\rho \geq 1$, da hipersuperfície algébrica $H = V(R_n.f)$ quando, e sòmente quando, forem verificadas as condições: 1) $P(\alpha)$ é um ponto múltiplo de ordem pelo menos ρ de H; 2) existe, pelo menos, uma derivada parcial de ordem ρ de f, em relação a $X_1,\ldots,X_n$, que não se anula no ponto $P(\alpha)$.

Passaremos agora a resolver o problema proposto na introdução dêste capítulo. Demonstraremos o seguinte

Teorema 1 - Um polinômio $F(X)$ de $R_n=k[X_1,\ldots,X_n]$ (k perfeito) pertence à potência simbólica $\mathfrak{p}^{(\rho)}$, $\rho \geq 1$, de um ideal primo $\mathfrak{p}$ de R_n, quando, e sòmente quando, tôdas as derivadas parciais de ordens $0,1,\ldots,\rho-1$ de f pertencem a $\mathfrak{p}$.

Demonstração - O teorema é imediato se $\mathfrak{p} = (0)$, ou, se $\mathfrak{p} = R_n$, ou, se $\rho = 1$. Suponhamos então que $\mathfrak{p} \neq (0)$, $\mathfrak{p} \neq R_n$ e $\rho > 1$. Seja Θ_1 o anel de quocientes de R_n em relação ao ideal $\mathfrak{p}$ e ponhamos $\mathfrak{P} = \Theta_1.\mathfrak{p}$. Pela proposição 30 do capítulo I temos $\mathfrak{P}^\rho \cap R_n = \mathfrak{p}^{(\rho)}$. Se $F(X) \in \mathfrak{p}^{(\rho)}$ teremos $F(X) \in \mathfrak{P}^\rho$. Pelas proposições 15 e 19 do capítulo IV temos

$$\frac{\partial^i F}{\partial X_1^{i_1} \dots \partial X_n^{i_n}} \in R_n \qquad e \qquad \frac{\partial^i F}{\partial X_1^{i_1} \dots \partial X_n^{i_n}} \in \mathfrak{P}$$

para $0 \leq i = i_1+\dots+i_n < \rho$. Portanto

$$\frac{\partial^i F}{\partial X_1^{i_1} \dots \partial X_n^{i_n}} \in \mathfrak{P} \cap R_n = \mathfrak{p}$$

para $i=0,1,\dots,\rho-1$ e para tôdas as soluções inteiras não negativas da equação $i_1+\dots+i_n=i$. Isto demonstra a condição necessária. Suponhamos agora que tôdas as derivadas parciais de ordens $0,1,\dots,\rho-1$ de F pertençam a $\mathfrak{p}$ e que $\rho > 1$ (se $\rho = 1$ a condição suficiente nada mais é do que o teorema dos zeros de Hilbert), $\mathfrak{p} \neq (0)$ e $\mathfrak{p} \neq R_n$. Seja $V = \mathcal{V}(\mathfrak{p}) \subset S_n$ e consideremos um ponto simples P_o de V (cap.V, corolário 8); ponhamos $\mathcal{O} = Q(P_o/S_n)$, $\mathfrak{m} = \mathfrak{m}(P_o/S_n)$ e $\mathfrak{p}^* = \mathcal{O}.\mathfrak{p}$. Pelo corolário 4 do capítulo V existe um sistema de parâmetros uniformizadores $t_1,\dots,t_n$ do ponto P_o, como ponto do espaço linear S_n, tal que $\mathfrak{p}^* = \mathcal{O}.(t_1,\dots,t_s)$, $\mathfrak{m} = \mathcal{O}.(t_1,\dots,t_n)$, onde $s = n-r$ e $r = \dim.V$. Pela proposição 31 do capítulo I teremos $\mathfrak{p}^{*(\rho)} \cap R_n = \mathfrak{p}^{(\rho)}$, portanto, o elemento $F(X)$, de R_n, pertencerá a $\mathfrak{p}^{(\rho)}$ quando, e sòmente quando, $F(X) \in \mathfrak{p}^{*(\rho)}$. Mas $\mathfrak{p}^{*\rho} \subset \mathfrak{p}^{*(\rho)}$, portanto, se demonstrarmos que $F(X) \in \mathfrak{p}^{*\rho}$ teremos também $F(X) \in \mathfrak{p}^{*(\rho)}$ e então $F(X) \in \mathfrak{p}^{(\rho)}$. De $\bigcap_{\mu=0}^{\infty} \mathfrak{p}^{*\mu} = (0)$ (cap.I, teorema 15) segue-se que $F(X)$ pertence exatamente a uma potência $\mathfrak{p}^{*\mu}$ de $\mathfrak{p}^*$, isto é, $F(X) \in \mathfrak{p}^{*\mu}$ e $F(X) \notin \mathfrak{p}^{*\mu+1}$ (ainda mais temos $\mu \geq 1$, pois, por hipótese, $F(X) \in \mathfrak{p} < \mathfrak{p}^*$). Portanto, $F(X)$ pode ser escrito como uma forma de grau μ em $t_1,\dots,t_s$, com coeficientes em $\mathcal{O}$, mas nem todos em $\mathfrak{p}^*$ (lema 1):

$$F(X) = \sum_{\mu_1+\dots+\mu_s=\mu} a_{(\mu_1,\dots,\mu_s)}(X)\, t_1^{\mu_1} \dots t_s^{\mu_s},$$

$a_{(\mu_1,\dots,\mu_s)}(X) \in \mathcal{O}$ e nem todos os coeficientes $a_{(\mu)}(X)$ estão em $\mathfrak{p}^*$. Pelo lema 2 resulta que nem tôdas as derivadas parciais, de ordem μ, de $F(X)$, estão em $\mathfrak{p}^*$ e, pela proposição 19 do capítulo IV, tôdas as derivadas parciais de ordens $1,2,\dots,\mu-1$ de $F(X)$ estão em $\mathfrak{p}^*$. Mas, por hipótese, tôdas as derivadas parciais de ordens

$1,2,\ldots,\rho-1$ de $F(X)$ estão em $\wp^*$, portanto, teremos $\mu \geq \rho$ e então $F(X) \in \wp^{*\mu} \subset \wp^{*\rho}$. Isto completa a demonstração do teorema 1.

Dêste teorema e da definição 1 resulta o

Corolário 1 - Seja V uma variedade algébrica irredutível do espaço linear S_n^k (k perfeito e $V \neq S_n$) e ponhamos $\wp = \mathfrak{J}(V) \subset R_n$. Então o conjunto formado por zero e por todos os polinômios f de R_n, $f \neq 0$, que verificam a condição: "todo ponto de V é um ponto múltiplo de ordem pelo menos ρ, $\rho \geq 1$, da hipersuperfície algébrica $H = \mathfrak{V}(R_n.f)$", é a potência simbólica ρ-ésima de $\wp$.

Êste corolário nos dá a solução do problema proposto na introdução dêste capítulo, no caso em que o corpo base k é perfeito.

Definição 3 - Seja V uma variedade algébrica irredutível do espaço linear S_n^k (k perfeito, $V \neq \emptyset$ e $V \neq S_n$) e seja H uma hipersuperfície algébrica do S_n. Diremos que V é uma sub-variedade **múltipla** de ordem ρ ($\rho \geq 1$) de H se estiverem verificadas as condições:
1) todo ponto de V é um ponto múltiplo de ordem pelo menos ρ de H;
2) existe pelo menos um ponto de V que é ponto múltiplo de ordem ρ de H.

Do corolário 1 e da relação $\wp^{(\rho)} \neq \wp^{(\rho+1)}$ (cap.I, teorema 19), onde $\wp = \mathfrak{J}(V)$ resultam os seguintes corolários:

Corolário 2 - Seja V uma variedade algébrica irredutível do espaço linear S_n^k (k perfeito, $V \neq \emptyset$ e $V \neq S_n$); então existe uma hipersuperfície algébrica H tal que V seja uma sub-variedade múltipla de ordem ρ, $\rho \geq 1$, de H.

Corolário 3 - Seja V uma sub-variedade irredutível de uma hipersuperfície algébrica H e suponhamos que V seja uma sub-variedade múltipla de ordem ρ ($\rho \geq 1$) de H. Então os pontos de V que são pontos múltiplos de ordem maior do que ρ de H formam uma sub-variedade algébrica própria de V.

Seja V uma variedade algébrica irredutível do espaço linear S_n^k (k perfeito) e consideremos a família $(\mathfrak{p}_\alpha)_{\alpha \in A}$ (onde A é um conjunto de índices) de todos os ideais máximais $\mathfrak{p}_\alpha$ de R_n que contêm $\mathfrak{p} = \mathfrak{J}(V)$. Sendo $\mathfrak{p}_\alpha$ um ideal máximal temos $\mathfrak{p}_\alpha^\rho = \mathfrak{p}_\alpha^{(\rho)}$, então, do teorema 1 segue-se o

Corolário 4 - $\bigcap_{\alpha \in A} \mathfrak{p}_\alpha^\rho = \mathfrak{p}^{(\rho)}$.

Examinaremos agora o mesmo problema para uma variedade algébrica qualquer V (não necessàriamente irredutível). Temos $V = \mathfrak{V}(\mathfrak{m})$, onde $\mathfrak{m}$ é um ideal do anel de polinômios $R_n = k[X_1, \ldots, X_n]$ (k perfeito), e $\mathfrak{J}(V) = \text{Rad. } \mathfrak{m}$ (teorema dos zeros de Hilbert), portanto, $\mathfrak{J}(V)$ é igual à intersecção dos ideais primos isolados de $\mathfrak{m}$. Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ êstes ideais e ponhamos $\mathfrak{m}^{(\rho)} = \mathfrak{p}_1^{(\rho)} \cap \ldots \cap \mathfrak{p}_h^{(\rho)}$ ($\rho \geq 1$). As variedades algébricas dos ideais $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ são as componentes irredutíveis (cap.II, §3) de V; precisamente, pondo $V_i = \mathfrak{V}(\mathfrak{p}_i)$ (i=1,...,h) segue-se que $V = V_1 \cup \ldots \cup V_h$ é a decomposição normal da variedade V. Seja f, $f \neq 0$, um polinômio de R_n; então $f \in \mathfrak{m}^{(\rho)}$ quando, e sòmente quando, $f \in \mathfrak{p}_i^{(\rho)}$ (i=1,...,h). Portanto, pelo teorema 1, teremos:

Corolário 5 - Um polinômio f de $R_n = k[X_1,\ldots,X_n]$ (k perfeito) pertence ao ideal $\mathfrak{a}^{(\rho)} = \mathfrak{p}_1^{(\rho)} \cap \ldots \cap \mathfrak{p}_h^{(\rho)}$ ($\rho \geq 1$; $\mathfrak{p}_1,\ldots,\mathfrak{p}_h$ são os ideais primos isolados de $\mathfrak{a}$) quando, e sòmente quando, tôdas as derivadas parciais de ordens $0,1,\ldots,\rho-1$ de f pertencerem ao ideal $\mathfrak{a}$.

Observando que todo ponto de V é um ponto múltiplo de ordem pelo menos ρ, $\rho \geq 1$, de uma hipersuperfície algébrica $H = \mathcal{V}(R_n.f)$, $f \in R_n$, $f \neq 0$ e $gr.f > 0$, quando, e sòmente quando, todo ponto de cada componente irredutível V_i ($1 \leq i \leq h$) de V é ponto múltiplo de ordem pelo menos ρ de H, obteremos, pela aplicação do corolário 1 o seguinte

Corolário 6 - Seja $V = \mathcal{V}(\mathfrak{a})$ uma variedade algébrica do espaço linear S_n^k (k perfeito, $V \neq \emptyset$ e $V \neq S_n$). Então o conjunto formado por zero e por todos os polinômios f de R_n, $f \neq 0$, que vericam à condição: "todo ponto de V é um ponto múltiplo de ordem pelo menos ρ, $\rho \geq 1$, da hipersuperfície algébrica $H = \mathcal{V}(R_n.f)$" é o ideal $\mathfrak{a}^{(\rho)} = \mathfrak{p}_1^{(\rho)} \cap \ldots \cap \mathfrak{p}_n^{(\rho)}$, onde $\mathfrak{p}_1,\ldots,\mathfrak{p}_h$ são os ideais primos isolados de $\mathfrak{a}$.

Finalmente, seja $(\mathfrak{p}_\alpha)_{\alpha \in A}$ a família de todos os ideais máximais de R_n que contêm o ideal $\mathfrak{J}(V)$; pelo corolário 4, teremos:

Corolário 7 - $\bigcap_{\alpha \in A} \mathfrak{p}_\alpha^{\rho} = \mathfrak{a}^{(\rho)} = \mathfrak{p}_1^{(\rho)} \cap \ldots \cap \mathfrak{p}_h^{(\rho)}$.

§ 3 - Resolução do problema quando o corpo base é imperfeito.

3.1.

Neste parágrafo só consideraremos o caso em que o corpo base k é imperfeito (isto é, k tem característica $p > 0$ e $k^p \neq k$). Seja $Z = (z_\alpha)_{\alpha \in A}$ uma p-base (cap.IV,§2) de k. No corpo $K = k(X_1,\ldots,X_n) = k^p(X_1,\ldots,X_n;(z_\alpha)_{\alpha\in A})$ estão definidas as derivações parciais mistas (cap.IV,§5) em relação a $X_1,\ldots,X_n$ (sôbre k) e em relação aos elementos z_α (sôbre k^p) da p-base Z. Seja V uma variedade algébrica irredutível do espaço linear S_n^k $(V \neq \emptyset)$ e consideremos um ponto simples P_o de V (já sabemos que existem pontos simples numa variedade algébrica — cap.V, corolário 12). Ponhamos $\mathfrak{p} = \mathfrak{J}(V)$, $\mathfrak{p}_o = \mathfrak{J}(P_o)$, $\mathfrak{o} = \mathfrak{o}(P_o/S_n)$, $\mathfrak{m} = \mathfrak{m}(P_o/S_n)$, $r = \dim.V$, $s = n - r$ e $\mathfrak{p}^* = \mathfrak{o}.\mathfrak{p}$. Consideremos um sistema de parâmetros locais $t_1,\ldots,t_n$, do ponto P_o, como ponto do espaço linear S_n, tal que $\mathfrak{p}^* = \mathfrak{o}.(t_1,\ldots,t_s)$ (cap.V, corolário 4). As derivações parciais mistas deixam invariante os aneis $R_n = k[X_1,\ldots,X_n]$ e $\mathfrak{o}$ (cap.IV, proposições 23 e 24). No que se segue iremos considerar sòmente um número finito de funções racionais em $X_1,\ldots,X_n$, com coeficientes em k, portanto, só teremos um número finito de coeficientes pertencentes a k; êstes coeficientes podem ser expressos como polinômios num número finito de elementos z_α da p-base Z, com coeficientes em k^p. Indicaremos por $M = \{z_1,\ldots,z_m\}$ um sub-conjunto finito de Z tal que o corpo $k_1 = k^p(z_1,\ldots,z_m)$ contenha todos os coeficientes das funções racionais em questão.

Seja $F(X;z)$ um elemento de $\mathfrak{o}$, com coeficientes em k^p, e consideremos o seu desenvolvimento de Taylor (cap.IV,§5.2):

$$F(X+u;z+w) = F(X;z) + F_1(u;w) + \ldots + F_\nu(u;w) + \ldots$$

onde

$$(9)\qquad F_\nu(u;w) = \sum_{\substack{\mu_1+\ldots+\mu_n+\nu_1+\ldots+\nu_m=\nu \\ 0\leq\nu_j\leq p-1}} \frac{\partial^\nu F(X;z)}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\, u_1^{\mu_1}\ldots u_n^{\mu_n} w_1^{\nu_1}\ldots w_m^{\nu_m}.$$

Se $F(X;z) \in \mathfrak{p}^{*\nu}$ $(\nu > 1)$ teremos, pela proposição 26 do capítulo IV:

$$\frac{\partial^{i} F(X;z)}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \in \mathfrak{p}^{*}$$

para $i=1,\ldots,\nu-1$ e para tôdas as soluções inteiras não negativas da equação $\mu_1 + \ldots + \mu_n + \nu_1 + \ldots + \nu_m = i$, onde $0 \leq \nu_j \leq p-1$ $(j=1,\ldots,m)$. Exprimiremos, abreviadamente, esta propriedade por

$$F_i(u;w) \equiv 0 \quad (\text{mod. } \mathfrak{p}^{*}) \quad \text{para } i=1,\ldots,\nu-1.$$

Suponhamos agora que $F(X;z) = a(X;z)\, f(X;z)$ com $a(X;z) \in \mathfrak{o}$ e $f(X;z) \in \mathfrak{p}^{*\nu}$ $(\nu>1)$. Afirmamos que

$$F_\nu(u;w) \equiv a(X;z)\, f_\nu(u;w) \quad (\text{mod. } \mathfrak{p}^{*}), \tag{10}$$

onde $f_\nu(u;w)$ é a forma de grau ν do desenvolvimento de Taylor do elemento $f(X;z)$. Com efeito, pelo teorema 18 do capítulo IV temos:

$$\frac{\partial^{\mu_\lambda} F(X;z)}{\partial X_\lambda^{\mu_\lambda}} = \sum_{j=0}^{\mu_\lambda} \frac{\partial^{j} a(X;z)}{\partial X_\lambda^{j}} \frac{\partial^{\mu_\lambda - j} f(X;z)}{\partial X_\lambda^{\mu_\lambda - j}} \qquad (\lambda = 1,\ldots,n)$$

mas (prop. 26, cap.IV)

$$\frac{\partial^{\mu_\lambda - j} f(X;z)}{\partial X_\lambda^{\mu_\lambda - j}} \in \mathfrak{p}^{*\nu-\mu_\lambda+1} \qquad \text{para} \qquad 1 \leq j \leq \mu_\lambda,$$

portanto

$$\frac{\partial^{\mu_\lambda} F(X;z)}{\partial X_\lambda^{\mu_\lambda}} \equiv a(X;z) \frac{\partial^{\mu_\lambda} f(X;z)}{\partial X_\lambda^{\mu_\lambda}} \qquad (\text{mod. } \mathfrak{p}^{*\nu-\mu_\lambda+1}).$$

D'aqui tiramos

$$\frac{\partial^{\mu_1+\ldots+\mu_n} F(X;z)}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n}} \equiv a(X;z) \frac{\partial^{\mu_1+\ldots+\mu_n} f(X;z)}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n}} \quad (\text{mod. } \mathfrak{p}^{*\nu-\mu_1-\ldots-\mu_n+1}). \tag{11}$$

Anàlogamente temos (cap.IV, teorema 18):

$$\frac{\partial^{\nu_j} F(X;z)}{\partial z_j^{\nu_j}} = \sum_{\lambda=0}^{\nu_j} \frac{\partial^{\lambda} a(X;z)}{\partial z_j^{\lambda}} \frac{\partial^{\nu_j - \lambda} f(X;z)}{\partial z_j^{\nu_j - \lambda}} \qquad (j=1,\ldots,m;\ 0 \leq \nu_j \leq p-1);$$

mas (prop.26, cap.IV):

$$\frac{\partial^{\nu_j - \lambda} f(X;z)}{\partial z_j^{\nu_j - \lambda}} \in \mathfrak{p}^{*\nu-\nu_j+1} \qquad \text{para} \qquad 1 \leq \lambda \leq \nu_j,$$

portanto

Multiplicando ambos os membros de (13) por $a_{(j)}(X;z)$ e somando em relação a tôdas as soluções inteiras não negativas da equação $j_1+\ldots+j_s=\nu$ virá:

$$\sum_{j_1+\ldots+j_s=\nu} a_{(j)}(X;z)\, T_{(j)}(X+u;z+w) = F(X;z) +$$

$$+\sum_{j_1+\ldots+j_s=\nu}\left(\sum_{i=1}^{n} a_{(j)}(X;z)\,\frac{\partial T_{(j)}(X;z)}{\partial X_i}\,u_i + \sum_{\ell=1}^{m} a_{(j)}(X;z)\,\frac{\partial T_{(j)}(X;z)}{\partial z_\ell}\,w_\ell\right)+$$

$$+\ldots+\sum_{j_1+\ldots+j_s=\nu}\left(\sum_{\substack{\mu_1+\ldots+\mu_n+\nu_1+\ldots+\nu_m=\nu\\ 0\le\nu_j\le\rho-1}} a_{(j)}(X;z)\,\frac{\partial^{\nu} T_{(j)}(X;z)}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\,\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\,u_1^{\mu_1}\ldots u_n^{\mu_n}\,w_1^{\nu_1}\ldots w_m^{\nu_m}\right).$$

Pondo $F(X;z) = H_\nu(t_1(X;z),\ldots,t_s(X;z))$ poderemos escrever esta última relação sob a forma:

$$(14)\quad H_\nu(t_1(X+u;z+w),\ldots,t_s(X+u;z+w)) = H\,(t(X;z)) + \sum_{i=1}^{n}\left(\sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X;z)\,\frac{\partial T_{(j)}(X;z)}{\partial X_i}\,u_i\right) +$$

$$+ \sum_{\ell=1}^{m}\left(\sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X;z)\,\frac{\partial T_{(j)}(X;z)}{\partial z_\ell}\,w_\ell\right) + \ldots +$$

$$+\ldots+\sum_{\substack{\mu_1+\cdots+\mu_n+\nu_1+\cdots+\nu_m=\nu\\ 0\le\nu_i\le p-1}}\left(\sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X;z)\,\frac{\partial^\nu T_{(j)}(X;z)}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\right)u_1^{\mu_1}\ldots u_n^{\mu_n}w_1^{\nu_1}\ldots w_m^{\nu_m}+$$

$$+\ \ldots\quad .$$

Esta fórmula nos mostra que a forma de grau ν do desenvolvimento de $H_\nu(t_1(X+u;z+w),\ldots,t_s(X+u;z+w))$ (que é obtido de $H_\nu(t(X;z))$ dando os "acréscimos" u e w sòmente às variáveis X e aos elementos z que comparecem em $t_1(X;z),\ldots,t_s(X;z)$ e deixando os coeficientes $a_{(j)}(X;z)$ "constantes") é igual à forma de grau ν que comparece no segundo membro da relação (9). Calcularemos, módulo p^*, a forma de grau ν de $H_\nu(t_1(X+u;z+w),\ldots,t_s(X+u;z+w))$ por um outro processo. Temos

$$t_\ell(X+u;z+w) = t_\ell(X;z) + \left(\sum_{i=1}^{n}\frac{\partial t_\ell}{\partial X_i}\,u_i + \sum_{j=1}^{m}\frac{\partial t_\ell}{\partial z_j}\,w_j\right) + \ldots. +$$

$$+\sum_{\substack{\mu_1+\cdots+\mu_n+\nu_1+\cdots+\nu_m=\nu\\ 0\le\nu_i\le p-1}}\frac{\partial^\nu t_\ell}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\,u_1^{\mu_1}\ldots u_n^{\mu_n}w_1^{\nu_1}\ldots w_m^{\nu_m}+\ldots\ ;$$

pondo

$$V_\ell = \left(\sum_{i=1}^{n}\frac{\partial t_\ell}{\partial X_i}\,u_i + \sum_{j=1}^{m}\frac{\partial t_\ell}{\partial z_j}\,w_j\right) + \ldots. +$$

$$+\sum_{\mu_1+\cdots+\mu_n+\nu_1+\cdots+\nu_m=\nu}\frac{\partial^\nu t_\ell}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\,u_1^{\mu_1}\ldots u_n^{\mu_n}w_1^{\nu_1}\ldots w_m^{\nu_m}+\ldots$$

$$t_\varrho(X+u;z+w) = t_\varrho(X;z) + V_\varrho$$

e então teremos

(15) $H_\nu(t_1(X+u;z+w),\ldots,t_s(X+u;z+w)) = H_\nu(t_1+V_1,\ldots,t_s+V_s)$.

Mas $H_\nu(t_1,\ldots,t_s)$ é um polinômio em $t_1,\ldots,t_s$, com coeficientes em $\mathfrak{G}$, logo, o desenvolvimento do segundo membro de (15) será da forma

$$H_\nu(t_1+V_1,\ldots,t_s+V_s) = H_\nu(t_1,\ldots,t_s) +$$

$$+ H_{\nu,1}(V_1,\ldots,V_s) + \ldots + H_{\nu,\nu}(V_1,\ldots,V_s),$$

onde $H_{\nu,q}(V_1,\ldots,V_s)$ $(1 \leq q \leq \nu)$ é uma forma de grau q em $V_1,\ldots,V_s$, com coeficientes em $\mathfrak{G}$. Consideremos o polinômio

$$H_\nu(Z_1,\ldots,Z_s) = \sum_{j_1+\ldots+j_s=\nu} a_{(j)}(X;z)\, Z_1^{j_1} \ldots Z_s^{j_s}$$

nas indeterminadas $Z_1,\ldots,Z_s$, obtido de $H_\nu(t_1,\ldots,t_s)$ substituindo t_j por Z_j $(j=1,\ldots,s)$. Teremos

$$H_{\nu,q}(V_1,\ldots,V_s) = \sum_{\sigma_1+\ldots+\sigma_s=q} \left(\frac{\partial^q H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{Z=t} V_1^{\sigma_1} \ldots V_s^{\sigma_s}.$$

Mas $H_\nu(t_1,\ldots,t_s) \in \mathfrak{p}^{*\nu}$, portanto

$$\left(\frac{\partial^q H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{Z=t} \in \mathfrak{p}^* \quad \text{para} \quad \sigma_1+\ldots+\sigma_s=q < \nu .$$

Então a forma de grau ν do desenvolvimento de $H_\nu(t_1(X+u;z+w),\ldots,t_s(X+u;z+w))$ (ver (14)) será côngrua, módulo $\mathfrak{p}^*$, à forma

$$\sum_{\sigma_1+\ldots+\sigma_s=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{Z=t} \left(\sum_{i=1}^{n} \frac{\partial t_i}{\partial x_i} u_i + \sum_{j=1}^{m} \frac{\partial t_1}{\partial z_j} w_j \right)^{\sigma_1} \cdots \left(\sum_{i=1}^{n} \frac{\partial t_s}{\partial x_i} u_i + \sum_{j=1}^{m} \frac{\partial t_s}{\partial z_j} w_j \right)^{\sigma_s}$$

portanto, pondo

$$V'_\ell = \sum_{i=1}^{n} \frac{\partial t_\ell}{\partial X_i} u_i + \sum_{j=1}^{m} \frac{\partial t_\ell}{\partial z_j} w_j \qquad (\ell = 1, \ldots, s),$$

teremos

$$\sum_{\substack{\mu_1+\cdots+\mu_n+\nu_1+\cdots+\nu_m=\nu \\ 0 \le \nu_j \le p-1}} \left(\sum_{\sigma_1+\cdots+\sigma_s=\nu} a_{(j)}(X;z) \frac{\partial^\nu T_{(j)}(X;z)}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right) u_1^{\mu_1} \ldots u_n^{\mu_n} w_1^{\nu_1} \ldots w_m^{\nu_m} \equiv$$

$$\equiv \sum_{\sigma_1+\cdots+\sigma_s=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{Z=t} V_1'^{\sigma_1} \ldots V_s'^{\sigma_s} \qquad (\text{mod. } \wp^*),$$

ou, então, pela fórmula (12):

$$(16) \qquad F_\nu(u;w) \equiv \sum_{\sigma_1+\cdots+\sigma_s=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{Z=t} V_1'^{\sigma_1} \ldots V_s'^{\sigma_s} \qquad (\text{mod. } \wp^*).$$

Observando que $\mathfrak{S}/\wp^* = \mathfrak{Q}(P/V)$, poderemos escrever a (16) sob a forma

$$F_\nu(u;w)_{X=\xi} = \sum_{\sigma_1+\cdots+\sigma_s=\nu} \left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{\substack{Z=t \\ X=\xi}} (V_1'^{\sigma_1} \ldots V_s'^{\sigma_s})_{X=\xi}.$$

Mas

$$\left(\frac{\partial^\nu H_\nu(Z)}{\partial Z_1^{\sigma_1} \ldots \partial Z_s^{\sigma_s}} \right)_{Z=t} = a_{(\sigma_1, \ldots, \sigma_s)}(X;z)$$

e pondo

$$U_\ell = (V'_\ell)_{X=\xi} = \sum_{i=1}^{n} \left(\frac{\partial t_\ell}{\partial X_i}\right)_{X=\xi} u_i + \sum_{j=1}^{m} \left(\frac{\partial t_\ell}{\partial X_j}\right)_{X=\xi} w_j$$

teremos

$$(17) \qquad F_\nu(u;w)_{X=\xi} = \sum_{\sigma_1+\cdots+\sigma_s=\nu} a_{(\sigma_1, \ldots, \sigma_s)}(\xi;z) U_1^{\sigma_1} \ldots U_s^{\sigma_s}.$$

Portanto, a forma $F_\nu(u;w)_{X=\xi}$ pode ser obtida da forma

$$\sum_{\sigma_1+\cdots+\sigma_s=\nu} a_{(\sigma)}(\xi;z)\ U_1^{\sigma_1}\ldots U_s^{\sigma_s}$$

por meio da transformação linear

(18) $$U_\ell = \sum_{i=1}^{n}\left(\frac{\partial t_\ell}{\partial X_i}\right)_{X=\xi} u_i + \sum_{j=1}^{m}\left(\frac{\partial t_\ell}{\partial z_j}\right)_{X=\xi} w_j \qquad (\ell=1,\ldots,s).$$

A matriz $\left\|\frac{\partial t_\ell}{\partial X_i}\quad\frac{\partial t_\ell}{\partial z_j}\right\|$ $(i=1,\ldots,n;\ \ell=1,\ldots,s;j=1,\ldots,m)$ tem característica n no ponto P_o (cap.V, corolário 9), portanto, a matriz $\left\|\frac{\partial t_\ell}{\partial X_i}\quad\frac{\partial t_\ell}{\partial z_j}\right\|$ $(i=1,\ldots,n;\ \ell=1,\ldots,s;j=1,\ldots,m)$ tem característica máxima s para $X=\xi$. Isto nos mostra que se a forma do segundo membro de (17) for diferente de zero (isto é, se nem todos os coeficientes $a_{(\sigma)}(\xi;z)$ forem nulos) também a sua transformada $F_\nu(u;w)_{X=\xi}$, por meio da transformação linear (18), será diferente de zero. Dêste resultado segue-se o seguinte lema:

Lema 3 - Seja

$$F(X;z) = H_\nu(t_1,\ldots,t_s) = \sum_{j_1+\cdots+j_s=\nu} a_{(j)}(X;z)\ t_1^{j_1}\ \ldots\ t_s^{j_s}$$

uma forma de grau ν em $t_1,\ldots,t_s$ com coeficientes $a_{(j)}(X;z)$ em $\mathfrak{G}$, mas nem todos em $\mathfrak{p}^*$; então nem tôdas as derivadas parciais mistas de $F(X;z)$, de ordem ν, estão em $\mathfrak{p}^*$.

Demonstração - Usaremos as mesmas notações anteriores. Pela proposição 17 do capítulo Iv segue-se que nem tôdas as derivadas parciais de ordem ν de $H_\nu(Z_1,\ldots,Z_s)$, em relação a $Z_1,\ldots,Z_s$, estão em $\mathfrak{p}^*$ (pois nem todos os coeficientes $a_{(j)}(X;z)$ estão em $\mathfrak{p}^*$). Isto nos permite afirmar que a forma do segundo membro de (17) é diferente de zero, portanto, pelo último resultado que estabelecemos acima, segue-se que a sua transformada $F_\nu(u;w)_{X=\xi}$, pela transformação linear (18), é diferente de zero. Então, pela fórmula (9), nem tôdas as derivadas parciais mistas, de ordem ν, de $F(X;z)$, estão em

ρ^* . (q.e.d.).

3.2.

Seja S_n^k o espaço linear de n dimensões sôbre um corpo imperfeito k. Consideremos um polinômio f, $f \neq 0$ e $gr.f > 0$, de $R_n = k[X_1,\ldots,X_n]$. Seja $Z = (z_\alpha)_{\alpha \in A}$ uma p-base de k. Daremos as seguintes definições:

Definição 4 - Diremos que um ponto $P(\alpha)$ do espaço linear S_n^k é um ponto múltiplo de ordem pelo menos ρ, $\rho \geq 1$, da hipersuperfície algébrica $H = \mathcal{V}(R_n.f)$ quando, e sòmente quando, for verificada a condição: tôdas as derivadas parciais mistas de ordens $0,1,\ldots,\rho-1$ de f em relação a $X_1,\ldots,X_n,z_1,\ldots,z_m$ (onde $z_1,\ldots,z_m$ é um sub-conjunto de Z tal que o corpo $k_1=k^p(z_1,\ldots,z_m)$ contenha todos os coeficientes de f(X)) se anulam no ponto $P(\alpha)$, isto é,

$$\left(\frac{\partial^i f}{\partial X_1^{i_1}\ldots\partial X_n^{i_n}\partial z_1^{j_1}\ldots\partial z_m^{j_m}}\right)_{X=\alpha} = 0$$

para $i=0,\ldots,\rho-1$ e para tôdas as soluções inteiras não negativas da equação $i_1+\ldots+i_n+j_1+\ldots+j_m=i$ tais que $0 \leq j_\ell \leq p-1$ $(\ell=1,\ldots,m)$.

Definição 5 - Diremos que um ponto $P(\alpha)$ do espaço linear S_n^k é um ponto múltiplo de ordem ρ da hipersuperfície algébrica $H = \mathcal{V}(R_n.f)$ quando, e sòmente quando, forem verificadas as condições: 1) $P(\alpha)$ é um ponto múltiplo de ordem pelo menos ρ de H; 2) existe, pelo menos, uma derivada parcial mista, de ordem ρ, de f em relação a

$X_1,\ldots,X_n,z_1,\ldots,z_m$ (onde $z_1,\ldots,z_m$ é tal que o corpo $k_1=k^p(z_1,\ldots,z_m)$ contenha todos os coeficientes de f) que não se anula em $P(\alpha)$.

Passaremos agora a resolver o problema proposto na introdução dêste capítulo, quando o corpo base k é imperfeito. Demonstraremos o seguinte:

Teorema 2 - Um polinômio F de $R_n=k[X_1,\ldots,X_n]$ pertence à potência simbólica $\mathfrak{p}^{(\rho)}$, de um ideal primo $\mathfrak{p}$ de R_n, quando,e sòmente quando, tôdas as derivadas parciais mistas de ordens $0,1,\ldots,\rho-1$ de F em relação a $X_1,\ldots,X_n,z_1,\ldots,z_m$ (onde $z_1,\ldots,z_m$ é tal que o corpo $k_1=k^p(z_1,\ldots,z_m)$ contenha todos os coeficientes de F) pertencem a $\mathfrak{p}$.

Demonstração - O teorema é imediato se $\mathfrak{p}=R_n$, ou, se $\mathfrak{p}=(0)$; suponhamos então que $\mathfrak{p}\neq(0)$ e $\mathfrak{p}\neq R_n$. Suponhamos que $F(X;z)\in\mathfrak{p}^{(\rho)}$. Seja $\mathcal{O}_1$ o anel de quocientes de R_n em relação ao ideal primo $\mathfrak{p}$ e ponhamos $\mathfrak{P}=\mathcal{O}_1\cdot\mathfrak{p}$. Pela proposição 30 do capítulo I teremos $\mathfrak{P}^\rho\cap R_n=\mathfrak{p}^{(\rho)}$, portanto, $F(X;z)\in\mathfrak{P}^\rho$. Pelas proposições 23 e 26 do capítulo IV teremos

$$\frac{\partial^i F(X;z)}{\partial X_1^{i_1}\ldots\partial X_n^{i_n}\partial z_1^{j_1}\ldots\partial z_m^{j_m}}\in R_\infty \quad\text{e}\quad \frac{\partial^i F(X;z)}{\partial X_1^{i_1}\ldots\partial X_n^{i_n}\partial z_1^{j_1}\ldots\partial z_m^{j_m}}\in\mathfrak{P}$$

para $0\leq i=i_1+\ldots+i_n+j_1+\ldots+j_m<\rho$ e $0\leq j_\ell\leq p-1$ $(\ell=1,\ldots,m)$. Portanto

$$\frac{\partial^i F(X;z)}{\partial X_1^{i_1}\ldots\partial X_n^{i_n}\partial z_1^{j_1}\ldots\partial z_m^{j_m}}\in\mathfrak{P}\cap R_n=\mathfrak{p},$$

isto demonstra a condição necessária. Suponhamos agora que tôdas as derivadas parciais mistas, de ordens $0,1,\ldots,\rho-1$, de $F(X;z)$, em relação a $X_1,\ldots,X_n,z_1,\ldots,z_m$, pertençam a $\mathfrak{p}$ e que $\rho>1$ (se $\rho=1$ a condição suficiente nada mais é do que o teorema dos zeros de Hilbert), $\mathfrak{p}\neq(0)$ e $\mathfrak{p}\neq R_n$. Seja $V=\mathfrak{V}(\mathfrak{p})\subset S_n$ e considere

mos um ponto simples P_o de V (cap.V, corolário 12); ponhamos $\mathcal{O} = \mathcal{Q}(P_o/S_n)$, $\mathfrak{m} = \mathfrak{m}(P_o/S_n)$ e $\mathfrak{p}^* = \mathcal{O}.\mathfrak{p}$. Pelo corolário 4 do capítulo V existe um sistema de parâmetros uniformizadores $t_1,\ldots,t_n$ do ponto P_o, como ponto do espaço linear S_n, tal que $\mathfrak{p}^* = \mathcal{O}.(t_1,\ldots,t_s)$, $\mathfrak{m} = \mathcal{O}.(t_1,\ldots,t_n)$, onde $s = n-r$ e $r = \dim.V$. Pela proposição 31 do capítulo I teremos $\mathfrak{p}^{*\rho} \cap R_n = \mathfrak{p}^{(\rho)}$, portanto, o elemento $F(X;z)$, de R_n, pertencerá à $\mathfrak{p}^{(\rho)}$ quando, e sòmente quando, $F(X;z) \in \mathfrak{p}^{*\rho}$. Mas $\mathfrak{p}^{*\rho} \subset \mathfrak{p}^{*(\rho)}$, portanto, se demonstrarmos que $F(X;z) \in \mathfrak{p}^{*\rho}$ teremos também $F(X;z) \in \mathfrak{p}^{*(\rho)}$ e então $F(X;z) \in \mathfrak{p}^{(\rho)}$. De $\bigcap_{\mu=0}^{\infty} \mathfrak{p}^{*\mu} = (0)$ (ver cap.I, teorema 15) segue-se que $F(X;z)$ ($F \neq 0$ - se $F = 0$ é imediato que $F \in \mathfrak{p}^{(\rho)}$) pertence exatamente a uma potência $\mathfrak{p}^{*\mu}$ de $\mathfrak{p}^*$, isto é, existe um inteiro μ tal que $F(X;z) \in \mathfrak{p}^{*\mu}$ e $F(X;z) \notin \mathfrak{p}^{*\mu+1}$ (ainda mais temos $\mu \geq 1$ pois, por hipótese, $F(X;z) \in \mathfrak{p} \subset \mathfrak{p}^*$). Portanto, $F(X;z)$ pode ser escrito como uma forma de grau μ em $t_1,\ldots,t_s$, com coeficientes em $\mathcal{O}$ mas nem todos em $\mathfrak{p}^*$ (lema 1):

$$F(X;z) = \sum_{j_1+\cdots+j_s=\mu} a_{(j)}(X;z)\, t_1^{j_1}\ldots t_s^{j_s},$$

onde $a_{(j)}(X;z) \in \mathcal{O}$ e nem todos $a_{(j)}$ estão em $\mathfrak{p}^*$. Pelo lema 3 nem tôdas as derivadas parciais mistas de ordem μ, de $F(X;z)$, em relação a $X_1,\ldots,X_n,z_1,\ldots,z_m$ estão em $\mathfrak{p}^*$, e pela proposição 26 do capítulo IV, tôdas as derivadas parciais mistas, de ordens $0,1,\ldots,\mu-1$, de $F(X;z)$, em relação a $X_1,\ldots,X_n,z_1,\ldots,z_m$ estão em $\mathfrak{p}^*$. Mas, por hipótese, tôdas as derivadas parciais mistas, de ordens $0,1,\ldots,\mu-1$, de $F(X;z)$, em relação a $X_1,\ldots,X_n,z_1,\ldots,z_m$ estão em $\mathfrak{p}^*$, portanto, teremos $\mu \geq \rho$ e então $F \in \mathfrak{p}^{*\mu} \subset \mathfrak{p}^{*\rho}$. Isto completa a demonstração da condição suficiente do teorema 2.

Dêste teorema e da definição 4 resulta o

Corolário 8 - Seja V uma variedade algébrica irredutível do espaço linear S_n ($V \neq \emptyset$ e $V \neq S_n$) e ponhamos $\mathfrak{p} = \mathfrak{J}(V) \subset R_n$. Então o conjunto formado por zero e por todos os polinômios f de R_n, $f \neq 0$,

que verificam a condição "todo ponto de V é um ponto múltiplo de ordem pelo menos ρ, $\rho \geq 1$, da hiper-superfície algébrica $H = U(R_n.f)$" é a potência simbólica ρ-ésima de $\mathfrak{p}$.

Êste corolário nos dá a solução do problema proposto na introdução dêste capítulo, no caso em que o corpo base k é imperfeito.

A definição de sub-variedade múltipla de ordem ρ de uma hiper-superfície algébrica H é a mesma que a definição 3 (onde por ponto múltiplo de ordem pelo menos ρ e de ordem ρ estaremos entendendo pontos que satisfazem, respectivamente, as definições 4 e 5). Pode-se então demonstrar (do mesmo modo que no §2.1) os corolários 2, 3 e 4 no caso em que o corpo base k é imperfeito.

Se V for uma variedade algébrica qualquer (não necessàriamente irredutível) também serão válidos, para o caso em que o corpo base k é imperfeito, os corolários 5, 6 e 7.

3.3.

Seja R um anel noetheriano com elemento unidade. Consideremos um ideal primo $\mathfrak{p}$ de R, $\mathfrak{p} \neq R$; seja $\mathfrak{q}$ um ideal primário pertencente a $\mathfrak{p}$. Pela prop.4 do cap.I existe um inteiro ρ, $\rho > 0$, tal que $\mathfrak{p}^\rho \subset \mathfrak{q}$. O menor expoente ρ que verifica esta condição é denominado expoente do ideal primário $\mathfrak{q}$.

Lema 4 - $\mathfrak{p}^{(\rho)} \subset \mathfrak{q}$, onde ρ é o expoente de $\mathfrak{q}$.

Demonstração - Temos $\mathfrak{p}^\rho = [\mathfrak{p}^{(\rho)}, \mathfrak{q}_1, \ldots, \mathfrak{q}_h]$, onde $\mathfrak{p} \subset \mathfrak{p}_i = \text{Rad.}\,\mathfrak{q}_i$ $(i=1,\ldots,h)$ (se $\mathfrak{p}^\rho$ for um ideal primário teremos $\mathfrak{p}^\rho = \mathfrak{p}^{(\rho)}$ e o lema é imediato). De $\mathfrak{p} \subset \mathfrak{p}_i$, $\mathfrak{p} \neq \mathfrak{p}_i$, segue-se que existe, para cada i, um elemento c_i tal que $c_i \in \mathfrak{p}_i$, $c_i \notin \mathfrak{p}$. De $c_i \in \mathfrak{p}_i$ vem $c_i^{\rho_i} \in \mathfrak{q}_i$ (cap.I, teorema 3), portanto, o elemento $c = c_1^{\rho_1} \ldots c_h^{\rho_h}$ pertence a $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_h$, mas não pertence a $\mathfrak{p}$. Seja agora f um elemento de $\mathfrak{p}^{(\rho)}$; então $cf \in \mathfrak{p}^\rho \subset \mathfrak{q}$, logo, $cf \in \mathfrak{q}$. Mas $c \notin \mathfrak{p}$, portanto, $f \in \mathfrak{q}$. (q.e.d.).

Seja $R_n = k[X_1,\ldots,X_n]$ um anel de polinômios de n

indeterminadas $X_1,\ldots,X_n$ sôbre o corpo k; consideremos um ideal primo $\mathfrak{p}$ de R_n, $\mathfrak{p} \neq (0)$ e $\mathfrak{p} \neq R_n$. Para cada inteiro ν, $\nu > 0$, faremos corresponder o inteiro $\rho(\nu)$ tal que $\mathfrak{p}^{(\nu)} \subset \mathfrak{p}^{\rho(\nu)}$ e $\mathfrak{p}^{(\nu)} \not\subset \mathfrak{p}^{\rho(\nu)+1}$ (a existência de um inteiro $\rho(\nu)$ satisfazendo estas condições resulta do teorema 15 do cap.I). Se $\nu_1 > \nu_2$ teremos $\rho(\nu_1) \geq \rho(\nu_2)$, portanto, a sucessão $\rho(1), \rho(2),\ldots, \rho(\nu),\ldots$ é não-decrescente. Demonstraremos no teorema abaixo que esta sucessão é não limitada. Precisamente, temos o

Teorema 3 - Tôda potência simbólica $\mathfrak{p}^{(\nu)}$ de $\mathfrak{p}$ está contida numa potência $\mathfrak{p}^{\rho(\nu)}$ de $\mathfrak{p}$, onde $\lim_{\nu \to +\infty} \rho(\nu) = +\infty$.

Demonstração - Para demonstrar o teorema 3 basta provar que a sucessão $\rho(1),\ldots, \rho(\nu),\ldots$ não é limitada. Seja N um inteiro positivo e seja

$$\mathfrak{p}^N = [\mathfrak{p}^{(N)}, \mathfrak{q}_1,\ldots,\mathfrak{q}_h] \tag{19}$$

uma decomposição normal de $\mathfrak{p}^N$. Temos $\mathfrak{p} \subset \mathfrak{p}_i = \text{Rad.}\,\mathfrak{q}_i$ $(i=1,\ldots,h)$. Indiquemos por ρ_i o expoente de $\mathfrak{q}_i$; pelo lema 4 temos $\mathfrak{p}_i^{(\rho_i)} \subset \mathfrak{q}_i$. Afirmamos que $\mathfrak{p}^{(\nu)} \subset \mathfrak{p}^N$ para todo $\nu \geq \nu_0 = \max.(N, \rho_1,\ldots,\rho_h)$ (e, portanto, a sucessão $\rho(1),\ldots,\rho(\nu),\ldots$ não é limitada). Com efeito, seja $Z = (z_\alpha)_{\alpha \in A}$ uma p-base de k (se k for perfeito, $Z = \emptyset$) e consideremos um elemento f de $\mathfrak{p}^{(\nu)}$, onde $\nu \geq \nu_0$. Seja $\{z_1,\ldots,z_m\}$ um sub-conjunto finito de Z tal que o corpo $k_1 = k^p(z_1,\ldots,z_m)$ (se k for perfeito, m=0; se p=0, $k^p=k$) contenha todos os coeficientes de f. Pelos teoremas 1 e 2 teremos

$$\frac{\partial^\lambda f}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}} \in \mathfrak{p}, \tag{20}$$

para $\lambda = 0,1,\ldots,\nu-1$ e para tôdas as soluções inteiras não negativas da equação $\mu_1+\ldots+\mu_n+\nu_1+\ldots+\nu_m = \lambda$, onde $0 \leq \nu_j \leq p-1$ $(j=1,\ldots,m$; sendo que esta última condição é vazia se k for perfeito). Como $\mathfrak{p} \subset \mathfrak{p}_i$ $(i=1,\ldots,h)$ teremos, pelos teoremas 1 e 2,

$f \in \mathfrak{p}_i^{(\nu)}$. Mas $\mathfrak{p}_i^{(\nu)} \subset \mathfrak{p}_i^{(\nu_0)} \subset \mathfrak{p}_i^{(\rho_i)} \subset \mathfrak{q}_i$, portanto, $f \in \mathfrak{q}_i$; por outro lado, $\nu \geq \nu_0 \geq N$, logo, $\mathfrak{p}^{(\nu)} \subset \mathfrak{p}^{(\nu_0)} \subset \mathfrak{p}^{(N)}$ e então $f \in \mathfrak{p}^{(N)}$. Portanto, pela (19), $f \in \mathfrak{p}^N$ para todo $\nu \geq \nu_0$. (q.e.d.).

§4 - Sôbre um teorema de O.Zariski.

4.1 - Pontos (W-μ)-regulares.

Seja W uma variedade algébrica irredutível do espaço linear S_n^k $(W \neq \emptyset)$ e seja P um ponto simples de W. Ponhamos $R_n = k[X_1,\ldots,X_n]$, $\mathcal{O} = \mathcal{Q}(P/S_n)$, $\mathfrak{m} = \mathfrak{m}(P/S_n)$, $\mathfrak{p} = \mathfrak{J}(W)$ e $\mathfrak{p}^* = \mathcal{O}.\mathfrak{p}$. Pelo corolário 4 do capítulo V existe um sistema de parâmetros uniformizadores do ponto P, como ponto do espaço linear S_n, tal que $\mathfrak{p}^\nu = \mathcal{O}.(t_1,\ldots,t_s)$ (onde $s = n-\rho$, $\rho = \dim.W$) e $\mathfrak{m} = \mathcal{O}.(t_1,\ldots,t_s,t_1',\ldots,t_\rho')$.

Lema 5 - $\mathfrak{p}^{*(\mu)} = \mathfrak{p}^{*\mu}$.

Demonstração - Basta demonstrar que $\mathfrak{p}^{*(\mu)} \subset \mathfrak{p}^{*\mu}$. Seja f, $f \neq 0$, um elemento de $\mathfrak{p}^{*(\mu)}$; pela demonstração do lema 4 existe um elemento c de $\mathcal{O}$, $c \notin \mathfrak{p}^*$, tal que $cf \in \mathfrak{p}^{*\mu}$. Por outro lado, f pertence exatamente a uma potência $\mathfrak{p}^{*\nu}$ de $\mathfrak{p}^*$ (pelo teorema 15 do capítulo I), isto é, $f \in \mathfrak{p}^{*\nu}$ e $f \notin \mathfrak{p}^{*\nu+1}$; ainda mais, temos $\nu \geq 1$, pois, $f \in \mathfrak{p}^*$. Provaremos que $\nu \geq \mu$ e, portanto, $f \in \mathfrak{p}^{*\nu} \subset \mathfrak{p}^{*\mu}$. Suponhamos, por absurdo, que $\nu < \mu$. Temos

$$f = \sum_{\nu_1+\ldots+\nu_s=\nu} a_{(\nu_1,\ldots,\nu_s)} t_1^{\nu_1} \ldots t_s^{\nu_s},$$

onde $a_{(\nu)} \in \mathcal{O}$ e nem todos os coeficientes $a_{(\nu)}$ pertencem a $\mathfrak{p}^*$ (lema 1). Então teremos

$$cf = \sum_{\nu_1+\ldots+\nu_s=\nu} (ca_{(\nu)})\, t_1^{\nu_1} \ldots t_s^{\nu_s},$$

que pertencerá a $\mathfrak{p}^{*\mu}$; mas $\nu < \mu$, portanto, todos os coeficientes $ca_{(\nu)}$ estão em $\mathfrak{p}^*$ (lema 1). Isto é absurdo pois $c \notin \mathfrak{p}^*$ e pelo menos um dos coeficientes $a_{(\nu)}$ não pertence a $\mathfrak{p}^*$. (q.e.d.).

Lema 6 - Se $\zeta \in \mathfrak{p}^{*\mu} \cap \mathfrak{m}^{\nu}$, onde $\nu \geq \mu$, e se $\{T_1,\ldots,T_{d_\mu}\}$ for uma base mínimal de $\mathfrak{p}^{*\mu}$, então ζ poderá ser escrito como uma forma linear em $T_1,\ldots,T_{d_\mu}$, com coeficientes em $\mathfrak{m}^{\nu-\mu}$ (se $\nu = \mu$, $\mathfrak{m}^0 = \mathfrak{o}$).

Demonstração - Observemos que os produtos $T_{(\mu_1,\ldots,\mu_s)} = t_1^{\mu_1} \ldots t_s^{\mu_s}$, $\mu_1 + \ldots + \mu_s = \mu$, formam uma base mínimal de $\mathfrak{p}^{*\mu}$ e que tôdas as bases mínimais de $\mathfrak{p}^{*\mu}$ têm o mesmo número d_μ de elementos, onde $d_\mu = \binom{s+\mu-1}{\mu}$. Como a passágem de uma base mínimal de $\mathfrak{p}^{*\mu}$ para uma outra base mínimal do mesmo ideal é obtida por meio de uma transformação linear, com coeficientes em $\mathfrak{o}$, mas cujo determinante não pertence a $\mathfrak{m}$, será bastante demonstrar o lema acima para a base $\{T_{(\mu)}\}$ de $\mathfrak{p}^{*\mu}$. Estas observações resultam, imediatamente, do fato que o sub-espaço vectorial de $\mathfrak{M}_\mu(P/S_n)$, gerado pelos vectores de $\tau\,\mathfrak{p}^{*\mu}$ ($\tau : \mathfrak{m}^\mu \longrightarrow \mathfrak{M}_\mu$), tem dimensão $d_\mu = \binom{s+\mu-1}{\mu}$. Se $\nu = \mu$ o lema é imediato; demonstraremos o lema por indução sôbre a diferença $\nu - \mu$. Suponhamos então que o lema seja verdadeiro para $\nu - \mu - 1$ e que $\nu > \mu$. Portanto, de $\zeta \in \mathfrak{p}^{*\mu} \cap \mathfrak{m}^{\nu}$ segue-se que ζ pode ser escrito sob a forma $\zeta = \sum' a_{(\mu)} T_{(\mu)}$, onde $a_{(\mu)} \in \mathfrak{m}^{\nu-\mu-1}$ em $\{t,t'\}$, com coeficientes em $\mathfrak{o}$. Mas $\zeta \in \mathfrak{m}^{\nu}$, portanto, todos os coeficientes das formas $a_{(\mu)}(t;t')$ pertencem a $\mathfrak{m}$ (pois $\mathfrak{o}$ é um anel local regular), logo, $a_{(\mu)} \in \mathfrak{m}^{\nu-\mu}$. (q.e.d.).

Seja V uma variedade algébrica irredutível do espaço linear S_n^k ($V \neq \emptyset$) e seja W, $W \neq \emptyset$, uma sub-variedade algébrica irredutível de V. Adotaremos as mesmas notações anteriores relativamente à variedade algébrica W. Em R_n consideremos o ideal $\mathfrak{a}_\mu = \mathfrak{J}(V) \cap \mathfrak{p}^{(\mu)}$ ($\mu \geq 1$) e seja $\{f_1,\ldots,f_{N_\mu}\}$ uma base dêste ideal. Seja $Z = (z_\alpha)_{\alpha \in A}$ uma p-base de k (Z = $\emptyset$ se k fôr perfeito) e consideremos um sub-conjunto finito $\{z_1,\ldots,z_m\}$ de Z tal que o corpo $k_1 = k^p(z_1,\ldots,z_m)$ contenha todos os coeficientes dos polinômios $f_1,\ldots,f_{N_\mu}$. Tôdas as derivadas parciais mistas, de ordens $0,1,\ldots,\mu-1$, de cada polinômio f_i, em relação a

$X_1,\ldots,X_n,z_1,\ldots,z_m$ (com a limitação usual $0 \leq \nu_j \leq p-1$, se k for imperfeito) pertencem a $\mathfrak{p}$. Consideremos a matriz

$$(21) \qquad M_\mu = \left\| \frac{\partial^\mu f_i}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right\|$$

de N_μ linhas e de q_μ colunas, onde q_μ é o número de soluções inteiras não negativas da equação $\mu_1+\ldots+\mu_n+\nu_1+\ldots+\nu_m=\mu$, onde $0 \leq \nu_j \leq p-1$ $(j=1,\ldots,m)$. Indiquemos por σ_μ a característica de M_μ para $X_\ell = \eta_\ell$ $(\ell=1,\ldots,n)$, onde $(\eta_1,\ldots,\eta_n)$ é o ponto geral de W. E' imediato que σ_μ não depende da base $\{f_1,\ldots,f_{N_\mu}\}$ escolhida para o ideal $\mathfrak{M}_\mu$.

Definição 6 - Diremos que um ponto $P(\alpha)$ de W é um ponto (W- μ)-regular de V, se forem verificadas as condições: a) P é um ponto simples de W; b) a matriz M_μ tem característica σ_μ em P.

Teorema 4 - Quasi todos os pontos de W [2] são pontos (W- μ)-regulares de V.

Demonstração - Provaremos que os pontos de W que não são pontos (W- μ)-regulares de V formam uma sub-variedade algébrica própria de W. Seja $\mathfrak{k}'_\mu$ o ideal gerado em R_n pelos menores de ordem σ_μ da matriz M_μ e consideremos o ideal $\mathfrak{k}_\mu = (\mathfrak{k}'_\mu, \mathfrak{p})$. Temos $\mathfrak{k}_\mu \supset \mathfrak{p}$ e $\mathfrak{k}_\mu \neq \mathfrak{p}$, portanto, $\mathfrak{V}(\mathfrak{k}_\mu)$ é uma sub-variedade algébrica própria de W. Os pontos singulares de W formam uma sub-variedade algébrica própria W_1 de W (cap.V, corolário 12). Portanto $W_1 \cup \mathfrak{V}(\mathfrak{k}_\mu)$ é uma sub-variedade algébrica própria de W e é imediato que um ponto P de W não é um ponto (W- μ)-regular de V quando, e sòmente quando, $P \in W_1 \cup \mathfrak{V}(\mathfrak{k}_\mu)$. (q.e.d.).

---

[2] Por "quasi todos os pontos de uma variedade algébrica irredutível W" entendemos o conjunto formado por todos os pontos de W exceto aqueles que pertencem a um número finito de sub-variedades algébricas próprias de W.

Seja P um ponto $(W-\mu)$-regular de V; podemos supôr (usando uma notação conveniente) que as primeiras σ_μ linhas da matriz M_μ sejam linearmente independentes sôbre $\Delta = k(P)$. Consideremos o anel local regular $\mathcal{O} = \mathcal{Q}(P/S_n)$ (cap.V, teorema 1) e ponhamos $\mathfrak{m} = \mathfrak{m}(P/S_n)$, $\mathfrak{p}^* = \mathcal{O}.\mathfrak{p}$, $\mathfrak{p}^* = \mathcal{O}.(t_1,\ldots,t_s)$ $(s = n-\varrho$ e $\varrho = \dim.W)$, $\mathfrak{m} = \mathcal{O}.(t_1,\ldots,t_s,t'_1,\ldots,t'_\varrho)$, $\mathfrak{p}_P(V) = \mathcal{O}.\mathfrak{J}(V)$, $\mathfrak{M}_\mu = \mathfrak{M}_\mu(P/S_n)$ e $\tau : \mathfrak{m}^\mu \longrightarrow \mathfrak{M}_\mu$. Suponhamos ainda que o corpo $k_1 = k^p(z_1,\ldots,z_m)$ contenha todos os coeficientes dos elementos $t_1,\ldots,t_s,t'_1,\ldots,t'_\varrho$. Observemos que $\mathcal{O}.\mathfrak{N}_\mu = \mathcal{O}.(\mathfrak{J}(V) \cap \mathfrak{p}^{(\mu)}) = \mathfrak{p}_P(V) \cap \mathfrak{p}^{*\mu}$ (pelo lema 5).

Lema 7 - Os vectores $\tau f_1,\ldots,\tau f_\sigma$ $(\sigma = \sigma_\mu)$ de $\mathfrak{M}_\mu$ são linearmente independentes sôbre $\Delta = k(P)$.

Demonstração - Se $\tau f_1,\ldots,\tau f_\sigma$ não fossem linearmente independentes sôbre $\Delta = k(P)$ teríamos (usando uma notação conveniente) uma relação da forma $\tau f_1 = \sum_{i=2}^{\sigma} \overline{\delta}_i \tau f_i$, onde $\overline{\delta}_i \in \Delta$. D'aqui tiramos $f_1 = \sum_{i=2}^{\sigma} \delta_i f_i + \alpha$ (onde $\alpha \in \mathfrak{m}^{r+1}$ e $\overline{\delta}_i =$ = $\mathfrak{m}$-resíduo de δ_i, $i=2,\ldots,\sigma$). Portanto, teremos

$$\left(\frac{\partial^\mu f_1}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\,\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\right)_P = \sum_{i=2}^{\sigma} \overline{\delta}_i \left(\frac{\partial^\mu f_i}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\,\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\right)_P ,$$

para tôdas as soluções inteiras não negativas da equação $\mu_1+\ldots+\mu_n+\nu_1+\ldots+\nu_m = \mu$, onde $0 \leq \nu_j \leq p-1$ $(j=1,\ldots,m)$. Isto nos mostra que as primeiras σ linhas da matriz M_μ não são linearmente independentes sôbre Δ, o que é absurdo. (q.e.d.).

Dêste lema resulta que os vectores $\tau f_1,\ldots,\tau f_\sigma$ podem ser imersos numa base de $\tau\,\mathfrak{p}^{*\mu}$ (sub-espaço vectorial de $\mathfrak{M}_\mu$). Indicaremos tal base por $\{\tau\omega_1,\ldots,\tau\omega_\sigma,\tau\omega_{\sigma+1},\ldots,\tau\omega_d\}$, onde $\omega_i = f_i$ $(i=1,\ldots,\sigma)$, $\omega_j \in \mathfrak{p}^{*\mu}$ $(j=\sigma+1,\ldots,d)$ e $d = d_\mu =$ $= \binom{s+\mu-1}{\mu}$. E' imediato que $\{\omega_1,\ldots,\omega_d\}$ é uma base mínimal de $\mathfrak{p}^{*\mu}$. Uma outra base mínimal de $\mathfrak{p}^{*\mu}$ é dada pelos produtos $T_{(\mu)} = t_1^{\mu_1}\ldots t_s^{\mu_s}$ $(\mu_1+\ldots+\mu_s = \mu)$; portanto, temos

$$\omega_i = \sum_{(\mu)} a_{(\mu),i}\, T_{(\mu)} \qquad (i=1,\ldots,d), \tag{22}$$

onde $a_{(\mu),i} \in \mathfrak{o}$ e $|a_{(\mu),i}| \in \mathfrak{m}$. Suponhamos que o corpo $k_1 = k^p(z_1,\ldots,z_m)$ contenha todos os coeficientes dos elementos $\omega_{\sigma+1},\ldots,\omega_d$.

Lema 8 - A matriz

$$\left\| \frac{\partial^\mu T_{(\mu)}}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right\|$$

tem característica máxima d para

$X_\ell = \eta_\ell$ $(\ell=1,\ldots,n)$.

Demonstração - Se esta matriz não tivesse característica máxima d para $X_\ell = \eta_\ell$ teríamos uma relação da forma

$$\sum_{(\mu)} \bar{A}_{(\mu)} \left(\frac{\partial^\mu T_{(\mu)}}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right)_{X=\eta} = 0,$$

onde $\bar{A}_{(\mu)} \in k[\eta_1,\ldots,\eta_n]$ e nem todos $\bar{A}_{(\mu)}$ são nulos. Então o elemento $\zeta = \sum_{(\mu)} A_{(\mu)} T_{(\mu)}$, onde $A_{(\mu)} \in R_n$ é tal que $\bar{A}_{(\mu)} =$ = $\wp$-resíduo de $A_{(\mu)}$, pertenceria a $\wp^{\times\mu+1}$ (teorema 2). Portanto, pelo lema 1, deveríamos ter $A_{(\mu)} \in \wp$, isto é, $\bar{A}_{(\mu)} = 0$, para todos os coeficientes, o que é absurdo. (q.e.d.).

Dêste lema resulta, pela relação (22), que a matriz

$$\left\| \frac{\partial^\mu \omega_i}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right\| \qquad (i=1,\ldots,d) \tag{23}$$

tem característica máxima d para $X = \eta$.

Lema 9 - Seja ζ um elemento de $\wp_p(V) \cap \wp^{\times\mu} \cap \mathfrak{m}^\nu$ $(\nu \geq \mu)$, onde P é um ponto $(W-\mu)$-regular de V. Então existe um elemento

$\zeta_1 = \sum_{i=1}^{\sigma} A_i f_i$, onde $A_i \in \mathfrak{m}^{\nu-\mu}$, tal que

$\zeta - \zeta_1 \in \wp_p(V) \cap \wp^{\times\mu+1} \cap \mathfrak{m}^\nu$.

Demonstração - De $\zeta \in \wp^{\times\mu} \cap \mathfrak{m}^\nu$ vem que ζ pode ser escrito sob a forma

$$\varsigma = \sum_{i=1}^{\sigma} A_i f_i + \sum_{j=\sigma+1}^{d} B_j \omega_j ,$$

onde $A_i \in m^{r-\mu}$, $B_j \in m^{r-\mu}$ (lema 6). Então teremos

$$(24) \quad \frac{\partial^\mu \varsigma}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \equiv \sum_{i=1}^{\sigma} A_i \frac{\partial^\mu f_i}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} +$$

$$+ \sum_{j=\sigma+1}^{d} B_j \frac{\partial^\mu \omega_j}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \qquad (\text{mod. } \mathcal{P}^*) .$$

Mas $\varsigma \in \mathcal{P}_P(V) \cap \mathcal{P}^{*\mu}$, portanto, o primeiro membro de (24) é uma combinação linear das primeiras σ linhas da matriz M_μ para $X = \eta$. Por outro lado, a matriz (23) tem característica máxima d para $X = \eta$, logo, deveremos ter $B_j \equiv 0$ (mod. $\mathcal{P}^*$). Então

$$\varsigma - \sum_{i=1}^{\sigma} A_i f_i = \sum_{j=\sigma+1}^{d} B_j \omega_j \in \mathcal{P}_P(V) \cap \mathcal{P}^{*\mu+1} \cap m^r . \quad \text{(q.e.d.)}.$$

Teorema 5 - Seja ς um elemento pertencente aos ideais $m^{r+1} + \mathcal{P}_P(V) \cap \mathcal{P}^{*\mu} \cap m^\nu$ e $\mathcal{P}^{*\nu}$, onde $r > \mu$ e P é um ponto $(V-\mu)$-regular de V. Então ς pertence também ao ideal $m^{r+1} + \mathcal{P}_P(V) \cap \mathcal{P}^{*\mu+1} \cap m^\nu$.

Demonstração - O elemento ς é da forma

$\varsigma = \varphi_{r+1}(t;t') + \varsigma_P$, onde $\varphi_{r+1}(t;t') \in m^{r+1}$ e $\varsigma_P \in \mathcal{P}_P(V) \cap \mathcal{P}^{*\mu} \cap m^r$. Pelo lema 9 existe um elemento $\varsigma_1 = \sum_{i=1}^{\sigma} A_i f_i$, onde $A_i \in m^{r-\mu}$ tal que

$$\varsigma_2 = \varsigma_P - \sum_{i=1}^{\sigma} A_i f_i \in \mathcal{P}_P(V) \cap \mathcal{P}^{*\mu+1} \cap m^r .$$

Indiquemos por τ o homomorfismo canônico de m^r sôbre $\mathcal{M}_r(P/S_n)$. Teremos $\tau\varsigma = \tau\varsigma_P$ e $\tau\varsigma_2 = \tau(\varsigma_P - \varsigma_1) = \tau\varsigma_P - \tau\varsigma_1 = \tau\varsigma - \tau\varsigma_1 = \tau(\varsigma - \varsigma_1)$; portanto, $\tau\varsigma_1 = \tau(\varsigma - \varsigma_2)$. Mas $\varsigma \in \mathcal{P}^{*\nu} \subset \mathcal{P}^{*\mu+1} \cap m^r$ e $\varsigma_2 \in \mathcal{P}^{*\mu+1} \cap m^r$, logo, ς_1 pertence ao ideal $m^{r+1} + \mathcal{P}^{*\mu+1} \cap m^\nu$. Portanto

$$\sum_{i=1}^{\sigma} A_i f_i = \varphi'_{r+1}(t;t') + \Phi(t),$$

onde

$$\Phi(t) = \sum_{(\mu)}' b_{(\mu)} T_{(\mu)},$$

com $b_{(\mu)} \in \wp^*$ e $\varphi'_{r+1}(t;t') \in \mathfrak{m}^{r+1}$. Por outro lado temos

$$f_i = \sum_{(\mu)}' a_{(\mu),i} T_{(\mu)} \tag{25}$$

logo

$$\sum_{(\mu)}' \left[\sum_{i=1}^{\sigma} (a_{(\mu),i} A_i - b_{(\mu)}) \right] T_{(\mu)} = \varphi'_{r+1}(t;t').$$

Mas $\mathfrak{G}$ é um anel local regular, portanto, desta relação vem

$$\sum_{i=1}^{\sigma} a_{(\mu),i} A_i - b_{(\mu)} \in \mathfrak{m}^{r-\mu+1}$$

e então

$$\sum_{i=1}^{\sigma} a_{(\mu),i} A_i = \Phi_{(\mu)} \in \wp^* + \mathfrak{m}^{r-\mu+1}. \tag{26}$$

Da relação (25) tiramos

$$\left(\frac{\partial^{\mu} f_i}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right)_P = \sum_{(\mu')}' a_{(\mu'),i}(P) \left(\frac{\partial^{\mu} T_{(\mu')}}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right)_P .$$

A matriz

$$\left\| \frac{\partial^{\mu} f_i}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right\|$$

de σ linhas, tem característica máxima σ no ponto P, pois P é um ponto $(V-\mu)$-regular de V (e, também, pela escolha de $f_1, \ldots, f_\sigma$); portanto, a matriz $\| a_{(\mu),i}(P) \|$ tem característica máxima σ. Então da relação (26), obtemos

$$A_i \in \wp^* + \mathfrak{m}^{r-\mu+1} \quad \text{para} \quad i=1,\ldots,\sigma,$$

logo, cada A_i pode ser escrito sob a forma $A_i = \pi_i + \psi_i$, onde $\pi_i \in \wp^*$ e $\psi_i \in \mathfrak{m}^{r-\mu+1}$. Portanto, temos

$$\varsigma_3 = \sum_{i=1}^{\sigma} A_i f_i = \sum_{i=1}^{\sigma} \pi_i f_i + \sum_{i=1}^{\sigma} \psi_i f_i,$$

onde $\varsigma_3 = \sum_{i=1}^{\sigma} \pi_i f_i \in \wp_P(V) \cap \wp^{\mu+1} \cap m^{\nu}$ e

$\varsigma_4 = \sum_{i=1}^{\sigma} \psi_i f_i \in m^{\nu-\mu+1} \cdot m^{\mu} = m^{\nu+1}$. Então

$$\varsigma = \varphi_{\nu+1} + \varsigma_P = (\varphi_{\nu+1} + \varsigma_4) + (\varsigma_P - \varsigma_4),$$

onde

$$\varphi_{\nu+1} + \varsigma_4 \in m^{\nu+1}$$

e

$$\varsigma_P - \varsigma_4 = (\varsigma_P - \varsigma_1) + \varsigma_3 \in \wp_P(V) \cap \wp^{\mu+1} \cap m^{\nu}.$$

(q.e.d.).

4.2 - Sôbre funções de $\mathfrak{J}(V)$ que se anulam, com uma dada ordem, em quasi todos os pontos de uma sub-variedade W de V.

Seja W uma sub-variedade irredutível, $W \neq \emptyset$, de uma variedade algébrica irredutível V do espaço linear S_n^k.

Teorema 6 - Se um elemento F de $R_n = k[X_1, \ldots, X_n]$ pertencer a $(\mathfrak{J}(P))^{\nu} + \mathfrak{J}(V)$ para quasi todos os pontos P de W, então existirá um elemento C de R_n, $C \notin \wp = \mathfrak{J}(W)$ tal que $CF \in \wp^{(\nu)} + \mathfrak{J}(V)$.

Demonstração - Suponhamos que $\nu = 1$; por hipótese temos $F \in \mathfrak{J}(P) + \mathfrak{J}(V) = \mathfrak{J}(P)$ para quasi todos os pontos P de W. Então $F \in \wp = \wp^{(1)} + \mathfrak{J}(V)$ (pois $\wp \supset \mathfrak{J}(V)$). Isto demonstra o teorema para $\nu = 1$. Suponhamos que o teorema seja verdadeiro para ν, $\nu \geqslant 1$, e seja F um elemento de R_n pertencente a $(\mathfrak{J}(P))^{\nu+1} + \mathfrak{J}(V)$ para quasi todos os pontos P de W. Indicaremos por W_1' a sub-variedade própria de W, cujos pontos são excluidos na hipótese anterior; quer dizer que temos $F \in (\mathfrak{J}(P))^{\nu+1} + \mathfrak{J}(V)$ para todos os pontos P pertencentes a $W - W_1'$. Como $(\mathfrak{J}(P))^{\nu+1} + \mathfrak{J}(V) \subset (\mathfrak{J}(P))^{\nu} + \mathfrak{J}(V)$, existirá, pela hipótese de indução, um elemento C_1 de R_n, $C_1 \notin \wp$, tal que $C_1 F \in \wp^{(\nu)} + \mathfrak{J}(V)$, portanto, $C_1 F = \alpha_{\nu} + f$, onde $\alpha_{\nu} \in \wp^{(\nu)}$ e $f \in \mathfrak{J}(V)$. Então o

o elemento $F_1 = C_1F - f$ pertence ainda a $(\mathfrak{J}(P))^{\nu+1} + \mathfrak{J}(V)$ para todos os pontos P de $W - W_1'$ e, além disso, $F_1 \in \mathfrak{p}^{(\nu)}$. Se demonstrarmos o teorema acima para o elemento F_1, o mesmo teorema será válido para o elemento F. Com efeito, se existir C_2, $C_2 \in R_n$, $C_2 \notin \mathfrak{p}$, tal que $C_2F_1 \in \mathfrak{p}^{(\nu+1)} + \mathfrak{J}(V)$, teremos $C_2C_1F + C_2f \in \mathfrak{p}^{(\nu+1)} + \mathfrak{J}(V)$. de onde vem, $C_2C_1F \in \mathfrak{p}^{(\nu+1)} + \mathfrak{J}(V)$, onde $C_2C_1 \notin \mathfrak{p}$. Então podemos supôr desde o início que $F \in (\mathfrak{J}(P))^{\nu+1} + \mathfrak{J}(V)$, para todos os pontos P de $W - W_1'$ e que $F \in \mathfrak{p}^{(\nu)}$. Seja S_μ o sub-conjunto de W formado pelos pontos que são pontos $(W-\mu)$-regulares de V; pelo teorema 4, $W-S_\mu$ é uma sub-variedade algébrica própria de W, portanto, também $W_1'' = (W-S_1) \cup \ldots \cup (W-S_\nu)$ é uma sub-variedade algébrica própria de W. Finalmente, temos que $W_1 = W_1' \cup W_1''$ é também uma sub-variedade algébrica <u>própria</u> de W. Observemos que se $P \in W - W_1$ então $P \notin W_1'$ e, além disso, P é um ponto $(W-1),\ldots,(W-\nu)$-regular de V. Por hipótese temos $F \in (\mathfrak{J}(P))^{\nu+1} + \mathfrak{J}(V)$ para todos os pontos P de $W - W_1$ e $F \in \mathfrak{p}^{(\nu)}$. Consideremos um ponto P_o de $W-W_1$ e ponhamos $\mathfrak{o} = Q(P_o/S_n)$, $\mathfrak{m} = \mathfrak{m}(P_o/S_n)$, $\mathfrak{p}^{\mathfrak{o}} = \mathfrak{o}.\mathfrak{p}$ e $\mathfrak{p}_{P_o}(V) = \mathfrak{o}.\mathfrak{J}(V)$. De $F \in (\mathfrak{J}(P)^{\nu+1} + \mathfrak{J}(V)$ vem (cap.I, prop.15) $F \in \mathfrak{m}^{\nu+1} + \mathfrak{p}_{P_o}(V)$ e como $F \in \mathfrak{p}^{(\nu)}$, também teremos $F \in \mathfrak{p}^{\mathfrak{o}^\nu}$. Portanto, $F \in \mathfrak{m}^{\nu+1} + \mathfrak{p}_{P_o}(V) \cap \mathfrak{p}^{\mathfrak{o}} \cap \mathfrak{m}^\nu$ e $F \in \mathfrak{p}^{\mathfrak{o}^\nu}$. Sendo P_o um ponto $(W-1),\ldots,(W-(\nu-1))$-regular virá, pelo teorema 5, $F \in \mathfrak{m}^{\nu+1} + \mathfrak{p}_{P_o}(V) \cap \mathfrak{p}^{\mathfrak{o}^\nu} \cap \mathfrak{m}^\nu$. Seja $\{f_1,\ldots,f_N\}$ uma base do ideal $\mathfrak{N}_\nu = \mathfrak{J}(V) \cap \mathfrak{p}^{(\nu)}$. Indicaremos por $\{z_1,\ldots,z_m\}$ um sub-conjunto finito de uma p-base $Z = (z_\alpha)_{\alpha \in A}$ de k tal que o corpo $k_1 = k^p(z_1,\ldots,z_m)$ ($Z = \emptyset$ se k for perfeito; $k^p = k$ se $p = 0$) contenha todos os coeficientes dos polinômios $f_1,\ldots,f_N,F$. A matriz

$$M_\nu = \left\| \frac{\partial^\nu f_i}{\partial X_1^{\mu_1} \ldots \partial X_n^{\mu_n} \partial z_1^{\nu_1} \ldots \partial z_m^{\nu_m}} \right\|$$

de N linhas e q colunas (onde q é o número de soluções inteiras não negativas da equação $\mu_1 + \ldots + \mu_n + \nu_1 + \ldots + \nu_m = \nu$, $0 \leq \nu_j \leq p-1$) tem mesma característica σ para $X_\ell = \eta_\ell$

$(\ell = 1,\ldots,n)$ e para $X_\ell = \alpha_\ell$, onde $(\eta_1,\ldots,\eta_n)$ é o ponto geral de W e $(\alpha_1,\ldots,\alpha_n)$ são as coordenadas do ponto P_o, pois P_o é um ponto $(W-v)$-regular de V. Consideremos a matriz

$$M'_v = \left\| \begin{array}{c} \dfrac{\partial^v f_i}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}} \\ \dfrac{\partial^v F}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}} \end{array} \right\|.$$

De $F \in \mathfrak{m}^{v+1} + \mathfrak{p}_{P_o}(V) \cap \mathfrak{p}^{*v} \cap \mathfrak{m}^v$ resulta que M'_v ainda tem característica σ para $X_\ell = \alpha_\ell$ $(\ell=1,\ldots,n)$. Êste resultado vale para todo ponto P_o de $W-W_1$; mas $W-W_1$ é formado por quasi todos os pontos de W, portanto, podemos afirmar que a matriz M'_v tem característica σ para $X_\ell = \eta_\ell$ $(\ell=1,\ldots,n)$. Então a última linha de M'_v é uma combinação linear, com coeficientes em $k(\eta)$, das primeiras N linhas, isto é, temos uma relação da forma

$$(27)\quad \bar{C}\left(\frac{\partial^v F}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\right)_{X=\eta} = \sum_{i=1}^{N} \bar{A}_i \left(\frac{\partial^v f_i}{\partial X_1^{\mu_1}\ldots\partial X_n^{\mu_n}\partial z_1^{\nu_1}\ldots\partial z_m^{\nu_m}}\right)_{X=\eta},$$

onde $\bar{C} \in k[\eta]$, $\bar{C} \neq 0$ e $\bar{A}_i \in k[\eta]$. Consideremos o elemento $F_2 = CF - \sum_{i=1}^{N} A_i f_i$, onde C e A_i são elementos de R_n tais que $\bar{C}$ = $\mathfrak{p}$-resíduo de C e $\bar{A}_i$ = $\mathfrak{p}$-resíduo de A_i. Tôdas as derivadas parciais mistas de ordens $0,1,\ldots,v-1$ de F_2 pertencem a $\mathfrak{p}$ (pois $F \in \mathfrak{p}^{(v)}$ e $f_i \in \mathfrak{p}^{(v)}$) e pela relação (27) tôdas as derivadas parciais mistas de ordem v também pertencem a $\mathfrak{p}$. Portanto, pelo teorema 2, teremos $F_2 \in \mathfrak{p}^{(v+1)}$, logo, $CF \in \mathfrak{p}^{(v+1)} + \mathfrak{J}(V)$, com $C \notin \mathfrak{p}$. (q.e.d.).

Seja $R = \mathfrak{R}[V]$ o anel das coordenadas de V; indicaremos por $\mathfrak{p}_1$ a imágem do ideal $\mathfrak{p} = \mathfrak{J}(W)$, pelo homomorfismo canônico de R_n sôbre R $(R = \mathfrak{R}[V] = R_n/\mathfrak{J}(V))$ e por $\mathfrak{p}(P/V)$ pelo mesmo homomorfismo.

Lema 10 - $\tau\mathfrak{p}^{(\nu)} \subset \mathfrak{p}_1^{(\nu)}$.

Demonstração - Seja ς um elemento pertencente a $\tau\mathfrak{p}^{(\nu)}$; teremos $\varsigma = \tau F$, com $F \in \mathfrak{p}^{(\nu)}$. Pela demonstração do lema 4 existe um elemento a de R_n, $a \notin \mathfrak{p}$, tal que $aF \in \mathfrak{p}^{\nu}$. D'aqui tiramos $\tau(aF) \in \mathfrak{p}_1^{\nu}$, logo, $\tau(a)\varsigma \in \mathfrak{p}_1^{(\nu)}$, com $\tau(a) \notin \mathfrak{p}_1$. Mas $\mathfrak{p}_1^{(\nu)}$ é um ideal primário pertencente ao ideal primo $\mathfrak{p}_1$, então de $\tau(a)\varsigma \in \mathfrak{p}_1^{(\nu)}$, com $\tau(a) \notin \mathfrak{p}_1$ vem $\varsigma \in \mathfrak{p}_1^{(\nu)}$. (q.e.d.).

Teorema 7 (O.Zariski) - Se um elemento ς de $\mathfrak{R}[V]$ pertencer a $[\mathfrak{p}(P/V)]^{\nu}$ para quasi todos os pontos P de W, então $\varsigma \in \mathfrak{p}_1^{(\nu)}$.

Demonstração - Seja F um elemento de R_n tal que $\tau F = \varsigma$. De $\varsigma \in [\mathfrak{p}(P/V)]^{\nu}$ vem $F \in (\mathfrak{J}(P))^{\nu} + \mathfrak{J}(V)$ para quasi todos os pontos P de W; pelo teorema 6, existe um elemento C de R_n, $C \notin \mathfrak{p}$, tal que $CF \in \mathfrak{p}^{(\nu)} + \mathfrak{J}(V)$. D'aqui tiramos $\tau(CF) \in \tau\mathfrak{p}^{(\nu)}$, logo, pelo lema 10, $\tau(C)\varsigma \in \mathfrak{p}_1^{(\nu)}$, com $\tau(C) \notin \mathfrak{p}_1$. Então $\varsigma \in \mathfrak{p}_1^{(\nu)}$. (q.e.d.).

Indicaremos por $Q(P/V)$ o anel de quocientes de $\mathfrak{R}[V]$ em relação ao ideal $\mathfrak{p}(P/V)$, $P \in V$; por $\mathfrak{m}(P/V)$ o único ideal máximal de $Q(P/V)$. Do mesmo modo $\mathfrak{m}(W/V)$ indicará o único ideal máximal de $Q(W/V)$ (anel de quocientes de $\mathfrak{R}[V]$ em relação ao ideal primo $\mathfrak{p}_1$). Demonstraremos o seguinte teorema, também devido a O.Zariski:

Teorema 8 - Se um elemento ς de $\mathfrak{J}(V)$ pertencer a $[\mathfrak{m}(P/V)]^{\nu}$ para quasi todos os pontos P de W, então $\varsigma \in [\mathfrak{m}(W/V)]^{\nu}$.

Demonstração - O elemento ς pode ser escrito sob a forma $\varsigma = \varsigma_1/\varsigma_0$, onde $\varsigma \in \mathfrak{R}[V]$ e $\varsigma_0 \notin \mathfrak{R}[V]$; como $\varsigma \in Q(P/V)$ podemos supôr que $\varsigma_0 \notin \mathfrak{m}(P/V)$ e, portanto, $\varsigma_0 \notin \mathfrak{m}(W/V)$. O elemento $\varsigma_1 = \varsigma_0\varsigma$ pertencerá a $[\mathfrak{p}(P/V)]^{\nu} = [\mathfrak{m}(P/V)]^{\nu} \cap R$ para quasi todos os pontos P de W, portanto, pelo teorema 7, teremos $\varsigma_1 = \varsigma_0\varsigma \in \mathfrak{p}_1^{(\nu)} = [\mathfrak{m}(W/V)]^{\nu} \cap R$. Isto nos mostra que $\varsigma_1 \in [\mathfrak{m}(W/V)]^{\nu}$ e como

$\zeta_0 \notin \mathfrak{p}_1$ teremos $\zeta = \zeta_1/\zeta_0 \in [m(W/V)]^{\nu}$. (q.e.d.).

No anel $R = \mathfrak{R}[V]$ consideremos o ideal $\mathfrak{k}_\nu = \bigcap_{P \in W} [\mathfrak{p}(P/V)]^{\nu}$ onde W é uma sub-variedade irredutível de V e a intersecção é tomada sôbre todos os pontos P de W. Pelo teorema 15 do cap.I existe um inteiro $\rho(\nu)$ tal que $\mathfrak{k}_\nu \subset \mathfrak{p}_1^{\rho(\nu)}$ e $\mathfrak{k}_\nu \notin \mathfrak{p}_1^{\rho(\nu)+1}$. Demonstraremos no teorema abaixo (também devido a O.Zariski) que a sucessão não decrescente $\rho(1), \ldots, \rho(\nu), \ldots$ não é limitada. Precisamente, temos o

Teorema 9 - O ideal $\mathfrak{k}_\nu = \bigcap_{P \in W} [\mathfrak{p}(P/V)]^{\nu}$ está contido numa potência $\mathfrak{p}_1^{\rho(\nu)}$ de $\mathfrak{p}_1$, onde $\lim_{\nu \to +\infty} \rho(\nu) = +\infty$.

Demonstração - Seja N um inteiro positivo e consideremos uma decomposição normal de $\mathfrak{p}_1^N$:

$$\mathfrak{p}_1^N = [\mathfrak{p}_1^{(N)}, \mathfrak{q}_1', \ldots, \mathfrak{q}_h'].$$

Temos: $\mathfrak{p}_1 \subset \mathfrak{p}_i' = \text{Rad. } \mathfrak{q}_i'$ $(i=1,\ldots,h)$. Seja ρ_i o expoente de $\mathfrak{q}_i'$ e ponhamos $\nu_0 = \max.(N, \rho_1, \ldots, \rho_h)$ e tomemos $\nu \geq \nu_0$. De $\zeta \in \mathfrak{k}_\nu$ vem $\zeta \in [\mathfrak{p}(P/V)]^{\nu}$ para todos os pontos P de W, logo, $\zeta \in \mathfrak{p}_1^{(\nu)}$ (teorema 7); mas $\mathfrak{p}_1^{(\nu)} \subset \mathfrak{p}_1^{(N)}$, portanto, $\zeta \in \mathfrak{p}_1^{(N)}$. De $\zeta \in \mathfrak{k}_\nu$ vem $\zeta \in [\mathfrak{p}(P/V)]^{\nu}$ para todos os pontos P da sub-variedade algébrica W_i, de W, determinanda pelo ideal $\mathfrak{p}_i'$, portanto, $\zeta \in \mathfrak{p}_i'^{(\nu)}$. Mas $\mathfrak{p}_i'^{(\nu)} \subset \mathfrak{p}_i'^{(\nu_0)} \subset \mathfrak{p}_i'^{(\rho_i)} \subset \mathfrak{q}_i$ (lema 4), portanto, $\zeta \in \mathfrak{q}_i$. Isto nos mostra que $\zeta \in \mathfrak{p}_1^{(N)} \cap \mathfrak{q}_1' \cap \ldots \cap \mathfrak{q}_h'$, logo, $\zeta \in \mathfrak{p}_1^N$. Portanto $\rho(\nu) \geq N$ para todo $\nu \geq \nu_0$. (q.e.d.).

Demonstraremos, a seguir, os teoremas 7 e 9 para o caso de uma sub-variedade redutível W de V. Indicaremos por $\mathfrak{A}$ a imágem do ideal $\mathfrak{J}(W)$, de R_n, pelo homomorfismo canônico τ de R_n sôbre $R = \mathfrak{R}[V] = R_n/\mathfrak{J}(V)$. Sejam $W_1, \ldots, W_h$ as componentes irredutíveis de W e ponhamos $\mathfrak{p}_i' = \tau(\mathfrak{J}(W_i))$. E' fácil ver que $\mathfrak{A} = \mathfrak{p}_1' \cap \ldots \cap \mathfrak{p}_h'$ é uma decomposição normal do ideal $\mathfrak{A}$. Ponhamos

$$\mathfrak{a}^{(\nu)} = \mathfrak{p}_1'^{(\nu)} \cap \ldots \cap \mathfrak{p}_h'^{(\nu)}.$$

Do teorema 7 resulta, imediatamente, o seguinte

Teorema 10 - Se um elemento ζ de R pertencer a $[\mathfrak{p}(P/V)]^{\nu}$ para quasi todos os pontos P de cada componente irredutível W_i de W, então ζ pertencerá ao ideal $\mathfrak{a}^{(\nu)}$.

Para demonstrar o teorema 9 quando W é uma sub-variedade redutível de V precisamos do seguinte

Lema 11 - Uma decomposição normal de $\mathfrak{a}^{\nu}$ é da forma $\mathfrak{a}^{(\nu)} \cap \mathfrak{b}_{\nu}$, onde todos os ideais primos do ideal $\mathfrak{b}_{\nu}$ são ideais primos de imersão de $\mathfrak{a}^{\nu}$.

Demonstração - Pela prop.13 do cap.I temos Rad. $\mathfrak{a}^{\nu}$ = = Rad. $\mathfrak{a}$, portanto, $\mathfrak{p}_1', \ldots, \mathfrak{p}_h'$ são os ideais primos isolados de $\mathfrak{a}^{\nu}$ (cap.I, prop.11). Para completar a demonstração falta provar que as componentes primárias de $\mathfrak{a}^{\nu}$ pertencentes aos ideais primos $\mathfrak{p}_1', \ldots, \mathfrak{p}_h'$ são, respectivamente, $\mathfrak{p}_1'^{(\nu)}, \ldots, \mathfrak{p}_h'^{(\nu)}$. Seja $\mathfrak{o}_i$ o anel de quocientes de R em relação ao ideal primo $\mathfrak{p}_i'$ e seja $\mathfrak{q}_i'$ a componente primária de $\mathfrak{a}^{\nu}$ pertencente ao ideal $\mathfrak{p}_i'$. Temos $\mathfrak{o}_i \mathfrak{a}^{\nu} = (\mathfrak{o}_i \mathfrak{a})^{\nu} = (\mathfrak{o}_i \cdot \mathfrak{p}_i')^{\nu}$ e $\mathfrak{o}_i \mathfrak{a}^{\nu} \cap R = (\mathfrak{o}_i \cdot \mathfrak{p}_i')^{\nu} \cap R =$ $= \mathfrak{p}_i'^{(\nu)}$ (prop.30, cap.I); mas $\mathfrak{q}_i = \mathfrak{o}_i \mathfrak{a}^{\nu} \cap R$ (cap.I, teorema 11), logo, $\mathfrak{q}_i = \mathfrak{p}_i'^{(\nu)}$. (q.e.d.).

Teorema 11 - O ideal $\mathfrak{b}_{\nu} = \bigcap_{P \in W} [\mathfrak{p}(P/V)]^{\nu}$ está contido numa potência $\mathfrak{a}^{\rho(\nu)}$ de $\mathfrak{a}$, onde $\lim_{\nu \to +\infty} \rho(\nu) = +\infty$.

Demonstração - Para cada inteiro ν ($\nu \geq 1$) faremos corresponder o inteiro $\rho(\nu)$ que verifica a condição $\mathfrak{b}_{\nu} \subset \mathfrak{a}^{\rho(\nu)}$ e $\mathfrak{b}_{\nu} \not\subset \mathfrak{a}^{\rho(\nu)+1}$. A sucessão $\rho(1), \ldots, \rho(\nu), \ldots$ é não decrescente. Provaremos que ela não é limitada. Seja N um inteiro positivo, temos $\mathfrak{a}^{N} = \mathfrak{a}^{(N)} \cap \mathfrak{b}_{\nu}$, onde os ideais primos de $\mathfrak{b}_{\nu}$ são os ideais primos de imersão de $\mathfrak{a}^{N}$ (lema 11). Seja ν' o máximo dos expoentes das componentes primárias de $\mathfrak{b}_{\nu}$ e ponhamos

$\nu_0 = \max.(N, \nu')$. Se $\mathfrak{P} \in \mathfrak{p}_\nu$, $\nu \geq \nu_0$, teremos (pelo teorema 10) $\mathfrak{P} \in \mathfrak{o}_\mathfrak{l}^{(\nu)} \subset \mathfrak{o}_\mathfrak{l}^{(\nu_0)} \subset \mathfrak{o}_\mathfrak{l}^{(N)}$ e também $\mathfrak{P} \in \mathfrak{p}$ (pois os ideais primos de $\mathfrak{p}$ são ideais primos de imersão de $\mathfrak{o}_\mathfrak{l}^N$, portanto, cada um deles contém, pelo menos um dos ideais primos $\mathfrak{p}_i'$ e, além disso, $\nu \geq \nu'$), portanto, $\mathfrak{P} \in \mathfrak{o}_\mathfrak{l}^N$. Isto nos mostra que $\rho(\nu) \geq N$ para todo $\nu \geq \nu_0$, logo, $\lim_{\nu \to +\infty} \rho(\nu) = +\infty$. (q.e.d.).

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

1. C.Chevalley - On the theory of local rings, Ann. of Math., vol. 44 (1943), pp.690-708.

2. I.S.Cohen - On the structure and ideal theory of complete local rings, Trans. of the A.M.S., vol.59 (1946), pp. 54-106.

3. I.S. Cohen and A. Seidenberg - Prime ideals and integral dependence, Bull. of the A.M.S., vol.52 (1946), pp.252 - 261.

4. J.A.Dieudonné - Teoria dos corpos comutativos, vols. I e II (notas de aulas por L.H.Jacy Monteiro) - Publicaçao da Sociedade de Matemática de S.Paulo (1946-1947).

5. W. Krull - Idealtheorie, Ergebnisse der Mathematik und ihrer Grenzgebiete, IV,3, Berlin, 1935.

6. W.Krull - Dimensionstheorie in Stellenringen, J. reine und angew. Math., vol.179 (1938), pp.204 - 226.

7. S.Mac-Lane - Modular fields, I, Separating transcendence basis, Duke Math. J., vol.5 (1939), pp.372-393.

8. L.H.Jacy Monteiro - Derivações de um corpo, Boletim da Sociedade de Matemática de S.Paulo, vol.2 (1947),pp.7-36.

9. F.K.Schmidt - Über die Erhaltung der Kettensätze der Idealtheorie bei beliebigen endlichen Köpererweiterungen, Math. Zeit., vol.41 (1936),pp.443-450.

10. F.K.Schmidt - Zusatz bei der Korrektur, J.reine und angew. Math., vol.177 (1937),pp.223-237.

11. O.Teichmüller - p-Algebren, Deutsche Mathematik, vol.1(1936), pp.362-368.

12. O.Teichmüller - Differentialrechnung bei Charakteristik p - J.reine und angew.Math., vol.175 (1936),pp.89-99.

13. B.L.van der-Waerden - Moderne Algebra, vols.I e II, 2ª edição, Berlin, 1937.

14. A.Weil - Foundations of Algebraic Geometry - American Mathematical Society, Colloquium Publications, vol.XXIX.

15. O.Zariski - Teoria dos ideais (notas de aulas por L.H.Jacy Monteiro) - 1945.

16. O.Zariski - Aneis locais generalizados e o conceito de ponto simples de uma variedade algébrica (notas de aulas por L.H.Jacy Monteiro) - 1945.

17. O.Zariski - Generalized semi-local rings, Summa Brasiliensis Mathematicae, 1947.

18. O.Zariski - A new proof of Hilbert's Nullstellensatz, Bull. of the A.M.S., vol.53 (1947),pp.362-368.

19. O.Zariski - The concept of a simple point of an abstract algebraic Variety, Trans. of the A.M.S., vol.62 (1947), pp.1-52.

I N D I C E.

CAPITULO V.

Pontos simples de uma variedade algébrica.

CAPITULO VI.

Sôbre as potências simbólicas de um ideal primo de um anel de polinômios.