O TEOREMA DE BEZOUT, O TEOREMA
FUNDAMENTAL DE MAX NOETHER E
APLICAÇÕES

Marcelo Reicher Soares

ORIENTADOR: Prof. Dr. Oziride Manzoli Neto

Dissertação apresentada ao Instituto
de Ciências Matemáticas de São Car-
los, da Universidade de São Paulo,
para obtenção do Título de Mestre
em Matemática.

SÃO CARLOS

1989

DEDICO esta Dissertação aos
meus pais, Olympio e Alzira;
à minha Esposa Ama e ao meu
Filho Rafael.

AGRADECIMENTOS

A jornada foi longa e felizmente, o número de pessoas que ajudaram foi bem maior do que aqueles que atrapalharam, no entanto, todos tiveram sua importância. Os primeiros suavizando o caminho difícil, os segundos fortalecendo nosso ímpeto, no intuito de chegarmos aqui.

Entre os que ajudaram, e eu os agradeço por isso, certamente estão: minha esposa, meu filho, meus pais, os colegas da pós-graduação, destacando-se: Aylton Pagamisse, Miriam P. Mendes, Rui M. O. Barros e Valter Locci. Faz-se necessário também, mencionar os colegas José L. Polli e Luiz R. A. Gabriel, bem como os companheiros do Departamento de Ciências da FEIS-UNESP. Ao meu amigo e orientador Oziride Manzoli Neto pela dedicação, competência e amizade que o distinguiu dentre meus mestres, um agradecimento especial. E a DEUS, sem o qual, nada do que foi feito far-se-ia.

Este trabalho contou com o apoio financeiro do CNPq, FAPESP e PICD-CAPES.

ABSTRACT

The purpose of this work is to show some applications of two important theorems, namely, Bezout's and Max Noether Fundamental Theorem.

Among these applications we have the classical Pascal's Theorem and Pappus's Theorems.

The (abelian) group structure on a cubic is presented in the final chapter.

We followed Fulton's book, Algebraic Curves, making the necessary details, to understand the above mentioned applications.

RESUMO

O propósito deste trabalho é mostrar algumas aplicações de dois teoremas importantes, quais sejam: Teorema de Bezout e Teorema Fundamental de Max Noether.

Entre as aplicações, nós temos os Teoremas clássicos de Pascal e de Pappa.

A estrutura (abeliana) de grupo numa cúbica é apresentada no último capítulo.

Nós seguimos o livro: Curvas Algébricas, de W. Fulton, fazendo os detalhes necessários para o entendimento das mencionadas aplicações.

I N D I C E

	Página
INTRODUÇÃO	01
CAPITULO I - ESPAÇOS AFINS	
1. Espaços Afins e Conjuntos Algébricos	03
2. Ideal de um Conjunto de Pontos	04
3. Componentes Irredutíveis de Conjuntos Algébricos ..	05
4. Hilbert Nullstellensatz	05
5. Variedades Afins - Troca Afim de Coordenadas	06
6. Funções Racionais e Anéis Locais	07
7. Anéis de Avaliação Discreta (D.V.R.) e Formas	08
8. Ideais Com Um Número Finito de Zeros	09
CAPITULO II - PROPRIÉDADES LOCAIS DE CURVAS PLANAS	
1. Curvas Planas - Multiplicidade	11
2. Multiplicidade e Anel Local	13
3. Número de Intersecção	13
CAPITULO III - VARIEDADES PROJETIVAS - ESPAÇO PROJETIVO	
1. Espaço Projetivo	18
2. Conjuntos Algébricos Projetivos	19
3. Variedades Projetivas e Afins	23
4. Curvas Planas Projetivas	25
5. Sistemas Lineares de Curvas	30

CAPITULO IV - TEOREMA DE BEZOUT E APLICAÇÕES

1. Teorema de Bezout	34
2. Aplicação no Estudo de Pontos Múltiplos	39

CAPITULO V - TEOREMA FUNDAMENTAL DE MAX NOETHER E APLICAÇÕES

1. O Teorema Fundamental de Max Noether	48
2. Algumas Aplicações do Teorema Fundamental de Max Noether	53

<i>BIBLIOGRAFIA</i>	60
---------------------------	----

INTRODUÇÃO

Os objetivos deste trabalho são: a demonstração e aplicação de dois Teoremas clássicos da teoria de Curvas Algébricas. São eles, o Teorema de Bezout e o Teorema Fundamental de Max Noether.

Estes Teoremas são abordados com um tratamento moderno, tendo como ferramenta principal a Álgebra Comutativa.

As demonstrações das propriedades do número de intersecção para duas curvas projetivas planas em um ponto são feitas por meio da redução do problema para o caso afim.

O texto referência utilizado foi o livro: Curvas Algébricas, de William Fulton. Outros textos também foram consultados para que as aplicações fossem "enriquecidas".

Conforme pode ser observado, a estrutura de grupo de uma cúbica foi feita em detalhe, pois é assunto interessante.

Pode-se notar também, que durante toda a dissertação, preocupamo-nos apenas com corpo de característica zero; aliás, tivemos também preferência pelos algebricamente fechado, pois assim não foi necessário fazer restrições a cada instante. Por isso, cumpre-nos alertar que muitos resultados valem em situações mais gerais, porém outros não.

Os Capítulos I, II e III nos dão uma introdução à linguagem aos fundamentos e uma coletânea de resultados válidos, no ambiente em que trabalharemos. O Capítulo IV contém a demonstração do Teorema de Bezout e sua aplicação no estudo de pontos múltiplos. Já o Capítulo V, contém a demonstração do Teorema Fundamental de Max Noether e sua aplicação

na demonstração dos Teoremas de Pascal e Pappas, além da descrição da estrutura de grupo (abeliano) sobre uma cúbica.

CAPITULO I - ESPAÇOS AFINS

Desejamos dar neste capítulo uma rápida introdução aos conceitos de espaços afins, conjuntos algébricos afins, variedades, etc. Os teoremas e resultados aqui apresentados estão provados nas bibliografias, geralmente no livro de: William Fulton - Curvas Algébricas. Só citaremos a bibliografia quando não estivermos nos referindo a tal livro. As demonstrações não são detalhadas aqui, pois não é nosso objetivo tornar óbvio o trabalho realizado na bibliografia, queremos sim caminhar rapidamente para espaços projetivos e trabalhar com os teoremas de: Bezout e Max Noether.

1. Espaços Afins e Conjuntos Algébricos

Seja K um corpo algebricamente fechado e de característica zero, indicamos por $A^n(K)$ ou simplesmente A^n o produto cartesiano de K com ele mesmo n -vezes; $K \times K \times \dots \times K$ (n -vezes).

$A^n(K)$ é chamado de n -espaço afim sobre K , e seus elementos $(a_1, \dots, a_n)$, $a_i \in K$, $i = 1, \dots, n$ de pontos.

Denotaremos por $K[x_1, \dots, x_n]$ o anel de polinômios a n -variáveis sobre K , assumimos as propriedades algébricas de $K[x_1, \dots, x_n]$ como por exemplo a de que é domínio de fatoração única e anel Noetheriano.

Dizemos que um ponto $(a_1, \dots, a_n) \in A^n(K)$ é zero de $F \in K[x_1, \dots, x_n]$ se $F(a_1, \dots, a_n) = 0$. O conjunto dos zeros de F é chamado de hipersuperfície definida por F e será denotado por $V(F)$. Uma hipersuperfície em $A^2(K)$ é chamada de curva plana afim. Se F é um polinômio de grau 1, $V(F)$ é chamado de

hiperplano.

Mais geralmente, temos que se I é um ideal em $K[x_1, \dots, x_n]$ então $V(I) = \{(a_1, \dots, a_n) \in A^n / F(a_1, \dots, a_n) = 0, \forall F, F \in I\}$. Um subconjunto $X \subset A^n(K)$ é um conjunto algébrico afim ou simplesmente conjunto algébrico, se $X = V(I)$, para algum I ideal de $K[x_1, \dots, x_n]$.

Citamos a seguir, algumas propriedades facilmente verificáveis:

- (1) Se I é um ideal de $K[x_1, \dots, x_n]$ gerado por um conjunto $S \subset K[x_1, \dots, x_n]$, então $V(I) = V(S)$.
- (2) Se $\{I_\alpha\}$ é uma coleção de ideais, então $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.
- (3) Se $I \subset J \subset K[x_1, \dots, x_n]$ são ideais, então $V(J) \subset V(I)$.
- (4) $V(F.G) = V(F) \cup V(G)$, $\forall F, G \in K[x_1, \dots, x_n]$ e $V(I) \cup V(J) = V(\{F.G / F \in I \text{ e } G \in J\})$.
- (5) $V(0) = A^n$, $V(1) = \emptyset$, $V(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\}$ para $a_i \in K$, assim qualquer conjunto finito em $A^n(K)$ é um conjunto algébrico.

2. Ideal de um Conjunto de Pontos

Para qualquer subconjunto $X \subset A^n(K)$ denotaremos por $I(X) = \{F \in K[x_1, \dots, x_n] / F(a_1, \dots, a_n) = 0, \text{ para todo } (a_1, \dots, a_n) \in X\}$. Segue algumas propriedades:

- (1) $X \subset Y \subset A^n(K) \Rightarrow I(Y) \subset I(X) \subset K[x_1, \dots, x_n]$.
- (2) $I(\emptyset) = K[x_1, \dots, x_n]$; $I(A^n(K)) = (0)$; se K é infinito $I(\{(a_1, \dots, a_n)\}) = (x_1 - a_1, \dots, x_n - a_n)$.
- (3) $I(V(S)) \supset S$ para qualquer conjunto S de polinômios, $V(I(X)) \supset X$ para qualquer conjunto X de pontos.
- (4) $V(I(V(S))) = V(S)$ para qualquer conjunto S de polinômios, $I(V(I(X))) = I(X)$ para qualquer conjunto X de pontos, assim

se V é conjunto algébrico $V = V(I(V))$, e se I é ideal de um conjunto algébrico $I = I(V(I))$.

3. Componentes Irredutíveis de Conjuntos Algébricos

Um conjunto algébrico $V \subset A^n$ é dito redutível se existirem conjuntos algébricos V_1, V_2 com $V = V_1 \cup V_2$ e $V_i \neq V$, $i = 1, 2$. Do contrário V é dito irredutível.

Proposição 1.1. Um conjunto algébrico V é irredutível se e somente se $I(V)$ é ideal primo.

Proposição 1.2. Se V é um conjunto algébrico em $A^n(K)$, então existem e são únicos os conjuntos algébricos irredutíveis $V_1, \dots, V_m$, tal que $V = V_1 \cup \dots \cup V_m$ e $V_i \not\subset V_j$ para todo $i \neq j$.

Os V_i da proposição acima são chamados de componentes irredutíveis de V e $V = V_1 \cup \dots \cup V_m$ é a decomposição de V em componentes irredutíveis.

4. Hilbert Nullstellensatz

O teorema de Nullstellensatz nos diz a exata relação entre ideais e conjuntos algébricos. Daremos primeiro a versão "fraca" e em seguida enunciaremos o Hilbert Nullstellensatz e alguns de seus corolários.

Proposição 1.3. (Weak Nullstellensatz) Se I é um ideal próprio em $K[x_1, \dots, x_n]$ então $V(I) \neq \emptyset$

Hilbert Nullstellensatz Seja I um ideal em $K[x_1, \dots, x_n]$, então $I(V(I)) = \text{rad}(I)$

onde $\text{rad}(I)$ = Ideal gerado por todos os $f \in K[x_1, \dots, x_n]$ para os

quais $\exists n \in \mathbb{N}$ tal que $f^n \in I$. Um ideal I é chamado de ideal radical se $\text{rad } I = I$.

Corolário 1. Se I é um ideal radical em $K[x_1, \dots, x_n]$, então $I(V(I)) = I$. Assim existe uma correspondência 1 a 1 entre ideais radicais e conjuntos algébricos.

Corolário 2. Se I é um ideal primo, então $V(I)$ é irredutível. Existe uma correspondência 1 a 1 entre ideais primos e conjuntos algébricos irredutíveis. Os ideais máximos correspondem a pontos.

Corolário 3. Existe uma correspondência 1 a 1 entre polinômios irredutíveis $F \in K[x_1, \dots, x_n]$ e hipersuperfícies irredutíveis $V(F)$ em $A^n(K)$.

Corolário 4. Seja I um ideal em $K[x_1, \dots, x_n]$, então $V(I)$ é um conjunto finito se e somente se $K[x_1, \dots, x_n]/I$ é um espaço vetorial de dimensão finita sobre K . Se isto ocorre, o número de pontos em $V(I)$ é $\leq \dim_K K[x_1, \dots, x_n]/I$.

5. Variedades Afins - Troca Afim de Coordenadas

Uma variedade afim $V \subset A^n(K)$ é qualquer conjunto algébrico V irredutível em $A^n(K)$. Se V é variedade, $I(V)$ é primo e chamaremos de anel coordenada de V ao domínio $\Gamma(V) = K[x_1, \dots, x_n]/I(V)$. Lembremos que V é variedade $\Rightarrow V$ irredutível $\Rightarrow I(V)$ primo.

Uma aplicação $T: V \rightarrow W$, onde $V \subset A^n$ e $W \subset A^m$ é chamada de aplicação polinomial, se $T = (T_1, \dots, T_m)$ e cada $T_i \in K[x_1, \dots, x_n]$.

Uma troca afim de coordenadas em A^n é uma aplicação polinomial $T: A^n \rightarrow A^n$ tal que $T = (T_1, \dots, T_n)$, cada T_i é um polinômio de grau 1 em $K[x_1, \dots, x_n]$ e T é uma bijeção; de uma maneira geral $T = T''_0 T'$, onde T' é uma aplicação linear inversível e T'' uma translação. Note que cada $T_i = \sum a_{ij} x_j + a_{i0}$; $T'_i = \sum a_{ij} x_j$; $T''_i = x_i + a_{i0}$. Se V é um conjunto algébrico $V^T = T^{-1}(V) = V(I^T)$, onde $I = I(V)$ e T uma troca projetiva de coordenadas, I^T é o ideal gerado pelo conjunto $\{F^T = F_0 T / F \in I\}$.

6. Funções Racionais e Aneis Locais

Se V é uma variedade em A^n e $\Gamma(V)$ seu anel coordenada, desde que $\Gamma(V)$ é domínio, nós podemos formar seu corpo quociente que denotaremos por $K(V)$ e o chamaremos de corpo de funções racionais sobre V . Um elemento de $K(V)$ é uma função racional sobre V .

Se $f \in K(V)$, dizemos que f está definido em $P \in V$, se $f = (a + I(V)) / (b + I(V))$, com $b(P) \neq 0$. Notemos que existem várias maneiras de escrevermos f como quociente de elementos de $\Gamma(V)$, f estará definida em P se existir um "denominador" para f que não se anula em P .

Sendo $P \in V$, definimos $O_P(V)$ como sendo o subconjunto de $K(V)$ formado por todos os $f \in K(V)$, tal que f está definida em P . É fácil verificar que $O_P(V)$ é um subanel de $K(V)$ contendo $\Gamma(V)$. Na realidade temos $K \subset \Gamma(V) \subset O_P(V) \subset K(V)$. $O_P(V)$ é chamado de anel local de V em P .

Se $f \in O_P(V)$, definimos o valor de f em P , $f(P)$ como segue: escrevemos $f = a/b$, $a, b \in \Gamma(V)$, $b(P) \neq 0$ e fazemos $f(P) = a(P)/b(P)$, como $\Gamma(P)$ é UFD, pois $K[x_1, \dots, x_n]$ é UFD,

é fácil chegar que $f(P)$ independe da escolha de a e b .

$M_P(V) = \{f \in O_P(V) / f(P) = 0\}$ é chamado de ideal maximal de V em P ; ele é o Kernel do homomorfismo avaliação $f \rightarrow f(P)$ de $O_P(V)$ em K . Assim $O_P(V)/M_P(V) \cong K$. Um elemento $f \in O_P(V)$ é uma unidade em $O_P(V)$, se e somente se $f(P) \neq 0$. Assim $M_P(V) = \{\text{não unidade de } O_P(V)\}$.

Sabemos da álgebra, que um anel local é aquele em que o conjunto das não unidades formam um ideal. Tal anel tem um único ideal maximal que contém todos os outros ideais próprios do anel. Sendo assim, temos que $O_P(V)$ é um anel local com ideal maximal $M_P(V)$. Este ideal tem proeminente papel no estudo moderno de variedades algébricas.

Proposição 1.4. $O_P(V)$ é um domínio local Noetheriano.

Se T é uma troca afim de coordenadas, não é difícil provar que $O_P(V^T) \cong O_Q(V)$, onde $Q \in V$ e $T(Q) = P$.

7. Anéis de Avaliação Discreta (D.V.R.) e Formas

Se R é um domínio que não é corpo, são equivalentes:

- (1) R é Noetheriano e local, seu ideal maximal é principal.
- (2) Existe um elemento irredutível $t \in R$, tal que todo não zero $z \in R$ pode ser escrito de maneira única como $z = ut^n$, onde u é unidade em R e n um inteiro não negativo.

Um anel satisfazendo as condições acima é chamado de Anel de Avaliação Discreta (D.V.R.). O elemento t é chamado de parâmetro uniformizador de R . Se K for o corpo quociente do domínio R , então todo $z \in K$ pode ser escrito como $z = ut^n$, com u unidade em R e $n \in \mathbb{Z}$, o expoente n é chamado de ordem de z e a função $\text{ord}: K \rightarrow \mathbb{Z} \cup \{\infty\}$, tal que $\text{ord}(z) = n$ e

$\text{ord}(a) = \infty \iff a = 0$ define $R = \{z \in K / \text{ord}(z) \geq 0\}$ e $M = \{z \in K / \text{ord}(z) > 0\}$. Mostraremos, mais à frente, sobre que condições $O_p(V)$ como D.V.R.

Se R é um domínio e $F \in R[x_1, \dots, x_n]$ é uma forma, definimos $F_* \in R[x_1, \dots, x_n]$ pondo $F_* = F(x_1, \dots, x_n, 1)$. Reciprocamente, para qualquer polinômio $f \in R[x_1, \dots, x_n]$ de grau d escrevemos $f = f_0 + f_1 + \dots + f_d$, onde f_i é forma de grau i e definimos $f^* \in R[x_1, \dots, x_{n+1}]$ colocando $f^* = x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \dots + f_d = x_{n+1}^d f(x_1/x_{n+1}, \dots, x_n/x_{n+1})$, f^* é uma forma de grau d . Tal processo é conhecido por desomogenização e homogenização, respectivamente, com respeito a x_{n+1} .

Proposição 1.5. (1) $(F.G)_* = F_* G_*$; $(f.g)^* = f^* g^*$.

(2) Se r é a maior potência de x_{n+1} que divide F , então $x_{n+1}^r (F_*)^* = F$; $(f^*)_* = f$.

(3) $(F+G)_* = F_* + G_*$; $x_{n+1}^t (f+g)^* = x_{n+1}^r f^* + x_{n+1}^s g^*$, onde $r = \deg(g)$; $s = \deg(f)$ e $t = r + s - \deg(f+g)$.

Corolário. A menos de x_{n+1} , fatorar uma forma $F \in R[x_1, \dots, x_{n+1}]$ é o mesmo que fatorar $F_* \in R[x_1, \dots, x_n]$. Em particular, se $F \in K[x, y]$ é uma forma, então F fatora-se em produto de fatores lineares.

8. Ideais Com Um Número Finito de Zeros

Enunciaremos agora, uma proposição que terá muita utilidade posteriormente.

Proposição 1.6. Se I é um ideal de $K[x_1, \dots, x_n]$ para o qual $V(I) = \{P_1, \dots, P_N\}$ é finito, então $K[x_1, \dots, x_n]/I$

é isomorfo a $\prod_{i=1}^N O_{P_i}(A^n)/IO_{P_i}(A^n)$ (produto direto de anéis).

Corolário 1. $\dim_K(K[x_1, \dots, x_n]/I) = \sum_{i=1}^N \dim_K(O_{P_i}(A^n)/IO_{P_i}(A^n))$.

Corolário 2. Se $V(I) = \{P\}$, então $K[x_1, \dots, x_n]/I$ é isomorfo a $O_P(A^n)/IO_P(A^n)$.

CAPITULO II - PROPRIEDADES LOCAIS DE CURVAS PLANAS

1. Curvas Planas - Multiplicidade

Dizemos que dois polinômios $F, G \in K[x,y]$ são equivalentes, se $F = \lambda G$, para algum não zero $\lambda \in K$. Nós redefinimos uma curva plana afim como sendo os zeros de uma classe de equivalência de polinômios, não constantes, sob a relação de equivalência acima.

Por abuso de linguagem, falaremos: "a curva plana $y^2 - x^3$ ". O grau de uma curva é o grau de um polinômio que define essa curva, uma curva de grau 1, é uma reta, assim falamos "a reta $ax + by + c$ " ou "a reta $ax + by + c = 0$ ".

Se $F = \prod F_i^{e_i}$, onde F_i são os fatores irredutíveis de F , chamaremos os F_i de componentes de F e e_i a multiplicidade da componente F_i .

F_i é simples se $e_i = 1$ e múltipla do contrário.

Se F é irredutível, então $V(F)$ é variedade em A^2 , uma vez que (F) é primo. Nós escreveremos então $\Gamma(F)$, $K(F)$, $O_P(F)$ no lugar de $\Gamma(V(F))$, $K(V(F))$, $O_P(V(F))$.

Se F for uma curva e $P = (a,b) \in F$, então P será chamado de ponto simples de F se $F_x(P)$ ou $F_y(P) \neq 0$. Neste caso a reta $F_x(P)(x-a) + F_y(P)(y-b) = 0$ é chamada de reta tangente a F em P . Um ponto que não é simples é chamado múltiplo ou singular. Uma curva com somente pontos simples é chamada de curva não singular.

Sejam: F qualquer curva e $P = (0,0)$, escrevemos $F = F_m + F_{m+1} + \dots + F_n$, onde F_i são formas de graus i em $K[x,y]$, $F_m \neq 0$, nós definimos m como sendo a multiplicidade de F

em $P = (0,0)$ e denotamos $m_P(F) = m$.

Notemos que $P \in F$, se e somente se, $m_P(F) > 0$, uma vez que se F_i é uma forma de grau i , $i \geq 1$, então $F_i(0,0) = 0$. Usando regras de derivação, é fácil chegar que P é ponto simples sobre F , se e somente se, $m_P(F) = 1$, e neste caso F_1 é exatamente a reta tangente a F em P . Se $m_P(F) = 2$, então P é chamado de ponto duplo, se $m_P(F) = 3$, um ponto triplo.

Desde que F_m é uma forma de grau m em duas variáveis, nós podemos escrever $F_m = \Pi L_i^{\Gamma_i}$, onde as L_i são retas distintas (prop. 1.5. corolário). As L_i são chamadas retas tangentes a F em $P = (0,0)$ e Γ_i é a multiplicidade da tangente. L_i é uma tangente simples se $\Gamma_i = 1$, dupla se $\Gamma_i = 2$, etc. Se F tem $m = m_P(F)$ tangentes distintas (simples) em P , nós dizemos que P é um ponto múltiplo ordinário de F . Um ponto duplo ($m_P(F) = 2$) ordinário é chamado de node. Por conveniência, nós dizemos que uma reta sobre P é uma tangente de multiplicidade zero, se ela não for tangente a F em P .

Se tivermos $F = \Pi F_i^{e_i}$, seguirá que $m_P(F) = \sum e_i m_P(F_i)$, uma vez que o termo de menor grau de F é o produto dos termos de menor grau de seus fatores.

Para estendermos estas definições para um ponto $P = (a,b) \neq (0,0)$, seja T a translação que leva $(0,0)$ em P , isto é, $T(x,y) = (x+a, y+b)$, então $F^T = F_0 T = F(x+a, y+b)$ e definimos $m_P(F)$ como sendo $m_{(0,0)}(F^T)$, isto é, escrevemos $F^T = G_m + G_{m+1} + \dots + G_n$, G_i formas de grau i e temos $m_P(F) = m_{(0,0)}(F^T) = m$. Se $G_m = \Pi L_i^{\Gamma_i}$, $L_i = \alpha_i \cdot x + \beta_i \cdot y$ as retas $\alpha_i(x-a) + \beta_i(y-b)$ são definidas como retas tangentes a F em P e Γ_i é a multiplicidade da tangente. Notemos que T leva os pontos de F^T em pontos de F , ($T(V(F_0 T)) = V(F)$) e as tangentes a F^T em $(0,0)$ nas tangentes a F em P . Desde que $F_x^T(P) =$

$F_x(P) = F_x^T(0,0)$ e $F_y(P) = F_y^T(0,0)$, P é um ponto simples sobre $F \iff m_P(F) = 1$, e as duas definições de retas tangentes para os pontos simples coincidem.

2. Multiplicidade e Anel Local

Se F for uma curva plana irredutível, $P \in F$, então enunciaremos proposições que relacionam a multiplicidade de F em P com o anel local $O_P(F)$. Adotaremos a seguinte convenção. Se $G \in K[x,y]$ sua imagem em $K[x,y]/(F)$ será g .

Proposição 2.1. P é um ponto simples de F , se e somente se, $O_P(F)$ é um anel de avaliação discreta, e neste caso, se $L = ax + by + c$ é qualquer reta sobre P que não é tangente a F em P , então a imagem l de L em $O_P(F)$ é um parâmetro uniformizador de $O_P(F)$.

Proposição 2.2. Seja P um ponto sobre uma curva irredutível F , então $m_P(F) = \dim_K(M_P^n(F)/M_P^{n+1}(F))$ para n suficientemente grande. Em particular, a multiplicidade de F em P depende somente do anel local $O_P(F)$.

3. Número de Intersecção

Definiremos agora, número de intersecção de duas curvas em um ponto, e afirmaremos que a definição dada satisfaz a 9 propriedades, que daremos a seguir. O cálculo do número de intersecção não é feito pela definição, e sim pelas propriedades e é relativamente simples, dependendo somente de manipulações de polinômios, como mostraremos em exemplos.

A demonstração pormenorizada de que a definição satisfaz as propriedades é feita em W.F. - Curvas Algébricas, e não a faremos aqui. No entanto, nos capítulos seguintes definiremos número de intersecção entre duas curvas planas projetivas em um ponto, e mostraremos que tal definição satisfaz a 8 propriedades; isto será feito por recorrência ao que enunciaremos aqui e usando isomorfismos, faremos os detalhes. Assim, o que se segue é fundamental.

Definição: Existe um único número de intersecção $I(P, F \cap G)$ definido para todas as curvas planas afins F, G e todo ponto $P \in A^2$, ele é dado por $I(P, F \cap G) = \dim_k (O_P(A^2)/(F, G))$.

A partir da definição de número de intersecção como a dimensão do espaço vetorial $(O_P(A^2)/(F, G))$, afirmamos que esta satisfaz 9 propriedades, que enunciaremos a seguir e a demonstração de que a definição é única e satisfaz as propriedades, esta em [2].

Dizemos que F e G se interceptam propriamente em P , se F e G não têm componente comum que passa por P .

Propriedade (1) $I(P, F \cap G)$ é um inteiro não negativo para qualquer F, G e P , tal que F e G se interceptam propriamente em P . $I(P, F \cap G) = \infty$ se F e G não se interceptam propriamente em P .

Propriedade (2) $I(P, F \cap G) = 0$, se e somente se, $P \notin F \cap G$. $I(P, F \cap G)$ depende somente das componentes de F e G que passam por P .

Propriedade (3) Se T é uma troca afim de coordenadas sobre A^n e $T(Q) = P$, então $I(Q, F^T \cap G^T) = I(P, F \cap G)$.

Propriedade (4) $I(P, F \cap G) = I(P, G \cap F)$.

Dizemos que F e G se interceptam transversalmente em P , se P é um ponto simples para F e G e se a reta tangente a F em P é diferente da reta tangente a G em P . Nós temos que:

Propriedade (5) $I(P, F \cap G) \geq m_P(F) \cdot m_P(G)$ com a igualdade ocorrendo, se e somente se, F e G não têm retas tangentes em comum em P .

Assim se F e G interceptam-se transversalmente em P , temos $I(P, F \cap G) = 1$.

O número de intersecção adiciona-se quando tomamos união de curvas.

Propriedade (6) Se $F = \prod_i^{\Gamma_i} F_i$ e $G = \prod_j^{S_j} G_j$, então $I(P, F \cap G) = \sum_{i,j} \Gamma_i S_j I(P, F_i \cap G_j)$.

Propriedade (7) $I(P, F \cap G) = I(P, F \cap (G + AF))$ para qualquer $A \in K[x, y]$.

Propriedade (8) Se P é um ponto simples sobre F , então $I(P, F \cap G) = \text{ord}_P^F(G)$.

Lembremos aqui, que se P é ponto simples, então $\mathcal{O}_P(F)$ é D.V.R. (proposição 2.1.) e em um D.V.R. temos uma função ordem. Esta, em particular, já foi tratada quando definimos D.V.R. (Capítulo I, parágrafo 7).

Propriedade (9) Se F e G não têm componentes comuns, então $\sum_P I(P, F \cap G) = \dim_K (K[x, y] / (F, G))$.

Não provaremos que a definição dada satisfaz as 9 propriedades, diremos no entanto, que as propriedades 2, 4 e 7

são óbvias, uma vez que a dimensão do espaço vetorial que define número de intersecção está diretamente ligada ao ideal gerado pelas curvas F, G em $O_P(A^2)$. A proposição 1.6 e seu corolário são fundamentais na prova das propriedades (1) e (9). Para a propriedade (6), devemos usar "seqüências exatas". A propriedade (3) vem do fato de que troca afim de coordenadas dá origem a isomorfismo de anéis locais. A propriedade (8) é uma consequência quase que direta do fato de $O_P(F)$ ser DVR e a propriedade (5), a mais difícil de ser demonstrada, demandando algum trabalho com "seqüências exatas e de lemas auxiliares".

Damos a seguir um exemplo do cálculo do número de intersecção entre duas curvas, usando as propriedades dadas.

Exemplo: Calcule $I(P, E \cap F)$, onde $P=(0,0)$, $E=(x^2+y^2)+3x^2y-y^3$
 $F=(x^2+y^2)^3 - 4x^2y^2$.

Usando a propriedade (7): $I(P, F \cap G) = I(P, F \cap (G+AF))$, substituímos F por $F-(x^2+y^2)E=(x^2+y^2)^3-4x^2y^2-(x^2+y^2)^3-(x^2+y^2)(3x^2y-y^3)=y|(x^2+y^2)(y^2-3x^2)-4x^2y|=y.G$.

Assim $I(P, E \cap F)=I(P, E \cap F-(x^2+y^2)E)=(P, E \cap yG) \stackrel{\text{Propriedade 6}}{=} I(P, E \cap y)+I(P, E \cap G)$.

Calculemos $I(P, E \cap G)$ substituindo G por $G+3E=(x^2+y^2)(y^2-3x^2)-4x^2y+3|(x^2+y^2)^2+3x^2y-y^3|=y(5x^2-3y^2+4y^3+4x^2y)=y.H$.

Assim $I(P, E \cap G)=I(P, E \cap (G+3E))=I(P, E \cap yH)=I(P, E \cap y)+I(P, E \cap H)$; logo $I(P, E \cap F)=2I(P, E \cap y)+I(P, E \cap H)$, porém

$$\begin{aligned} \text{i)} \quad I(P, E \cap y) &= I(P, (x^4+2x^2y^2+y^4+3x^2y-y^3) \cap y) \\ &= I(P, x^4+y(2x^2y+y^3+3x^2-y^2) \cap y) \stackrel{\text{propriedade 7}}{=} \\ &= I(P, x^4 \cap y) \stackrel{\text{Propriedade 5}}{=} 4I(P, x \cap y) \end{aligned}$$

ii) $E=(x^2+y^2)^2+3x^2y-y^3$ e $H=5x^2-3y^2+4y^3+4x^2y$ e as

tangentes a E e H são $3x^2y - y^3 = y(3x^2 - y^2) = y(\sqrt{3}x + y)(\sqrt{3}x - y)$ de E
 $5x^2 - 3y^2 = (\sqrt{5}x + \sqrt{3}y)(\sqrt{5}x - \sqrt{3}y)$ de H. Logo E e H não têm tangen-
tes comuns. Pela propriedade (5), temos que $I(P, E \cap H) =$
 $= m_P(E) \cdot m_P(H) = 3 \cdot 2 = 6$.

De **i)** e **ii)** vem que $I(P, E \cap F) = 2I(P, E \cap y) + I(P, E \cap H) =$
 $= 2(4) + 6 = 14$.

CAPITULO III - VARIEDADES PROJETIVAS - ESPAÇO PROJETIVO

1. Espaço Projetivo

No espaço projetivo afim, temos curvas que não se interceptam, porém têm direções assintóticas, isto é, seus pontos tornam-se arbitrariamente próximos sem, no entanto, serem comuns. A idéia de "ampliar" o espaço afim, de maneira a fazer com que tais curvas se interceptem "no infinito", deu origem ao espaço projetivo.

Um n -espaço projetivo sobre um corpo K , denotado por $P^n(K)$ ou simplesmente P^n , é definido como sendo o conjunto de todas as retas por $(0, \dots, 0)$ em $A^{n+1}(K)$. Qualquer ponto $(x) = (x_1, \dots, x_{n+1}) \neq (0, \dots, 0)$ determina uma única tal reta, a saber $\{(\lambda x_1, \dots, \lambda x_{n+1}) / \lambda \in K\}$. Dois pontos (x) e (y) determinam a mesma reta se existir um elemento não nulo $\lambda \in K$, tal que $x_i = \lambda y_i$, $\forall i$, $i = 1, \dots, n+1$; diremos que (x) e (y) são equivalentes, neste caso. Então, P^n pode ser pensado como o conjunto das classes de equivalência dos pontos em $A^{n+1} - \{(0, \dots, 0)\}$.

Os elementos de P^n serão chamados pontos. Se um ponto $P \in P^n$ é determinado como acima por algum $(x_1, \dots, x_{n+1}) \in A^{n+1}$, nós dizemos que $(x_1, \dots, x_{n+1})$ é um conjunto de coordenadas homogêneas para P . Notemos que se indicarmos $P = (x_1, \dots, x_{n+1}) \in P^n$ teremos que ao menos para um i , $i = 1, \dots, n+1$, $x_i \neq 0$, definimos então $U_i = \{(x_1, \dots, x_{n+1}) \in P^n / x_i \neq 0\}$ e cada $P \in U_i$ tem um único conjunto de coordenadas homogêneas, tal que $P = (x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_{n+1})$.

Se definirmos $\phi_i: A^n \rightarrow U_i$ por $\phi_i(a_1, \dots, a_n) =$

$= (a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$, então ϕ_i marcará uma correspondência entre pontos de A^n e pontos de U_i . Tal correspondência será um a um. Notemos então que $P^n = \bigcup_{i=1}^{n+1} U_i$, assim P^n é coberto por $n+1$ conjuntos; cada um deles em correspondência 1 a 1 com o n -espaço afim.

Por conveniência, nós nos concentraremos sobre U_{n+1} e denotaremos por $H_\infty = P^n - U_{n+1} = \{(x_1, \dots, x_{n+1} / x_{n+1} = 0\}$, este é chamado de hiperplano no infinito. A correspondência $(x_1, \dots, x_n, 0) \longleftrightarrow (x_1, \dots, x_n)$ mostra que H_∞ pode ser identificado com P^{n-1} . Assim, $P^n = U_{n+1} \cup H_\infty$.

Estaremos interessados, particularmente, em $P^2(K)$ ou plano projetivo $P^2(K) = \{(x, y, 1) / (x, y) \in A^2\} \cup \{(x, y, 0) / (x, y) \in P^1\}$, neste, H_∞ é chamado reta no infinito.

2. Conjuntos Algébricos Projetivos

Um ponto $P \in P^n$ é um zero de um polinômio $F \in K[x_1, \dots, x_{n+1}]$ se $F(x_1, \dots, x_{n+1}) = 0$, para toda escolha de coordenadas homogêneas $(x_1, \dots, x_{n+1})$ de P ; então nós escrevemos $F(P) = 0$. Se nós escrevermos F como uma soma de formas, cada forma se anulará para qualquer conjunto de coordenadas homogêneas de P , caso $F(P) = 0$.

Para qualquer conjunto S de polinômios em $K[x_1, \dots, x_{n+1}]$ nós escreveremos $V(S) = \{P \in P^n / P \text{ é zero de cada } F \in S\}$. Se I for ideal gerado por S , obviamente $V(S) = V(I)$. Se $I = (F^1, \dots, F^r)$, onde $F^i = \sum_j F_j^i$, F_j^i forma de grau j , então $V(I) = V(\{F_j^i\})$. Logo $V(S) = V(\{F_j^i\})$ é o conjunto dos zeros de um número finito de formas.

Definição: Um conjunto algébrico projetivo é aquele formado pelos zeros de um número finito de formas.

Se $X \subset \mathbb{P}^n$ nós escreveremos $I(X) = \{F \in K[x_1, \dots, x_{n+1}] / \text{todo } P \in X \text{ é zero de } F\}$, $I(X)$ é um ideal chamado ideal de X .

Um ideal $I \subset K[x_1, \dots, x_{n+1}]$ é chamado homogêneo, se para todo $F = \sum_{i=0}^m F_i \in I$, F_i forma de grau i , nós tivermos $F_i \in I$. Para qualquer $X \subset \mathbb{P}^n$, $I(X)$ é um ideal homogêneo.

Proposição 3.1. Um ideal $I \subset K[x_1, \dots, x_{n+1}]$ é homogêneo, se e somente se é gerado por um número finito de formas.

Um conjunto algébrico $V \subset \mathbb{P}^n$ é irredutível se não for a união de dois conjuntos algébricos "menores".

Proposição 3.2. $V \subset \mathbb{P}^n$ é irredutível, se e somente se $I(V)$ é primo.

Um conjunto algébrico irredutível em $\mathbb{P}^n$ é chamado de Variedade Projetiva. Qualquer conjunto algébrico projetivo pode ser escrito de maneira única como a união de variedades projetivas, suas componentes irredutíveis.

As operações:

$$\left\{ \begin{array}{l} \text{ideais homogêneos} \\ \text{em } K[x_1, \dots, x_{n+1}] \end{array} \right\} \begin{array}{c} \xrightarrow{U} \\ \xleftarrow{I} \end{array} \left\{ \begin{array}{l} \text{conjuntos algébricos} \\ \text{em } \mathbb{P}^n(K) \end{array} \right\}$$

satisfazem propriedades semelhantes àquelas descritas no capítulo I, parágrafos 1 e 2. Usaremos as notações V_P, I_P para as operações projetivas e V_a, I_a para as operações afins quando houver risco de confusão.

Proposição 3.3. (Nullstellensatz Projetivo) Seja I um ideal homogêneo em $K[x_1, \dots, x_{n+1}]$, então:

(1) $V_P(I) = \emptyset$, se e somente se $\exists N \in \mathbb{Z}_+$, tal

que I contém todas as formas de grau $> N$.

(2) Se $V_P(I) \neq \emptyset$, então $I_P(V_P(I)) = \text{rad}(I)$.

Existe uma correspondência um a um entre hipersuperfícies projetivas $V = V(F)$ e as formas (não constantes) F que define V , desde que tomemos o cuidado de fazer com que F não tenha fatores múltiplos (F é determinada a menos de multiplicação por $\lambda \in K$, $\lambda \neq 0$). Hipersuperfícies irredutíveis corresponde a formas irredutíveis. Um hiperplano é uma hipersuperfície definida por uma forma de grau um.

Se V é uma variedade projetiva em P^n , $I(V)$ é ideal primo, logo o anel $\Gamma_h(V) = K[x_1, \dots, x_{n+1}] / I(V)$ é um domínio, e este é chamado de anel coordenada homogênea de V .

Mais geralmente, se I é qualquer ideal homogêneo em $K[x_1, \dots, x_{n+1}]$, denotamos $\Gamma = K[x_1, \dots, x_{n+1}] / I$. Um elemento $f \in \Gamma$ será chamado uma forma de grau d se existir uma forma F de grau d em $K[x_1, \dots, x_{n+1}]$, cujo resíduo em Γ é f .

Proposição 3.4. Todo elemento $f \in \Gamma$ pode ser escrito unicamente como $f = f_0 + \dots + f_m$, f_i forma de grau i .

Denotaremos por $K_h(V)$ o corpo quociente de $\Gamma_h(V)$, ele é chamado corpo das funções homogêneas de V . Os elementos de $\Gamma_h(V)$, excetuando-se as constantes, não definem funções sobre V , igualmente muitos elementos de $K_h(V)$ não podem ser pensados como funções.

No entanto, se f e g são formas em $\Gamma_h(V)$ de mesmo grau d , então f/g define uma função, no mínimo onde g não é zero, pois $f(\lambda(x))/g(\lambda(x)) = \lambda^d f(x)/\lambda^d g(x) = f(x)/g(x)$. Assim, o valor de f/g independe da escolha de coordenadas homogêneas.

O corpo de funções de V , denotado $K(V)$, é definido por $\{z \in K_h(V) / \text{para algumas formas } f, g \in \Gamma_h(V) \text{ de mesmo grau } z = f/g\}$. Não é difícil verificar que $K(V)$ é subcorpo de $K_h(V)$. Aí temos, na verdade, $K \subset K(V) \subset K_h(V)$, porém $\Gamma_h(V) \not\subset K(V)$. Elementos de $K(V)$ são chamados de funções racionais sobre V .

Dizemos que $z \in K(V)$ está definida em $P \in V$ se z pode ser escrito como $z = f/g$, f e g formas de mesmo grau e $g(P) \neq 0$. Nós denotamos $O_P(V) = \{z \in K(V) / z \text{ está definida em } P\}$, este é um subanel de $K(V)$; ele é um anel local pois o conjunto das não unidade forma um ideal, seu ideal maximal é denotado por $M_P(V) = \{z / z = f/g, g(P) \neq 0, f(P) = 0\}$.

O valor $z(P)$ de uma função $z \in O_P(V)$ está bem definido.

Se $T: A^{n+1} \longrightarrow A^{n+1}$ é uma troca linear de coordenadas, então T leva retas sobre a origem em retas sobre a origem. Dessa forma, T determina uma aplicação de P^n em P^n , chamada troca projetiva de coordenadas. Se V é um conjunto algébrico de P^n , então $V^T = T^{-1}(V)$ também é um conjunto algébrico em P^n (desde que $V^T = T^{-1}(V) = V(\{F_0 T / F \in I\}) = V(I^T)$). Se $V = V(F_1, \dots, F_r)$ e $T = (T_1, \dots, T_{n+1})$, T_i formas de grau 1, então $V^T = V(F_1^T, \dots, F_r^T)$, onde $F_i^T = F_i(T_1, \dots, T_{n+1})$, V é variedade, se e somente se, V^T é variedade e T induz isomorfismos: $\Gamma_h(V) \cong \Gamma_h(V^T)$; $K(V) \cong K(V^T)$; $O_P(V) \cong O_Q(V^T)$ se $T(Q) = P$.

Dado um ponto $P \in P^n$, podemos pensá-lo como um vetor não nulo de A^{n+1} e pensar uma troca projetiva de coordenadas T de P^n , como isomorfismo de A^{n+1} . Com esta idéia e as propriedades de transformações lineares entre espaços vetoriais, podemos fazer várias afirmações, dentre elas:

Afirmção 1: Sejam P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) três pontos em P^2

que não estão na mesma reta, então existe uma troca projetiva de coordenadas $T:P^2 \longrightarrow P^2$, tal que $T(P_i) = Q_i$, $i = 1, 2, 3$.

Afirmção 2: Duas retas quaisquer em P^2 interceptam-se em um ponto (e cabe dizer que uma reta por P e Q em P^2 é o conjunto $\{\alpha P + \beta Q / \alpha, \beta \in K, \alpha \neq 0 \text{ ou } \beta \neq 0\}$ que corresponde em A^3 a um hiperplano pela origem, exceto a própria origem).

Afirmção 3: Sejam L_1, L_2, L_3 (resp. M_1, M_2, M_3) retas em $P^2(K)$ que não passam sobre um mesmo ponto, então existe uma troca projetiva de coordenadas $T:P^2 \longrightarrow P^2$, tal que $T(L_i) = M_i$, $\forall i, i = 1, 2, 3$.

Afirmção 4: A intersecção de n hiperplanos em P^n é não vazia.

Afirmção 5: Para qualquer conjunto finito de pontos em P^2 , existe uma reta não passando por qualquer um deles.

Observação: Uma reta no plano projetivo é formada pelos zeros de uma forma de grau 1.

3. Variedades Projetivas e Afins

Podemos, como já dissemos anteriormente, considerar A^n como subconjuntos de P^n , por meio de aplicações $\phi_i:A^n \longrightarrow U_i \subset P^n$ (estaremos particularmente interessados quando $i = n+1$). Vejamos as relações entre conjuntos algébricos em A^n e aqueles em P^n .

Se V é um conjunto algébrico em A^n , $I = I(V) \subset K[x_1, \dots, x_n]$, denotamos por I^* , o ideal em

$K[x_1, \dots, x_{n+1}]$ gerado por $\{F^*/F \in I\}$ (Veja capítulo 1, parágrafo 7, para notações). I^* é um ideal homogêneo, pois é gerado por um número finito de formas. Definimos então V^* como sendo $V(I^*) \subset P^n$.

De outra maneira, se V for conjunto algébrico em P^n , $I = I(V) \subset K[x_1, \dots, x_{n+1}]$, denotaremos I_* o ideal em $K[x_1, \dots, x_n]$, gerado pelo conjunto $\{F_*/F \in I\}$ e definimos V_* como sendo $V(I_*) \subset A^n$.

- Proposição 3.5. (1) Se $V \subset A^n$, $\phi_{n+1}(V) = V^* \cap U_{n+1}$ e $(V^*)_* = V$.
 (2) Se $V \subset W \subset A^n$, então $V^* \subset W^* \subset P^n$. Se $U \subset W \subset P^n$, então $V_* \subset W_* \subset A^n$.
 (3) Se V é irredutível em A^n , então V^* é irredutível em P^n .
 (4) Se $V = \bigcup_i V_i$ é a decomposição irredutível de V em A^n , então $V^* = \bigcup_i V_i^*$ é a decomposição irredutível de V^* em P^n .
 (5) Se $V \subset A^n$, então V^* é o menor conjunto algébrico em P^n , que contém $V, (\phi_{n+1}(V))$.
 (6) Se $V \subset A^n$, então nenhum componente de V^* estará em $+$ ou conterá $H_\infty = P^n - U_{n+1}$.
 (7) Se $V \subset P^n$, nenhuma componente de V está em H_∞ ou contém H_∞ , então $V_* \subset A^n$ e $(V_*)^* = V$.

Se V é um conjunto algébrico em A^n , $V^* \subset P^n$ é chamado o fecho projetivo de V . Se $V = V(F)$ é uma hipersuperfície afim, então $V^* = V(F^*)$, desde que se $I = (F)$ é o ideal de uma hipersuperfície, então $I^* = (F^*)$.

Se V é uma variedade em P^n e $U \supset H_\infty$, então $V = P^n$ ou $V = H_\infty$. Além disso, se $V = P^n$, $V_* = A^n$ e se $V = H_\infty$, $V_* = \emptyset$.

Dessa forma, dizemos que, exceto para variedades projetivas que

encontram-se em H_∞ , existe uma correspondência, um a um, entre variedades afins e projetivas.

Dada uma variedade V e seu fecho projetivo $V^* \subset \mathbb{P}^n$, se $f \in \Gamma_h(V^*)$ é uma forma de grau d , nós podemos definir $f_* \in \Gamma_h(V)$, como segue: $f \in \Gamma_h(V^*) \Rightarrow f = F + I(V^*)$, fazemos então $f_* = F_* + I(V)$ (Realçando o fato de que $F \in I^* \Leftrightarrow F_* \in I$, mostramos que tal associação independe da escolha de $F \in K[x_1, \dots, x_{n+1}]$. De fato, se $F + I(V^*) = G + I(V^*) \Rightarrow \Rightarrow F + I(V)^* = G + I(V)^* \Rightarrow (F-G) \in I(V)^* \Rightarrow (F-G)_* \in I(V) \Rightarrow (F_* - G_*) \in I(V) \Rightarrow F_* + I(V) = G_* + I(V)$). Podemos a partir daí, definir um isomorfismo $\alpha: K(V^*) \rightarrow K(V)$, tal que $\alpha(f/g) = f_*/g_*$, onde f e g são formas de mesmo grau sobre V^* . Se $P \in V$, nós podemos considerar $P \in V^*$ (por meio de ϕ_{n+1}) e então α induz isomorfismo $\mathcal{O}_P(V^*) \cong \mathcal{O}_P(V)$. Usamos α para identificarmos $K(V)$ com $K(V^*)$ e $\mathcal{O}_P(V)$ com $\mathcal{O}_P(V^*)$. Qualquer variedade projetiva $V \subset \mathbb{P}^n$ é coberta por $n+1$ conjuntos $V \cap U_i$. Se nós formarmos V_* com respeito a U_i (ou U_{n+1}), os pontos sobre $V \cap U_i$ correspondem a pontos sobre V_* , e os anéis locais são isomorfos. Assim, questões acerca de V , próximas a um ponto P , podem ser reduzidas a questões acerca de variedade afim V_* (Pelo menos em questões que podem ser respondidas olhando-se para $\mathcal{O}_P(V)$).

4. Curvas Planas Projetivas

Uma curva plana projetiva é uma hipersuperfície em $\mathbb{P}^2$ e não fazemos restrições ao fato da forma que tal hipersuperfície ter componentes múltiplas. Dizemos que duas formas $F, G \in K[x, y, z]$ são equivalentes, se existe um $\lambda \in K$, $\lambda \neq 0$, tal que $G = \lambda.F$. Uma curva projetiva plana é uma classe

de equivalência de formas. O grau de uma curva é o grau de uma forma que a define. Curvas de graus 1, 2, 3 e 4 são chamadas de retas, cônicas, cúbicas e quárticas, respectivamente.

Se F for uma forma irredutível, escreveremos $O_P(F)$, $\Gamma_h(F)$, $K(F)$, $K_h(F)$ no lugar de $O_P(V(F))$; $\Gamma_h(V(F))$; $K(V(F))$; $K_h(V(F))$. Notemos que, se $P = (x, y, 1)$, então $O_P(F)$ é canonicamente isomorfo a $O_{(x,y)}(F_*)$, onde $F_* = F(x, y, 1)$ é a curva afim correspondente. Assim, quando formos tratar de assunto que dizem respeito ao anel local $O_P(F)$, podemos pensar em $O_{(x,y)}(F_*)$ e no caso afim correspondente.

A proposição 2.2 do capítulo 2 nos diz que a multiplicidade de um ponto sobre uma curva afim, depende somente do anel local da curva no ponto. Se F é uma curva plana projetiva, $P \in U_i$ ($i = 1, 2$ ou 3), podemos desomogenizar F com respeito a x_i e definir a multiplicidade de F em $P = (x, y, 1)$, $m_P(F)$ como sendo $m_{P'}(F_*)$, onde $P' = (x, y, 1) \sim (x, y)$. A multiplicidade de uma curva projetiva plana será então invariante por troca projetiva de coordenada e independente da escolha de U_i , uma vez que dependerá somente de $O_P(F)$ (que é isomorfo a $O_{P'}(F_*)$).

Usaremos a seguinte notação: se tivermos um conjunto finito de pontos $P_1, \dots, P_n \in P^2$, nós podemos achar uma reta L que não passa por qualquer dos pontos (Afirmação 4, cap. 3, parag. 2). Se F for uma curva de grau d , denotaremos $F_* = F/L^d \in K(P^2)$. F_* depende de L , porém se escolhermos uma outra reta L' , então $F/L'^d = (L/L')^d F_*$, com L/L' unidade em $O_{P_i}(P^2)$; $i = 1, \dots, n$.

Notemos que é possível achar uma troca projetiva de coordenadas, tal que L venha a ser a reta z no infinito e pela identificação natural entre $K(A^2)$ e $K(P^2)$ (dada no

parágrafo 3 deste capítulo), tal que $F_* = F/z^d$ é levado em $F_* = F(x,y,1)$, este como definido no capítulo 1, parágrafo 7.

Se um ponto P é simples sobre uma curva projetiva plana irreduzível F , ($m_P(F) = 1$), então $O_P(F)$ é DVR (Notemos que $m_P(F) = m_P(F_*) = 1$, logo pela proposição 2.1., $O_P(F_*)$ é DVR, porém $O_P(F)$ é isomorfo a $O_P(F_*)$), e nós denotaremos por ord_P^F a correspondente função ordem de $K(F)$.

Se G for uma forma em $K[x,y,z]$ e $G_* = G/L^d \in O_P(P^2)$, definimos $\text{ord}_P^F(G) = \text{ord}_P^F(\bar{G}_*)$, onde $\bar{G}_*$ é o resíduo de G_* em $O_P(F)$.

Se F e G são curvas planas projetivas, $P \in P^2$, nós definimos: $I(P, F \cap G) = \dim_K |O_P(P^2) / (F_*, G_*)|$, esta definição independe da maneira como F_* e G_* foram formados, uma vez que (F_*, G_*) será sempre o mesmo ideal em $O_P(P^2)$. O número de intersecção para curvas planas projetivas, como acabamos de definir, satisfaz, com pequenas alterações, as propriedades de (1) a (8), dadas no Capítulo II, parágrafo 3, como veremos a seguir:

A primeira observação importante a se fazer é que se T for troca projetiva de coordenadas, ela induz um isomorfismo entre $O_P(P^2)/(F_*, G_*)$ e $O_Q(P^2)/((F_0T)_*, (G_0T)_*)$, $T(Q) = P \left[\begin{pmatrix} \bar{H} \\ \bar{K} \end{pmatrix} \in \frac{O_P(P^2)}{(F_*, G_*)} \longrightarrow \begin{pmatrix} \bar{H}_0T \\ \bar{K}_0T \end{pmatrix} \in \frac{O_Q(P^2)}{((F_0T)_*, (G_0T)_*)} \right]$, assim temos a propriedade (3) $I(P, F \cap G) = I(Q, F^T \cap G^T)$.

Logo, podemos pensar P sempre em U_3 , e $F_* = F/z^d$ pode ser identificado com $F_* = F(x,y,1)$, uma vez que $O_P(P^2)/(F_*, G_*)$ é isomorfo a $O_{P'}(A^2)/(F(x,y,1), G(x,y,1))$, assim $I(P, F \cap G) = I(P', F_* \cap G_*) = \dim_K |O_{P'}(A^2)/(F_*, G_*)|$.

Já para obtermos a propriedade (1): $I(P, F \cap G) \in \mathbb{Z}_+$,

para quaisquer curvas planas projetivas F, G e qualquer $P \in P^2$, tais que F e G interceptem-se propriamente em P e $I(P, F \cap G) = \infty$, se F e G não se interceptam propriamente em P. Devemos observar o seguinte:

Se F_* e G_* tiverem fator comum passando por $P' = (x, y)$, então F e G terão fator comum passando por $P = (x, y, 1)$. De

$$\text{fato, se } \begin{cases} F_* = \alpha H_1 \\ G_* = \alpha H_2 \end{cases}, \quad (x, y) = 0 \Rightarrow \begin{cases} (F_*)^* = \alpha^* H_1^* \\ (G_*)^* = \alpha^* H_2^* \end{cases} \quad e$$

$$\alpha^*(x, y, 1) = (\alpha^*)_*(x, y) = \alpha(x, y) = 0 \Rightarrow \begin{cases} F = z^{\Gamma_1} (F_*)^* = z^{\Gamma_1} \alpha^* H_1^* \\ G = z^{\Gamma_2} (G_*)^* = z^{\Gamma_2} \alpha^* H_2^* \end{cases},$$

$\alpha^*(x, y, 1) = 0$. Assim se F e G interceptam-se propriamente em P, F_* e G_* também se interceptarão propriamente em P' . Se F e G não se interceptam propriamente em P, então F_* e G_* também não.

$$\text{De fato, se } \begin{cases} F = \alpha H_1 \\ G = \alpha H_2 \end{cases}, \quad \alpha(P) = 0 \Rightarrow \begin{cases} F_* = \alpha_*(H_1)^* \\ G_* = \alpha_*(H_2)^* \end{cases} \quad e \quad \alpha_*(x, y) = \alpha(x, y, 1) = 0.$$

A propriedade (4) é trivial, pois $(F_*, G_*) = (G_*, F_*)$, logo $I(P, F \cap G) = I(P, G \cap F)$.

Para a propriedade (2): $I(P, F \cap G) = 0$, se e somente se, $P \notin F \cap G$ e $I(P, F \cap G)$ depende somente das componentes de F e G que passam por P. Notamos que se $P = (x, y, 1)$ é tal que $F(P) \neq 0$ ou $G(P) \neq 0 \Rightarrow F(x, y, 1) = F_*(x, y) \neq 0$ ou $G(x, y, 1) = G_*(x, y) \neq 0 \Rightarrow (x, y) \notin F_* \cap G_* \Rightarrow I(P, F \cap G) = I(P', F_* \cap G_*) = 0$, já se $I(P, F \cap G) = 0 \Rightarrow I(P', F_* \cap G_*) = 0 \Rightarrow (x, y) \notin F_* \cap G_* \Rightarrow F(x, y, 1) \neq 0$ ou $G(x, y, 1) \neq 0 \Rightarrow P \notin F \cap G$.

$$\text{A propriedade (6): } I(P, \Pi F_i^{e_i} \cap \Pi G_j^{s_j}) = \sum_{i,j} e_i s_j I(P, F_i \cap G_j)$$

é consequência de que $I(P, F \cap G) = (P', F_* \cap G_*) = I(P', (\Pi F_i^{e_i})_* \cap (\Pi G_j^{s_j})_*) = I(P', \Pi (F_i^*)^{e_i} \cap \Pi (G_j^*)^{s_j})$ (caso afim)

$$= \sum_{i,j} e_i s_j I(P', F_i^* \cap G_j^*) = \sum_{i,j} e_i s_j I(P, F_i \cap G_j).$$

Se F e G são curvas projetivas planas e A é uma forma com grau $\deg A = \deg G - \deg F$, é fácil ver que $(F_*, G_*) = (F_*, (G+AF)_*)$. Assim, $\dim_k |O_P(P^2)/(F_*, G_*)| = \dim_k |O_P(P^2)/(F_*, (G+AF)_*)|$ e portanto a propriedade (7): $\underline{I(P, F \cap G) = I(P, F \cap (G+AF))}$.

Se $P = P_1 = (0, 1, 0)$ e F é uma curva de grau n , $F = \sum_{i=0}^n F_i(x, y)y^{n-i}$, F_i forma de grau i , então $m_P(F) = m_{P'}(F_*) = m_{(0,0)}(\sum_{i=0}^n F_i(x, a)) = \text{menor } i, \text{ tal que } F_i \neq 0$, além disso, os fatores desse F_i , que são aqueles que determinam as retas tangentes a F_* em $(0,0)$, determinarão após homogenização, as retas tangentes a F em P . Dessa forma, dizemos que os fatores desse F_i determinam as tangentes a F em P e além disso: $I(P, F \cap G) = I(P', F_* \cap G_*) \geq m_{P'}(F_*) \cdot m_{P'}(G_*) = m_P(F) \cdot m_P(G)$. A igualdade, no caso afim, ocorre se e somente se F_* e G_* não têm tangentes comuns em P' ; logo, a igualdade, no caso projetivo, também ocorrerá, se e somente se F e G não tiverem tangentes comuns em P , ou seja, vale a propriedade (5).

Propriedade (8): Se P é um ponto simples sobre F , então $I(P, F \cap G) = \text{ord}_P^F(G)$. De fato, como $m_P(F) = m_{P'}(F_*) = 1$, segue que $O_P(F)$, que é isomorfo a $O_{P'}(F_*)$, é DVR. Se $\bar{G}_*$ denotar a imagem de G em $O_P(F)$, teremos que $\text{ord}_P^F(G) \stackrel{(\text{def.})}{=} \text{ord}_P^F(\bar{G}_*)$ (pelo isomorfismo) $\text{ord}_{P'}^{F_*}(\overline{G(x, y, 1)})$ (prop. (8) afim) $= I(P', F_* \cap G_*) = I(P, F \cap G)$, onde a última igualdade é pelo isomorfismo entre $O_P(P^2)/(F_*, G_*)$ e $O_{P'}(A^2)/(F(x, y, 1), G(x, y, 1))$.

Fazendo-se uso da propriedade (5) e do fato de que uma reta no espaço projetivo é uma forma de grau 1, podemos provar que uma reta L é tangente a uma curva F em P , se e somente se, $I(P, F \cap L) > m_P(F)$.

P será chamado de ponto múltiplo ordinário, se F tiver $m_P(F)$ tangentes distintas em P .

Se T é uma troca projetiva de coordenadas, já vimos que T induz isomorfismos entre $\Gamma_h(V)$ e $\Gamma_h(V^T)$; $K(V)$ e $K(V^T)$; $\mathcal{O}_P(V)$ e $\mathcal{O}_Q(V^T)$. Assim, tudo o que dissermos para uma curva, valerá para curvas projetivamente equivalentes, isto é, para curvas F e G , para as quais existe troca projetiva de coordenadas T , tal que $F = G^T = G_0 T$.

Um ponto será ponto múltiplo para uma curva F , se e somente se, $F(P) = F_x(P) = F_y(P) = F_z(P) = 0$. O fato de que duas curvas projetivas planas, sem componentes comuns, interceptam-se em um número finito de pontos, é provado em [4] e será usado posteriormente.

5. Sistemas Lineares de Curvas

Levando-se em conta a seguinte ordenação de monômios de grau d em $K[x,y]$: $x^d y^0, x^{d-1} y^1, x^{d-2} y^2, \dots, x y^{d-1}, x^0 y^d$ é fácil ver que existem $d+1$ tais monômios, se considerarmos que para cada monômio de grau $i \leq d$ em $K[x,y]$ existe um monômio de grau d em $K[x,y,z]$ (basta multiplicar estes monômios de $K[x,y]$ por z^{d-i}), não é difícil concluir que existem $N = 1/2(d+1)(d+2)$ monômios de grau d em $K[x,y,z]$. Se impusermos uma ordenação fixa em tais monômios, $M_1, \dots, M_N$, poderemos, dada uma curva projetiva plana F de grau d , identificá-la com a N -upla $(a_1, \dots, a_N) \in A^N(K)$, onde os a_i 's são tais que $F = \sum_{i=1}^N a_i M_i$.

Obviamente $(a_1, \dots, a_N)$ e $(\lambda a_1, \dots, \lambda a_N)$ determinarão a mesma curva plana projetiva, o que nos leva a fazer uma correspondência biunívoca entre curvas de grau d e pontos de $P^{N-1} = P^{1/2d(d+3)}$. Dizemos, por exemplo, que a cônica $ax^2 + bxy + cxz + dy^2 + ey^2 + fz^2$ corresponde a $(a,b,c,d,e,f) \in P^5$, e que as cônicas formam um P^5 .

Se impusermos condições para formarmos um subconjunto de curvas de grau d , as curvas que satisfazem tais condições, formarão um subconjunto de $P^{1/2d(d+3)}$. Se tal subconjunto for do tipo $V(H_2, \dots, H_r) \subset P^{1/2d(d+3)}$, com H_i forma de grau 1, $\forall i, i = 1, \dots, r$, ele será chamado de Sistema Linear de Curvas.

Observe o seguinte: Se $V = V(H_1, \dots, H_r) \subset P^n(K)$ com H_i 's formas de grau 1 em $K[x_1, \dots, x_{n+1}]$, então V é chamado de subvariedade linear. A tais conjuntos estão associados números, a que chamamos dimensão de V . O número que associamos a uma subvariedade linear V é obtido da seguinte forma: encontra-se uma troca projetiva de coordenadas T , tal que $V^T = T^{-1}(V) = V(x_{m+2}, \dots, x_{n+1})$, o número m é a chamada dimensão de V (obviamente é passível de prova que tal número é invariante para V).

Proposição 3.6. (1) Se $P \in P^2$ é um ponto fixo, então o conjunto de curvas de grau d que contém P , forma um hiperplano em $P^{1/2d(d+3)}$.

(2) Se $T: P^2 \rightarrow P^2$ é uma troca projetiva de coordenadas, então a aplicação $F \mapsto F^T$ do conjunto das curvas de grau d , nele mesmo é uma troca projetiva de coordenadas sobre $P^{1/2d(d+3)}$.

Assim para qualquer conjunto de pontos de P^2 , as curvas de grau d , que os contém, formam uma subvariedade linear de $P^{1/2d(d+3)}$.

Desde que pela afirmação 4 (capítulo 3, parágrafo 2) a intersecção de n hiperplanos em P^n é não vazia. Segue que existe uma curva de grau d passando por quaisquer $1/2d(d+3)$

pontos.

Suponha agora, que fixemos um ponto $P \in P^2$ e um inteiro $\Gamma < d+1$. Afirmamos que as curvas F de grau d , tal que $m_P(F) \geq \Gamma$ formam uma subvariedade linear de $P^{1/2d(d+3)}$, com dimensão $1/2d(d+3) - \Gamma(\Gamma+1)/2$. De fato, pela proposição 3.6, podemos assumir $P = (0,0,1)$. Escrevemos então $F = \sum_{i=0}^d F_i(x,y)z^{d-i}$, onde F_i é forma de grau i . Como $m_P(F) = m_{(0,0)}(F_*) = m_{(0,0)}(\sum_{i=0}^d F_i(x,y))$, teremos que $m_P(F) \geq \Gamma$, se e somente se $F_0 = F_1 = \dots = F_{\Gamma-1} = 0$, ou seja, os coeficientes dos monômios $x^\ell y^j z^k$, para os quais $\ell + j \leq \Gamma - 1$ são zero e existem $\Gamma(\Gamma+1)/2 = 1 + 2 + \dots + \Gamma$, tais monômios, logo igual número de coeficientes. Assim, a dimensão da subvariedade é $1/2d(d+3) - \Gamma(\Gamma+1)/2$.

Se buscarmos um grau maior de abstração, poderemos então fixar $P_1, \dots, P_n$ pontos de P^2 e $\Gamma_1, \dots, \Gamma_n$ inteiros não negativos e denotar por $V(d; \Gamma_1 P_1, \dots, \Gamma_n P_n)$ o conjunto das curvas de grau d , tal que $m_{P_i}(F) \geq \Gamma_i$, $i = 1, \dots, n$.

Vejamos agora, uma proposição que será útil no estudo de pontos múltiplos, a ser desenvolvido posteriormente.

Proposição 3.7. (1) $V(d; \Gamma_1 P_1, \dots, \Gamma_n P_n)$ é uma subvariedade linear de $P^{1/2d(d+3)}$ de dimensão $\geq 1/2d(d+3) - \sum \Gamma_i(\Gamma_i+1)/2$.

(2) Se $d \geq (\sum \Gamma_i) - 1$, então $\dim V(d; \Gamma_1 P_1, \dots, \Gamma_n P_n) = 1/2d(d+3) - \sum (\Gamma_i(\Gamma_i+1))/2$.

Demonstração: (1) O fato de $V(d; \Gamma_1 P_1, \dots, \Gamma_n P_n)$ ser subvariedade linear é óbvio, a partir de que $V(d; \Gamma_1 P_1, \dots, \Gamma_n P_n) = \bigcap_{i=1}^n V(d; \Gamma_i P_i)$ e como a dimensão de cada $V(d; \Gamma_i P_i) = 1/2d(d+3) - \Gamma_i(\Gamma_i+1)/2$, $i = 1, \dots, n$, segue que a dimensão de $V(d; \Gamma_1 P_1, \dots, \Gamma_n P_n) \geq 1/2d(d+3) - \sum_{i=1}^n (\Gamma_i(\Gamma_i+1))/2$.

(2) Prova-se por indução sobre $m = (\sum \Gamma_i) - 1$.

Para $m \leq 1$ o resultado é óbvio. Assim, supomos $m > 1$ ($\Rightarrow d > 1$), podemos ter dois casos:

i) $\Gamma_i = 1, \forall i, i = 1, \dots, n$, denotando-se $V_i = V(d; P_1, \dots, P_i)$, por indução é suficiente mostrar que $V_n \neq V_{n-1}$, pois assim $\dim V_n \leq \dim V_{n-1} - 1$ e usando-se a parte (1) desta proposição, mostra-se o desejado. Para mostrar que $V_n \neq V_{n-1}$ escolhem-se retas L_i passando por P_i , mas não por $P_j, j \neq i$, e uma reta L_0 não passando por qualquer dos P_i 's, assim $F = L_1, \dots, L_{n-1} L_0^{d-n+1} \in V_{n-1}$, porém $F \notin V_n$.

ii) Algum $\Gamma_i > 1$, digamos $\Gamma = \Gamma_1 > 1$, pela proposição 3.6 podemos supor $P = P_1 = (0, 0, 1)$. Seja $V_0 = V(d; (\Gamma-1)P, \Gamma_2 P_2, \dots, \Gamma_n P_n)$ para $F \in V_0$. Seja $F_* = \sum_{i=0}^{\Gamma-1} a_i x^i y^{\Gamma-1-i} + \text{higher terms}$, denotaremos $V_i = \{F \in V_0 / a_j = 0, \text{ se } j < i\}$, claramente $V_0 \supset V_1 \supset \dots \supset V_r = V(d; \Gamma P, \Gamma_2 P_2, \dots, \Gamma_n P_n)$ e é suficiente mostrar que $V_i \neq V_{i+1}, i = 0, \dots, \Gamma-1$, pois daí a $\dim V_\Gamma \leq \dim V_0 - \Gamma$ e pela hipótese de indução mais a parte (1) desta proposição obtém-se o desejado. Para mostrar que $V_i \neq V_{i+1}, i = 0, \dots, \Gamma-1$, fazemos a seguinte construção: $\omega_0 = V((d-1); (\Gamma-2)P, \Gamma_2 P_2, \dots, \Gamma_n P_n)$, para $F \in \omega_0$. Seja $F_* = \sum_{i=0}^{\Gamma-2} a_i x^i y^{\Gamma-2-i} + \text{higher terms}$, denotando $\omega_i = \{F \in \omega_0 / a_j = 0, \text{ se } j < i\}$. Temos pela indução que $\omega_0 \supset \omega_1 \supset \dots \supset \omega_{\Gamma-1} = V(d-1; \Gamma-1 P, \Gamma_2 P_2, \dots, \Gamma_n P_n)$ e escolhendo-se $F_i \in \omega_i, F_i \notin \omega_{i+1}, i = 0, \dots, \Gamma-2$, temos que $yF_i \in V_i$ e $yF_i \notin V_{i+1}$ e $xF_{\Gamma-2} \in V_{\Gamma-1}, xF_{\Gamma-2} \notin V_r$. Portanto $V_i \neq V_{i+1}, i = 0, \dots, \Gamma-1$ e a prova está completa.

CAPITULO IV - TEOREMA DE BEZOUT E APLICAÇÕES

1. Teorema de Bezout

Chegamos agora à parte que queríamos dar ênfase, a saber, o Teorema de Bezout. O que faremos a seguir, visará, após demonstração minuciosa, explorar o resultado do Teorema de Bezout, aplicando-o ao estudo de pontos múltiplos, para o que, deveremos utilizar também o estudo de Sistemas Lineares de Curvas, já feito anteriormente. Mesmo quando partirmos para o estudo do Teorema Fundamental de Max Noether, continuaremos a utilizar resultados do Teorema de Bezout para podermos falar, por exemplo, do grau de um ciclo-intersecção ou para descrever peculiaridades importantes das condições de Max Noether em um ponto; até mesmo resultados obtidos em passos da demonstração do Teorema de Bezout serão utilizados posteriormente.

Levando-se em conta o que já dissemos sobre o fato da intersecção de duas curvas planas projetivas, sem componente comum, ser um conjunto finito de pontos, consideraremos o problema do cálculo do número de elementos desse conjunto finito, contando de maneira apropriada, isto é, levando-se em consideração o número de intersecção das duas curvas nos pontos. O Teorema de Bezout nos dirá exatamente, o número de pontos comuns entre as curvas. A garantia de que a intersecção é não vazia, é também consequência["] do Teorema de Bezout.

Teorema de Bezout: Sejam F e G curvas planas projetivas de graus m e n , respectivamente. Se F e G não têm componentes comuns, então

$$\sum_{P \in P^2} I(P, F \cap G) = m.n.$$

Demonstração: Lembrando que $F \cap G$ é finito, e usando as afirmações 5 e 3 (parágrafo 2, capítulo III), podemos assumir, por uma troca projetiva de coordenadas, se necessário que $V(F, G, z) = \emptyset$. Usando-se a definição de $I(P, F \cap G)$, o isomorfismo $O_P(P^2) / (F_*, G_*) \cong O_P(A^2) / (F_*, G_*)$ e a proposição 1.6 (Capítulo I, parágrafo 8), temos que:

$$\begin{aligned} \sum_P I(P, F \cap G) &= \sum_P I(P, F_* \cap G_*) = \sum_P (\dim_K |O_P(P^2) / (F_*, G_*)|) = \\ &= \sum_P (\dim_K |O_P(A^2) / (F_*, G_*)|) = \dim_K |K[x, y] / (F_*, G_*)|. \end{aligned}$$

Para simplificarmos a notação denotaremos:

$\Gamma_* = K[x, y] / (F_*, G_*)$; $\Gamma = K[x, y, z] / (F, G)$; $R = K[x, y, z]$ e escrevemos Γ_d (respectivamente R_d) para o espaço vetorial das formas de grau d em Γ (respectivamente R). Se mostrarmos que: $\dim_K \Gamma_d = m.n$ para d suficientemente grande e que $\dim_K(\Gamma_*) = \dim_K(\Gamma_d)$, o teorema estará provado.

i) Mostraremos que $\dim \Gamma_d = m.n$ para todo $d \geq m + n$: Sejam as seguintes aplicações $\Pi: R \longrightarrow \Gamma$, tal que $\Pi(H) = H + (F, G)$, $\phi: R \times R \longrightarrow R$, tal que $\phi(A, B) = AF + BG$, $\Psi: R \longrightarrow R \times R$, tal que $\Psi(C) = (GC, -FC)$. Se usarmos o fato de que F e G não têm fatores comuns, não é difícil checar que a sequência:

$$0 \longrightarrow R \xrightarrow{\Psi} R \times R \xrightarrow{\phi} R \xrightarrow{\Pi} \Gamma \longrightarrow 0$$

é exata. (Na verdade, a única passagem mais complicada é mostrar que $\text{Ker } \phi \subset \text{Im } \Psi$, isto é, que para $\phi(A, B) = AF + BG = 0$ existe $C \in R$, tal que $\Psi(C) = (GC, -FC) = (A, B)$, ou seja,

devemos resolver $\begin{cases} GC = A \\ -FC = B \end{cases}$ com $AF + BG = 0$ e F, G sem fatores comuns. Agora $AF + BG = 0 \iff BG = -AF \implies F/B \text{ e } G/-A$,

$$\text{isto é } \begin{cases} B = F\alpha \\ A = -\beta.G \end{cases} \implies \begin{cases} -FC = B = F\alpha \\ GC = A = -\beta G \end{cases} \implies \alpha = \beta = -C, \text{ logo,}$$

$$\Psi(-\alpha) = (G(-\alpha), -F(-\alpha)) = (-\beta G, F\alpha) = (A, B).$$

Se restringirmos tais aplicações para formas de vários graus, obteremos a seguinte sequência exata:

$$0 \longrightarrow R_{d-m-n} \xrightarrow{\Psi} R_{d-m} \times R_{d-n} \xrightarrow{\phi} R_d \xrightarrow{\Pi} \Gamma_d \longrightarrow 0$$

(notemos que $\Psi(R_{d-m-n}) \subset R_{d-m} \times R_{d-n}$; $\phi(R_{d-m} \times R_{d-n}) \subset R_d$ e $\Pi(R_d) = \Gamma_d$, além do mais, as contas para mostrar que a sequência é exata, é idêntica às feitas para a outra sequência acima).

Em $K[x,y]$ o número de monômios de grau d é $d+1$, e para cada monômio de grau menor ou igual a d em $K[x,y]$ existe um monômio de grau d em $K[x,y,z]$, logo $\dim_K(R_d) = (d+1)(d+2)/2$. Além disso, se tivermos uma sequência exata de espaços vetoriais de dimensão finita: $0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_3 \longrightarrow V_4 \longrightarrow 0$, então $\dim V_4 = \dim V_1 - \dim V_2 + \dim V_3$, desde que $\dim_K(R_{d-m} \times R_{d-n}) = \dim_K(R_{d-m}) + \dim_K(R_{d-n})$. Teremos que $\dim \Gamma_d = m.n$, para $d \geq m+n$. Assim nosso primeiro passo da demonstração foi completado.

ii) Mostraremos que a aplicação $\alpha: \Gamma \longrightarrow \Gamma/\alpha(H+(F,G)) = zH + (F,G)$ é injetiva: (desde que, claramente, d é um homomorfismo, mostraremos que seu núcleo é (F,G)) devemos mostrar que se $zH = AF + BG$, então $H = A'F + B'G$, para algum A', B' . Para qualquer $J \in K[x,y,z]$, denotaremos $J(x,y,0)$ por J_0 . Desde que F, G e z não têm zeros comuns, teremos que F_0 e G_0 são formas relativamente primas em $K[x,y]$ (do contrário, F e G teriam infinitos zeros em comum, logo não poderiam deixar de ter fator comum).

Se $zH = AF + BG$, então $A_0F_0 = -B_0G_0$, logo F_0/B_0 , ou

seja $B_0 = F_0 \cdot C$ e $-G_0/A_0$, ou seja, $A_0 = -G_0 \cdot C$, onde $C \in K[x,y]$.

Consideremos agora, $A_1 = A + CG$ e $B_1 = B - CF$, assim,
 $(A_1)_0 = A_0 + C_0 G_0 = A_0 + CG_0 = A_0 - A_0 = 0 = B_0 - B_0 = B_0 - CF_0 =$
 $B_0 - C_0 F_0 = (B_1)_0$, e portanto, $A_1 = zA'_1$ e $B_1 = zB'_1$, logo $zH =$
 $= AF + BG = (A_1 - CG)F + (B_1 + CF)G = A_1 F + B_1 G = zA'_1 F + zB'_1 G \Rightarrow$
 $\Rightarrow z(H - A'_1 F - B'_1 G) = 0 \Rightarrow H = A'_1 F + B'_1 G$, como desejado.

Dessa forma $\alpha: \Gamma \rightarrow \Gamma$ é homomorfismo injetor.

iii) Seja $d \geq m+n$ e escolhamos $A_1, \dots, A_{m,n} \in R_d$,
 cujos resíduos em Γ_d formam uma base para Γ_d (Notemos que em
 (i) mostramos que $\dim_K \Gamma_d = m.n$, para $d \geq m+n$, assim é
 natural escolhermos uma base em Γ_d com $m.n$ elementos que o
 geram, como K espaço vetorial). Se $A_{i*} = A_i(x,y,1) \in K[x,y]$, de-
 notaremos por a_i o resíduo de A_{i*} em Γ_* . Mostraremos então, que
 $a_1, \dots, a_{m,n}$ formam uma base para Γ_* : primeiro observemos que para $d \geq m+n$
 Γ_d e Γ_{d+1} têm a mesma dimensão, $m.n$ e a aplicação α , de (ii), restrita a
 a Γ_d é isomorfismo de Γ_d e Γ_{d+1} , desde que ela é linear e injetiva en-
 tre espaços vetoriais de mesma dimensão. Segue então, que os resíduos de
 $z^\Gamma A_1, \dots, z^\Gamma A_{m,n}$ formam uma base para $\Gamma_{d+\Gamma}$, para todo $\Gamma \geq 0$.

Os a_i geram Γ_* : Se $h = \bar{H} = H + (F_*, G_*) \in \Gamma_*$, $H \in$
 $K[x,y]$, algum z^{NH*} é uma forma de grau $d + \Gamma$. Assim, temos
 que $z^{NH*} \in R_{d+\Gamma} \Rightarrow \overline{z^{NH*}} \in \Gamma_{d+\Gamma} \Rightarrow \overline{z^{NH*}} = \sum_{i=1}^{m.n} \lambda_i (z^\Gamma A_i + (F,G)) \Rightarrow$

$$\Rightarrow z^{NH*} + (F,G) = \sum_{i=1}^{m.n} \lambda_i z^\Gamma A_i + (F,G) = \sum_{i=1}^{m.n} \lambda_i z^\Gamma A_i + (F,G) \Rightarrow$$

$$\Rightarrow z^{NH*} - \sum_{i=1}^{m.n} \lambda_i z^\Gamma A_i \in (F,G) \Rightarrow z^{NH*} = \sum_{i=1}^{m.n} \lambda_i z^\Gamma A_i + BF + CG \quad \text{para}$$

$$\lambda_i \in K, B \text{ e } C \in K[x,y,z]. \quad \text{Dessa forma} \quad H = (z^{NH*})_* =$$

$$= \sum_{i=1}^{m.n} \lambda_i A_{i*} + B_* F_* + C_* G_* \Rightarrow (H - \sum_{i=1}^{m.n} \lambda_i A_{i*}) \in (F_*, G_*) \Rightarrow H + (F_*, G_*) =$$

$$= h = \left(\sum_{i=1}^{m.n} \lambda_i A_{i*} \right) + (F_*, G_*) = \sum_{i=1}^{m.n} \lambda_i (A_{i*} + (F_*, G_*)) = \sum_{i=1}^{m.n} \lambda_i a_i, \quad \text{como}$$

desejávamos.

Os a_i são independentes: pois se $\sum \lambda_i a_i = 0 \implies \sum \lambda_i (A_{i*} + (F_*, G_*)) = (F_*, G_*) \implies \sum \lambda_i A_{i*} \in (F_*, G_*) \implies \sum \lambda_i A_{i*} = BF_* + CG_*$ e pela proposição 1.5 (Capítulo I, parágrafo 7), temos que para certos Γ, s, t ; $z^\Gamma \sum_{i=1}^{m.n} \lambda_i A_i = (z^s B^*)F + (z^t C^*)G \implies \sum_{i=1}^{m.n} \lambda_i \left| z^\Gamma A_i + (F, G) \right| = 0$ em Γ_{r+d} . Como os $z^\Gamma A_i + (F, G)$ formam uma base para $\Gamma_{d+\Gamma}$, temos que cada $\lambda_i = 0$.

Dessa forma, $\dim_K \Gamma_* = \dim_K \Gamma_d = m.n$ e o teorema está provado.

Corolário 1: Se F e G não têm componentes comuns, então

$$\sum_P m_P(F).m_P(G) \leq (\deg F).(\deg G).$$

Demonstração: Pela propriedade (5), para número de intersecção, temos que $I(P, F \cap G) \geq m_P(F).m_P(G) \implies \sum_P I(P, F \cap G) \geq \sum_P m_P(F).m_P(G)$ e pelo teorema de Bezout, temos que $(\deg F).(\deg G) = \sum_P I(P, F \cap G) \geq \sum_P m_P(F).m_P(G)$.

Corolário 2: Se F e G encontram-se em $m.n$ pontos distintos, onde $m = \deg F$, $n = \deg G$, então esses pontos são todos pontos simples sobre F e sobre G .

Demonstração: Lembrando o fato de que $I(P, F \cap G) = 0 \iff P \notin F \cap G$ e como $\sum_P I(P, F \cap G) \stackrel{P \text{ (Bezout)}}{=} m.n$. Temos $m.n$ parcelas com valores inteiros maiores ou iguais a um, cuja soma é exatamente $m.n$. Obviamente $I(P_i, F \cap G) = 1, \forall i, i = 1, \dots, m.n$. Pela propriedade (5), de número de intersecção, temos que $1 = I(P_i, F \cap G) \geq m_{P_i}(F).m_{P_i}(G) \implies m_{P_i}(F) = m_{P_i}(G) = 1$, uma vez que $P_i \in F \cap G, \forall i, i = 1, \dots, m.n$. Portanto, todos são pontos simples sobre F e sobre G .

Corolário 3: Se duas curvas de graus m e n têm mais que $m.n$ pontos em comum, então elas têm uma componente em comum.

Demonstração: Pela definição de número de intersecção, temos que $I(P, F \cap G) \geq 1$, desde que P pertença a $F \cap G$, como existem mais que $m.n$ pontos em $F \cap G$, temos que $\sum_P I(P, F \cap G) > m.n$ e pela contra recíproca do Teorema de Bezout, F e G têm componentes comuns.

2. Aplicação no Estudo de Pontos Múltiplos

Se F for uma curva projetiva plana irredutível de grau n , utilizando, principalmente, o teorema de Bezout e alguns outros resultados que demonstramos abaixo, encontraremos um majorante para o número de elementos do conjunto dos pontos múltiplos de F .

Encontraremos também, um majorante para a soma: $\sum_P (m_P(F) | m_P(F) - 1 |) / 2$, que dependerá apenas do grau da curva F , e a partir daí, poderemos tirar algumas conclusões a respeito da curva em questão, dizendo se é singular ou se tem pontos duplos ou triplos.

Mostraremos também, que o majorante encontrado para a soma acima é o melhor possível, isto é, o resultado não pode ser fortalecido

Como já vimos anteriormente, P é o ponto múltiplo para uma curva projetiva plana F se $F(P) = F_x(P) = F_y(P) = F_z(P) = 0$. Demonstramos abaixo, duas afirmações que usaremos para nossos propósitos.

Afirmação 1: Para qualquer curva plana projetiva F , tal que

$F_x \neq 0$, temos que $m_P(F_x) \geq m_P(F) - 1$.

Demonstração: Observemos inicialmente, que se $P \notin F$ ou P é ponto simples de F , o resultado é trivial ($m_P(F_x) \geq -1$ e $m_P(F_x) \geq 0$, respectivamente). Dessa forma, trabalhamos apenas com P ponto múltiplo de F , isto é, $m_P(F) \geq 2$.

Assim $m_P(F) = m_{P'}(F_*) = m_{P'}(F_2 + \dots + F_\Gamma) =$ menor i , tal que $F_i \neq 0$, $i = 2, \dots, \Gamma$.

Note que as F_i 's são formas em x, y ; x, z ; y, z , conforme P esteja em U_3 , U_2 , U_1 , respectivamente. Temos então, 3 casos:

i) $P \in U_1 \Rightarrow (F_*)^* = x^{\Gamma-2}F_2 + x^{\Gamma-3}F_3 + \dots + F_\Gamma \Rightarrow$
 $\Rightarrow F = x^\ell (F_*)^* = x^{\ell+\Gamma-2}F_2 + x^{\ell+\Gamma-3}F_3 + \dots + x^\ell F_\Gamma \Rightarrow F_x =$
 $= (\ell+\Gamma-2)x^{\ell+\Gamma-3}F_2 + (\ell+\Gamma-3)x^{\ell+\Gamma-4}F_3 + \dots + \ell x^{\ell-1}F_\Gamma \Rightarrow (F_x)_* =$
 $= (\ell+\Gamma-2)F_2 + (\ell+\Gamma-3)F_3 + \dots + \ell F_\Gamma \Rightarrow m_P(F_x) =$ menor i , tal
 que $F_i \neq 0$, logo $m_P(F_x) \geq m_P(F) - 1$.

ii) $P \in U_2 \Rightarrow F = y^{\ell+\Gamma-2}F_2 + y^{\ell+\Gamma-3}F_3 + \dots + y^\ell F_\Gamma \Rightarrow$
 $\Rightarrow F_x = y^{\ell+\Gamma-2}(F_2)_x + y^{\ell+\Gamma-3}(F_3)_x + \dots + y^\ell (F_\Gamma)_x \Rightarrow m_P(F_x) =$
 $= m_{P'}((F_x)_*) = m_{P'}((F_2)_x + (F_3)_x + \dots + (F_\Gamma)_x) = j - 1$, onde
 j é o menor índice para o qual $(F_j)_x \neq 0$ (Note que este existe, do contrário $F_x = 0$), como a derivada de uma forma de grau d é uma forma de grau $d - 1$, temos que $m_P(F_x) \geq m_P(F) - 1$, com a igualdade ocorrendo quando $(F_j)_x \neq 0$, para j igual ao i que determina a $m_P(F)$.

iii) $P \in U_3$, é análogo ao caso (ii)

Portanto, de (i), (ii) e (iii) temos que $m_P(F_x) \geq m_P(F) - 1$.

Afirmção 2: Se F for uma curva plana projetiva não nula, então

F_x, F_y ou F_z é diferente de zero.

De fato, se $\deg F = n$, temos pelo Teorema de Euler que $nF = xF_x + yF_y + zF_z$, logo F_x, F_y ou $F_z \neq 0$, do contrário $F = 0$.

Para encontrarmos um majorante para o número de elementos do conjunto dos pontos múltiplos de uma curva irreduzível F , é conveniente mostrar inicialmente, que tal conjunto é finito. Se F é uma curva irreduzível, dizer que F tem um número finito de pontos múltiplos é equivalente a afirmar que $V(F, F_x, F_y, F_z)$ é finito.

Se denotarmos por $z_x = V(F) \cap V(F_x)$; $z_y = V(F) \cap V(F_y)$ e $z_z = V(F) \cap V(F_z)$, teremos que $V(F, F_x, F_y, F_z) = z_x \cap z_y \cap z_z$. Se mostrarmos que z_x, z_y ou z_z é finito, teremos concluído o que queremos. Pela afirmação 2, acima, temos que F_x, F_y ou $F_z \neq 0$ e como F é irreduzível, segue que F e a derivada que não é nula, não têm componentes comum, e como a intersecção de duas curvas projetivas planas sem componentes comum é um conjunto finito, segue que z_x, z_y ou z_z é finito, donde concluimos que o conjunto dos pontos múltiplos de uma curva projetiva plana irreduzível é finito.

Mostraremos agora, que se F for uma curva plana projetiva irreduzível de grau n , então $\sum m_p(F) |m_p(F) - 1| \leq n(n-1)$.

A primeira coisa a se notar é que a afirmação 1, feita atrás também, vale quando $F_y \neq 0$ ou $F_z \neq 0$. Como F é irreduzível e F_x, F_y ou $F_z \neq 0$, segue que F e a derivada não nula, não têm componentes comuns. Suponha que $F_x \neq 0$, assim pelo corolário 1 do Teorema de Bezout, segue que: $\sum m_p(F).m_p(F_x) \leq \deg(F).\deg(F_x) = n(n-1)$. Se acrescentarmos a esta desigualdade a afirmação 1, dada acima, temos que:

$$\sum m_P(F) \cdot |m_P(F) - 1| \leq \sum m_P(F) \cdot m_P(F_X) \leq n(n-1) \quad (I)$$

Estamos agora, em condições de provar que: o conjunto dos pontos múltiplos de uma curva projetiva plana irreduzível de grau n , tem no máximo $1/2n(n-1)$ pontos múltiplos, de fato, como tal conjunto é finito, suponhamos que sejam seus pontos $P_1, \dots, P_\Gamma$ e a multiplicidade de F nos P_i 's, sejam respectivamente, $n_1, \dots, n_\Gamma$, temos necessariamente que $n_i \geq 2$, $\forall i, i = 1, \dots, \Gamma$ (pois, do contrário $P_i \notin F$ ou P_i é ponto simples de F).

Pela desigualdade (I), obtida acima, temos que: $n_1(n_1-1) + \dots + n_\Gamma(n_\Gamma-1) \leq n(n-1)$, logo $2 \cdot 1 + \dots + 2 \cdot 1 \leq n_1(n_1-1) + \dots + n(n-1) \leq n(n-1) \Rightarrow 2\Gamma \leq n(n-1) \Rightarrow \Gamma \leq n(n-1)/2$, e portanto, temos no máximo $1/2n(n-1)$ pontos múltiplos.

Obtivemos a desigualdade $\sum m_P(F) |m_P(F) - 1| \leq n(n-1)$. Mostraremos, no entanto, que esta desigualdade não é o melhor resultado possível. Vejamos, por exemplo, o problema:

(a) Seja F uma cônica irreduzível, $P = (0,1,0)$ um ponto simples de F e $z = 0$ a reta tangente a F em P . Mostrar que $F = ayz - bx^2 - cxz - dz^2$, com $a, b \neq 0$.

Solução: Uma cônica em $K[x,y,z]$ é da forma $F = \alpha_1 x^2 + \alpha_2 y^2 + \alpha_3 z^2 + \alpha_4 xy + \alpha_5 xz + \alpha_6 yz$. Como P é ponto simples de F , temos que $F(P) = 0$. Logo, $F(0,1,0) = \alpha_1 0 + \alpha_2 1 + \alpha_3 0 + \alpha_4 0 + \alpha_5 0 + \alpha_6 0 = 0 \Rightarrow \alpha_2 = 0$. Logo $F = \alpha_1 x^2 + \alpha_3 z^2 + \alpha_4 xy + \alpha_5 xz + \alpha_6 yz$. Além disso, temos que, sendo $z = 0$, a reta tangente a F em P , $F_x(P)x + F_y(P)y + F_z(P)z = z \Leftrightarrow (2\alpha_1 0 + \alpha_4 1 + \alpha_5 0)x + (\alpha_4 0 + \alpha_6 0)y + (2\alpha_3 0 + \alpha_5 0 + \alpha_6 1)z = z \Leftrightarrow \alpha_4 x + \alpha_6 z = z \Leftrightarrow \alpha_4 = 0$.

Logo, $F = \alpha_1 x^2 + \alpha_3 z^2 + \alpha_5 xz + \alpha_6 yz$. Seja então, $\alpha_1 = -b$; $a = \alpha_6$; $\alpha_5 = -c$ e $\alpha_3 = -d$, então,

$$F = ayz - bx^2 - cxz - dz^2$$

com $b \neq 0$ (pois, do contrário $F = (ay + cx - dz)z$, porém F é irreduzível) e $a \neq 0$ (do contrário $F = -(bx^2 + cxz + dz^2) \Rightarrow F_x(P) = -(2b \cdot 0 + c \cdot 0) = 0$; $F_y(P) = 0$; $F_z(P) = -(c \cdot 0 + 2d \cdot 0) = 0$ e a reta tangente a F em P $F_z(P)x + F_y(P)y + F_z(P)z \neq z$).

(b) Achar uma troca projetiva de coordenadas T_0 , tal que $F^{T_0} = yz - x^2$.

Solução: Desde que a composição de duas trocas projetivas de coordenadas é uma troca projetiva de coordenadas, encontraremos T_0 em dois passos. T_0 será a composta das duas transformações necessárias para obtermos o que desejamos.

(i) Seja $T = (T_1, T_2, T_3)$, tal que $T_1(x, y, z) = x/2$, onde α é tal que $\alpha^2 = b$; $T_2(x, y, z) = y/2$ e $T_3(x, y, z) = z$. Assim, teremos que $(F_0 T)(x, y, z) = aT_2 \cdot T_3 - bT_1^2 - cT_1 \cdot T_3 - dT_3^2 = yz - x^2 - c'xz - dz^2$.

(ii) Seja $T' = (T'_1, T'_2, T'_3)$, onde $T'_1(x, y, z) = x$; $T'_2(x, y, z) = y + c'x + d'z$; $T'_3(x, y, z) = z$, então $(F^T)^{T'} = T'_2 \cdot T'_3 - (T'_1)^2 - c' \cdot T'_1 \cdot T'_3 - d'(T'_3)^2 = yz - x^2$.

Seja então $T_0 = T_0 T'$, assim $F^{T_0} = (F^T)^{T'} = yz - x^2$.

(c) Mostrar que, a menos de equivalência projetiva, existe somente uma cônica irreduzível. Qualquer cônica irreduzível é não singular.

Se F é uma cônica irreduzível, então F é um polinômio homogêneo de grau 2 em $K[x, y, z]$, logo, tem infinitos

zeros. Como o conjunto dos pontos múltiplos é finito, como provamos, segue que o conjunto dos pontos simples de F é infinito. Seja T , uma troca projetiva de coordenadas que leva um dos pontos simples sobre $(0,1,0)$ e sua reta tangente sobre a reta z (ver afirmação 1 e 3, Capítulo III, parágrafo 2), assim teríamos por tal troca projetiva de coordenadas, que $F_0 T$ seria como a da parte (a), logo projetivamente equivalente a $yz - x^2$.

Notemos que a multiplicidade é invariante por troca projetiva de coordenadas e como toda cônica irreduzível é projetivamente equivalente a $yz - x^2$, e esta, por sua vez é tal que $G_x = -2x$, $G_y = z$, $G_z = y$, logo não singular, afirmamos que "toda cônica irreduzível é não singular".

Dessa forma, se fossemos aplicar a desigualdade $\sum m_p(F) |m_p(F) - 1|/2 \leq n(n-1)/2$, para as cônicas irreduzíveis, obteríamos que: $\sum m_p(F) |m_p(F) - 1|/2 \leq n(n-1)/2 = 2(2-1)/2 = 1$, o que abriria a possibilidade de termos $\sum m_p(F) |m_p(F) - 1| = 2$ e isto nos possibilitaria pensar em um $P \in F$, tal que $m_P(F) = 2$; porém como vimos no último problema, isto não ocorre, pois toda cônica irreduzível é não singular. Desta forma, devemos poder aprimorar nosso resultado e realmente podemos:

Proposição 4.1. Se F é uma curva irreduzível de grau n , então $\sum m_p(F) |m_p(F) - 1|/2 \leq (n-1)(n-2)/2$.

Demonstração: Usaremos a notação m_p no lugar de $m_p(F)$. Tínhamos até agora que $\sum m_p(m_p - 1)/2 \leq n(n-1)/2 \implies n(n-1)/2 - \sum m_p(m_p - 1)/2 \geq 0$. Além disso, como $(n-1)(n-1+3)/2 \geq (n-1)n/2$, temos que $\Gamma = (n-1)(n-1+3)/2 - \sum m_p(m_p - 1)/2 \geq n(n-1)/2 - \sum m_p(m_p - 1)/2 \geq 0$.

Escolhemos $Q_1, \dots, Q_r$ pontos simples de F (estes existem, pois o conjunto dos zeros de F é infinito e o conjunto dos pontos múltiplos de F é finito). Se considerarmos a proposição 3.7, do Capítulo 3, com $d = n - 1$, temos $\omega = V((n-1); (m_{P_1} - 1)P_1, \dots, (m_{P_\ell} - 1)P_\ell, 1Q_1, \dots, 1Q_r)$, onde os P_i 's, com $i = 1, \dots, \ell$ são os pontos múltiplos de F . Assim, existe uma curva $G \in \omega$, tal que $m_P(G) \geq m_P(F) - 1$, para todo P e $m_{Q_i}(G) \geq 1$, $\forall i$, $i = 1, \dots, r$.

Aplicando o corolário 1 do Teorema de Bezout a F e G , que não têm componentes comuns, uma vez que F é irredutível, $\deg G = n - 1$ e $\deg F = n$, obtemos que: $\sum m_P(F) \cdot m_P(G) \leq n(n-1)$, (I).

$$\begin{aligned} \text{Porém, } \sum m_P(F) \cdot m_P(G) &= m_{Q_1}(F) \cdot m_{Q_1}(G) + \dots + \\ &+ m_{Q_r}(F) \cdot m_{Q_r}(G) + \sum_{P \neq Q} m_P(F) \cdot m_P(G) \geq r + \sum_{P \neq Q} m_P(F) \cdot m_P(G) \geq r + \\ &+ \sum_{P \neq Q} m_P(F) |m_P(F) - 1| = r + \sum_{P \in P^2} m_P(F) \cdot |m_P(F) - 1|, \quad \text{(II).} \end{aligned}$$

Obtemos então de (I) e (II), que: $n(n-1) \geq r + \sum m_P(F) |m_P(F) - 1|$. Substituindo o valor de r , vem que: $n(n-1) - (n-1)(n+2)/2 + \sum m_P(m_P - 1)/2 \geq \sum m_P(m_P - 1) \iff \iff (2n^2 - 2n) - (n^2 + n - 2)/2 \geq \sum m_P(m_P - 1)/2 \iff (n-1)(n-2)/2 \geq \sum m_P(m_P - 1)/2$, como queríamos demonstrar.

Notemos, que a partir desta desigualdade, o resultado do problema anterior, sobre cônica irredutível, podia ser obtido pela simples substituição de n por 2 na fórmula, assim teríamos que: $\sum m_P(m_P - 1)/2 \leq (2 - 1)(2 - 2)/2 = 0 \implies \sum m_P(m_P - 1) = 0 \implies m_P(F) = 0$ ou $m_P(F) = 1$ (Note que cada parcela da soma $\sum m_P(m_P - 1)/2$ é positiva) e isso nos levaria a concluir que uma cônica irredutível é não singular, poupando grande esforço. Além disso, podemos encontrar um resultado mais significativo para o majorante do conjunto dos pontos múltiplos de uma curva projetiva plana irredutível de grau n , é este

Para pequenos valores de n , a desigualdade nos dá mais resultados interessantes. Eis alguns exemplos:

(i) Uma reta F é não singular, uma vez que $n = 1$ e $\sum m_P(m_P - 1)/2 \leq (1 - 1)(1 - 2)/2 = 0 \Rightarrow \sum m_P(m_P - 1) = 0 \Rightarrow m_P(F) = 0$ ou $m_P(F) = 1$, para todo P .

(ii) Se tivermos uma cúbica irreduzível, então $n = 3$ e $\sum m_P(m_P - 1)/2 \leq (3 - 1)(3 - 2)/2 = 1 \Rightarrow \sum m_P(m_P - 1) \leq 2$. Assim a cúbica pode ter no máximo um ponto duplo, pois se P_0 é um ponto sobre a cúbica, para o qual $m_{P_0}(F) = 2$, então teríamos que $\sum_{P \neq P_0} m_P(m_P - 1) + m_{P_0}(F) \leq 2 \Rightarrow \sum_{P \neq P_0} m_P(m_P - 1) + 2 \leq 2 \Rightarrow \sum_{P \neq P_0} m_P(m_P - 1) = 0 \Rightarrow m_P(F) = 0$ ou $m_P(F) = 1$, ou seja os pontos restantes são simples ou não pertencem a curva.

(iii) Se considerarmos uma quártica F irreduzível, teremos $n = 4$ e $\sum m_P(m_P - 1)/2 \leq (4 - 1)(4 - 2)/2 = 3 \Rightarrow \sum m_P(m_P - 1) \leq 6$, logo a quártica tem no máximo três pontos duplos ou um ponto triplo.

Notemos finalmente, que a curva $H(x, y) = x^n + y^{n-1}z$ tem o ponto $P = (0, 0, 1)$ com multiplicidade $n - 1$, isto é, $m_P(H) = m_{(0,0)}(H_*) = m_{(0,0)}(x^n + y^{n+1}) = n - 1$. Assim sendo, $m_P(H) \cdot (m_P(H) - 1) = (n - 1)(n - 2)$ e como $\sum m_P(m_P - 1)/2 \leq (n - 1)(n - 2)/2$, segue que todos os seus outros pontos são simples e que o resultado da proposição 4.1 não pode ser melhorado, pois não existe $\phi(n) < (n - 1)(n - 2)/2$, tal que $\sum m_P(m_P - 1)/2 \leq \phi(n)$.

Um resultado interessante a se notar é: Se uma curva projetiva plana é não singular, então ela é irreduzível ou equivalentemente, se for redutível, terá pontos múltiplos. De fato, se $F = G \cdot H$, onde G e H são irreduzíveis distintas e de graus > 0 , então $I(P, G \cap H) \stackrel{\text{Bezout}}{=} (\deg G) \cdot (\deg H) > 0$.

Logo, existe pelo menos um $P \in H \cap G$. Como $m_P(F) = m_P(F_*) = m_P(G_* \cdot H_*) = m_P(G_*) + m_P(H_*) \geq 1 + 1 = 2$, segue que P é o ponto múltiplo de F , ou seja, se F é redutível, existe ponto múltiplo para F (Observação: Se $G = H$, então todo ponto de F seria múltiplo).

CAPITULO V - TEOREMA FUNDAMENTAL DE MAX NOETHER E APLICAÇÕES

1. O Teorema Fundamental de Max Noether

O Teorema Fundamental de Max Noether tem várias aplicações interessantes, como é o caso dos Teoremas de Pascal e Pappa. Além disso, possibilita-nos falar sobre adição em uma cúbica e mostrar a estrutura de grupo abeliano, obtida a partir de tal definição. No que segue, os resultados que levaram em conta o grau de um ciclo-intersecção, estarão indiretamente sendo uma aplicação do Teorema de Bezout, uma vez que este número é definido pelo Teorema de Bezout.

Um zero-ciclo sobre P^2 é uma soma formal $\sum_{P \in P^2} n_P P$, onde os n_P 's são inteiros e todos, menos um número finito deles são zero. O grau de um zero-ciclo $\sum n_P P$ é definido como sendo $\sum n_P$. O zero-ciclo é positivo, se cada $n_P \geq 0$.

Diremos que um zero-ciclo $\sum n_P P$ é maior do que o zero-ciclo $\sum m_P P$ e escreveremos $\sum n_P P \succ \sum m_P P$, se $n_P \geq m_P$, para cada P .

Sejam F e G curvas planas projetivas de graus m e n , respectivamente, que não têm componentes comuns. Definimos o ciclo-interseção $F.G$ como sendo $\sum_{P \in P^2} I(P, F \cap G) P$. O Teorema de Bezout nos diz que $F.G$ é um zero-ciclo positivo de grau $m.n$ (uma vez que $I(P, F \cap G) \geq 0$, $\forall F, P, G$ e $\sum I(P, F \cap G) = m.n$).

Muitas propriedades de número de intersecção traduz-se para propriedades de ciclo-intersecção, por exemplo: $F.G = G.F$, uma vez que $F.G = \sum I(P, F \cap G) P \stackrel{*}{=} I(P, G \cap F) = G.F$, onde (*) refere-se a propriedade (4) para número de intersecção; $F.GH = F.G + H$, pois $F.GH = \sum I(P, F \cap GH) P \stackrel{*}{=}$

$$\stackrel{*}{=} \sum |I(P, F \cap G) + I(P, F \cap H)|P = \sum I(P, F \cap G)P + \sum I(P, F \cap H)P =$$

$$= F.G + F.H, \text{ onde } (*) \text{ refere-se a propriedade (6) para número}$$

$$\text{de intersecção; } F.(G + AF) = F.G, \text{ desde que } A \text{ seja uma forma com}$$

$$\text{deg } A = \text{deg } G - \text{deg } F, \text{ de fato: } F.(G + AF) = \sum I(P, F \cap G + AF)P \stackrel{*}{=} \sum I(P, F \cap G)P = F.G, \text{ onde } (*) \text{ refere-se a propriedade (7) para}$$

$$\text{número de intersecção.}$$

O Teorema de Max Noether diz respeito a seguinte situação: Suponha F, G e H curvas, e $H.F \succ G.F$, isto é, H intercepta F em um ciclo maior que G o faz, quando é que existe uma curva B , tal que $B.F = H.F - G.F$? (Notemos que $B.F = H.F - G.F \iff \sum I(P, B \cap F)P = (\sum I(P, H \cap F)P) - (\sum I(P, G \cap F)P) = \sum |I(P, H \cap F) - I(P, G \cap F)|P \implies \sum I(P, B \cap F) = \sum I(P, H \cap F) - \sum I(P, G \cap F)$ e pelo Teorema de Bezout, temos que, $(\text{deg } B)(\text{deg } F) = (\text{deg } H)(\text{deg } F) - (\text{deg } G)(\text{deg } F) \implies (\text{deg } B) = (\text{deg } H) - (\text{deg } G)$).

Para acharmos tal B , é suficiente achar formas A, B tal que $H = AF + BG$, pois então, $H.F = BG.F = G.F + B.F$, isto é, $H.F = \sum I(P, H \cap F)P = \sum I(P, AF + BG \cap F)P = \sum I(P, BG \cap F)P = \sum I(P, B \cap F)P + \sum I(P, G \cap F)P = B.F + G.F \implies B.F = H.F - G.F$, como queríamos inicialmente.

Sejam $P \in P^2$, F, G curvas com componentes não comuns sobre P , H uma outra curva. Dizemos que as condições de Noether são satisfeitas em P (com respeito a F, G e H) se $H_* \in (F_*, G_*) \subset O_P(P^2)$, isto é, existirem $a, b \in O_P(P^2)$, tal que $H_* = aF_* + bG_*$ (para notação, veja Capítulo III, parágrafo 4).

Após estas considerações, vejamos o Teorema de Max Noether:

Teorema Fundamental de Max Noether Sejam F, G e H curvas

planas projetivas. Assuma que F e G não têm componentes comuns, então existe uma equação $H = AF + BG$ (com A, B , formas de graus $(\deg H) - (\deg F)$, $(\deg H) - (\deg G)$, respectivamente) se e somente se, as condições de Noether são satisfeitas em todo $P \in F \cap G$.

Demonstração: Se $H = AF + BG$, então, uma vez que os graus A e B são determinados convenientemente, é claro que $H_* = A_*F_* + B_*G_*$, para qualquer $P \in F \cap G$, ou seja $H_* \in (F_*, G_*) \subset O_P(P^2)$, para qualquer $P \in F \cap G$.

Para provarmos a recíproca, assumiremos, como fizemos no Teorema de Bezout, que $V(F, G, z) = \emptyset$, (isto nos auxiliará no momento de identificarmos $O_{P_i}(P^2)/(F_*, G_*)$ com $O_{P_i}(A^2)/(F_*, G_*)$). As condições de Noether, dizem que o resíduo de H_* em $O_P(P^2)/(F_*, G_*)$ é zero para cada $P \in F \cap G$. Como F e G não têm componentes comum, segue que F_* e G_* não têm componentes comuns em $K[x, y]$ (corolário da proposição 1.5, capítulo I, parágrafo 7). Assim $V(F_*, G_*)$ é finito, e pela proposição 1.6, Capítulo I, parágrafo 8, segue que

$$\sum_{i=1}^{\Gamma} O_{P_i}(P^2)/(F_*, G_*) \cong \sum_{i=1}^{\Gamma} O_{P_i}(A^2)/(F_*, G_*) \cong K[x, y]/(F_*, G_*), \text{ onde}$$

supomos que existem Γ pontos em $F \cap G$, e o último isomorfismo nos garante que H_* é zero em $K[x, y]/(F_*, G_*)$ (imagem de zero é zero, por isomorfismo), logo $H_* = aF_* + bG_*$, com $a, b \in K[x, y]$. Pela proposição 1.5, Capítulo I, parágrafo 7, existem Γ , A , B , tais que $z^\Gamma H = AF + BG$, porém na demonstração do Teorema de Bezout, provamos que a multiplicação por z sobre $K[x, y, z]/(F, G)$ é injetiva, logo $H = A'F + B'G$, para algum $A', B' \in K[x, y, z]$. Se $A' = \sum A'_i$, $B' = \sum B'_i$ com A'_i e B'_i formas de grau i , então $H = A'_s F + B'_t G$, onde $s = (\deg H) - (\deg F)$

e $t = (\deg H) - (\deg G)$.

Certamente, o pleno uso deste Teorema depende de encontrarmos critérios que assegurem que as condições de Noether são válidas em um ponto P . Para isso temos:

Proposição 5.1. Sejam F, G, H curvas planas, $P \in F \cap G$. As condições de Noether são satisfeitas em P , se qualquer das condições abaixo forem verdadeiras:

- (1) F e G encontrem-se transversalmente em P , $P \in H$.
- (2) P é um ponto simples de F e $I(P, H \cap F) \geq I(P, G \cap F)$.

Demonstração: (2) Faremos uso nesta prova, do seguinte resultado algébrico: $P \in V \subset A^n$ é variedade, $I = I(V)$ e $I \subset J \subset K[x_1, \dots, x_n]$ ideais. Se J' denota a imagem de J em $\Gamma(V)$, então: $O_P(A^n)/JO_P(A^n)$ é isomorfo a $O_P(V)/J'O_P(V)$ ($P/q \mapsto P + I(V)/q + I(V) + J'O_P(V)$ é um homomorfismo sobrejetor com núcleo $JO_P(A^n)$).

O fato de $I(P, H \cap F) \geq I(P, G \cap F) \Rightarrow \text{ord}_P^F(H) \geq \text{ord}_P^F(G)$; pela propriedade (8) de número de intersecção, assim $\bar{H}_* \in (\bar{G}_*) O_P(F)$, e pelo resultado algébrico acima, temos que $O_P(F)/(\bar{G}_*) \cong O_P(P^2)/(F_*, G_*)$, logo o resíduo de H_* em $O_P(P^2)/(F_*, G_*)$ é zero, como desejávamos.

(1) É consequência de (2) acima, de fato, se F e G encontram-se transversalmente em P , então $m_P(F) = m_P(G) = 1$, além disso, F e G não têm tangentes comuns em P , logo P é ponto simples de F , e pela propriedade (5) de número de intersecção, temos que $I(P, F \cap G) = m_P(F) m_P(G) = 1 \cdot 1 = 1$. Como

$$P \in H \cap F \Rightarrow I(P, H \cap F) \geq 1 \Rightarrow I(P, H \cap F) \geq 1 = I(P, F \cap G).$$

Segue então do item (2) acima, o desejado.

Corolário : Se

(1) F e G encontram-se em $(\deg F) \cdot (\deg G)$ pontos distintos e H passa por esses pontos, ou

(2) Todos os pontos de $F \cap G$ são pontos simples de F e $H.F > G.F$,

então, existe uma curva B, tal que $B.F = H.F - G.F$.

Demonstração: (1) Se F e G encontram-se em $(\deg F) \cdot (\deg G)$ pontos distintos, segue pelo corolário 2 do Teorema de Bezout que tais pontos são todos pontos simples sobre F e sobre G, isto é, $m_P(F) = m_P(G) = 1$, para todo $P \in F \cap G$. Se fizermos $F.G = \sum I(P, F \cap G)P = 1P_1 + \dots + 1P_r$, onde $r = (\deg F) \cdot (\deg G)$. Como o grau de $F.G$ é $(\deg F) \cdot (\deg G) \Rightarrow I(P, F \cap G) = 1$, para todo $P \in F \cap G$.

Assim, temos que F e G encontram-se transversalmente em cada $P \in F \cap G$ e estes pontos pertencem a H. Logo, por (1) da proposição 5.1, segue que as condições de Noether são satisfeitas em cada $P \in F \cap G$. Sendo assim, pelo Teorema Fundamental de Max Noether, existem A e B, formas de graus determinados, tais que $H = AF + BG$, logo existe B, tal que $B.F = H.F - G.F$.

(2) $H.F > G.F \Rightarrow \sum I(P, H \cap F)P > \sum I(P, G \cap F)P \Leftrightarrow \Leftrightarrow I(P, H \cap F) \geq I(P, G \cap F)$ para todo P, além disso, todos os pontos $P \in F \cap G$ são pontos simples de F, segue da proposição 5.1 (2) que as condições de Noether são satisfeitas em cada $P \in F \cap G$, assim existe B, tal que $B.F = H.F - G.F$.

2. Algumas Aplicações do Teorema Fundamental de Max Noether

Daremos a seguir, algumas aplicações interessantes do Teorema Fundamental de Max Noether. Dentre elas estão os Teoremas de Pascal e Pappas. Definiremos também adição sobre uma cúbica e mostraremos que a cúbica, com esta operação é um grupo abeliano.

Proposição 5.2: Sejam C, C' , cúbicas, $C'.C = \sum_{i=1}^9 P_i$. Suponha que Q é uma cônica e $Q.C = \sum_{i=1}^6 P_i$. Assuma que os pontos $P_1, \dots, P_6$ são pontos simples sobre C , então P_7, P_8 e P_9 encontram-se sobre uma reta.

Demonstração: Temos, por hipótese, que todos os pontos de $Q \cap C$ são pontos simples de C , e como $I(P, C' \cap C) \geq I(P, Q \cap C)$ para todo P , segue que $C'.C \succ Q.C$. Assim, pelo corolário (2) da prop. 5.1., existe B , tal que $B.C = C'.C - Q.C \Rightarrow \sum I(P, B \cap C) = \sum I(P, C' \cap C) - \sum I(P, Q \cap C)$ e pelo Teorema de Bezout, temos que $\deg B = \deg C' - \deg Q = 3 - 2 = 1$, e como ainda $B.C = C'.C - Q.C = P_7 + P_8 + P_9$, segue que B é uma reta passando por P_7, P_8 e P_9 .

Desta proposição, segue o clássico Teorema de Pascal (o hexágono místico).

Teorema de Pascal: Se um hexágono é inscrito em uma cônica irreduzível, então os pares de lados opostos encontram-se em pontos colineares.

Demonstração: Sejam as retas: F_i , definida por P_i e P_{i+1} , com $i = 1, \dots, 5$ e F_6 , definida por P_6 e P_1 . Consideremos as cúbicas: $C = F_1 F_3 F_5$, $C' = F_2 F_4 F_6$, e Q a cônica irreduzível, na qual o hexágono está inscrito. Queremos mostrar que P_7 , P_8 e P_9 são colineares (veja o desenho acima). Temos que $C \cdot C' = \sum_{i=1}^9 I(P, C \cap C')P = \sum I(P, (F_1 F_3 F_5) \cap (F_2 F_4 F_6))P = \sum_{i=1}^9 P_i$; $C \cdot Q = \sum I(P, (F_1 F_3 F_5) \cap Q)P = \sum_{i=1}^6 P_i$, todos os pontos de $C \cap Q$ são simples para C . Assim, pela proposição 5.2 acima, temos que P_7 , P_8 e P_9 são colineares.

Outro resultado interessante é o seguinte: se a intersecção dos lados opostos de um hexágono são três pontos colineares, então os vértices de tal hexágono encontram-se sobre uma cônica. De fato, tomando-se como referência o mesmo desenho acima, suponha que P_7 , P_8 e P_9 pertençam a reta B e sejam as cúbicas $C = F_1 F_3 F_5$ e $C' = F_2 F_4 F_6$, temos então que $C \cdot C' = \sum_{i=1}^9 P_i$ e que $B \cdot C = P_7 + P_8 + P_9$. Assim sendo $C \cdot C' \succ B \cdot C$, e $P_1, \dots, P_6$ são pontos simples sobre C . Logo, pelo corolário (2) da proposição 5.1, existe uma curva Q , tal que $Q \cdot C = C \cdot C' - B \cdot C$, com $\deg Q = \deg C' - \deg B = 3 - 1 = 2$. Assim Q é cônica

e $Q.C = \sum_{i=1}^6 P_i$. Portanto, os vrtices do hexgono esto sobre uma cnica.

Vejamos agora, o teorema de Pappas:

Teorema de Pappas: Sejam L_1, L_2 duas retas, tais que $P_1, P_2, P_3 \in L_1$ e $Q_1, Q_2, Q_3 \in L_2$ (nenhum desses pontos em $L_1 \cap L_2$). Seja L_{ij} a reta entre P_i e Q_j , $i \neq j$. Para cada i, j, k com $\{i, j, k\} = \{1, 2, 3\}$. Seja $R_k = L_{ij} \cap L_{ji}$, ento R_1, R_2 e R_3 so colineares.

Demonstrao: Seja a cnica $Q = L_1 L_2$ e as cbicas $C = L_{32} L_{13} L_{21}$, $C' = L_{23} L_{31} L_{12}$, temos que $C \cap Q$ um conjunto com $(\deg Q)(\deg C)$ pontos distintos $(P_1, P_2, P_3, Q_1, Q_2, Q_3)$, logo, pelo corolrio (2) do Teorema de Bezout, so todos pontos simples sobre C e Q , em particular sobre C . Temos ainda que $C.C' = \sum I(P, C \cap C')P = P_1 + P_2 + P_3 + Q_1 + Q_2 + Q_3 + R_1 + R_2 + R_3$, $Q.C = \sum I(P, Q \cap C)P = P_1 + P_2 + P_3 + Q_1 + Q_2 + Q_3 \Rightarrow C.C' \sim Q.C$ e pelo corolrio (2) da proposio 5.1 existe B , tal que $B.C = C.C' - Q.C \Rightarrow B.C = R_1 + R_2 + R_3$, e pelo Teorema de Bezout $\deg B = \deg C' - \deg Q = 3 - 2 = 1$. Portanto R_1, R_2 e R_3 so colineares.

Mostraremos agora, que: Se C for uma cúbica irreduzível, L uma reta, tal que $L.C = P_1 + P_2 + P_3$, P_i distintos, L_i as retas tangentes a C em P_i ; $L_i.C = 2P_i + Q_i$, para algum Q_i ($i = 1, 2, 3$). Então Q_1, Q_2 e Q_3 são colineares.

De fato, denotemos por C' a cúbica $C' = L_1 L_2 L_3$, temos que C e C' não têm componentes comuns, pois $L_i \cap C = \{P_i, Q_i\}$. Assim, $C.C' = \sum I(P, C \cap C')P = \sum I(P, C \cap (L_1 L_2 L_3))P = L_1.C + L_2.C + L_3.C = 2P_1 + 2P_2 + 2P_3 + Q_1 + Q_2 + Q_3$. Sendo L uma reta, L^2 é uma cônica, além disso, $L^2.C = L.C + L.C = 2P_1 + 2P_2 + 2P_3$ e $C.C' > L^2.C$. Como $L.C = P_1 + P_2 + P_3$, e estes são distintos; segue pelo corolário (2) do Teorema de Bezout que P_1, P_2, P_3 são pontos simplés sobre C . Logo pelo corolário (2) da proposição 5.1, segue que existe B , tal que $B.C = C'.C - L^2.C = Q_1 + Q_2 + Q_3$. Pelo Teorema de Bezout, temos que $\deg B = \deg C' - \deg L^2 = 3 - 2 = 1$.

Portanto, os Q_i 's estão alinhados, uma vez que pertencem a reta B .

Partiremos agora, para o objetivo de definir a adição sobre uma cúbica. Fazemos antes, no entanto, uma proposição que nos auxiliará a provar que a operação que definiremos é associativa.

Proposição 5.3 Seja C uma cúbica irreduzível, C' e C'' cúbicas.

Suponha $C.C' = \sum_{i=1}^9 P_i$, onde os P_i 's não são necessariamente distintos, porém são simples sobre C , e suponha que $C'' = C = \sum_{i=1}^8 P_i + Q$, então $Q = P_9$.

Demonstração: Seja L uma reta sobre P_9 que não passa por Q .

Temos que $L.C = P_9 + R + S$, com $R, S \in L \cap C$. Assim,

$$(LC'').C = \sum I(P, LC'' \cap C)P = L.C + C''.C = P_9 + R + S + \sum_{i=1}^8 P_i + Q = \sum_{i=1}^9 P_i + Q + R + S = C'.C + Q + R + S. \text{ Dessa forma,}$$

observamos que $(LC'').C \succ C'.C$, e por hipótese, todos os pontos sobre $C' \cap C$ são pontos simples sobre C . Assim pelo corolário (2) da proposição 5.1, existe B , tal que $B.C = (LC'').C - C'.C = Q + R + S$ e temos que $\deg B = \deg (L.C'') - \deg C' = 4 - 3 = 1$, logo B é uma reta que contém R e S , logo coincide com $L \Rightarrow L.C = B.C \Rightarrow P_9 = Q$.

Adição sobre uma cúbica: Seja C uma cúbica não singular, portanto irredutível, como vimos no último capítulo. Para quaisquer dois pontos $P, Q \in C$, existe uma única reta L , tal que $L.C = P + Q + R$, para algum $R \in C$ (se $P = Q$, então L é a tangente a C em P). Definimos $\phi = C \times C \rightarrow C$, colocando $\phi(P, Q) = R$, ϕ é como uma adição sobre C , porém não existe identidade. Para remediar isso, escolheremos um ponto 0 sobre C e então definimos uma adição $\oplus$ sobre C como segue: $P \oplus Q = \phi(0, \phi(P, Q))$.

Proposição 5.4: A cúbica não singular C com a operação $\oplus$ forma um grupo abeliano com o ponto 0 sendo a identidade.

Demonstração: Pela maneira como definimos ϕ é óbvio que $\oplus$ é uma operação fechada em C . Mostraremos então, que:

(i) $\oplus$ é comutativa, dados $P, Q \in C$, existe uma única reta L , tal que $L.C = P + Q + R$, claramente $\phi(P, Q) = \phi(Q, P) = R$, assim $P \oplus Q = \phi(0, \phi(P, Q)) = \phi(0, R) = \phi(0, \phi(Q, P)) = Q \oplus P$.

(ii) $0 \in C$ é o elemento neutro, uma vez que dado $P \in C$, temos uma

reta única L , com $L.C = O + P + R$. Assim, $P \oplus O = \phi(O, \phi(P, O)) = \phi(O, R) = P$.

(iii) $\oplus$ é associativa, suponha $P, Q, R \in C$. Seja $L_1.C = P + Q + S'$; $M_1.C = O + S' + S$; $L_2.C = S + R + T'$; $M_2.C = Q + R + U'$; $L_3.C = O + U' + U$; $M_3.C = P + U + T''$, desde que: $(P \oplus Q) \oplus R = |\phi(O, \phi(P, Q))| \oplus R = |\phi(O, S')| \oplus R = S \oplus R = \phi(O, \phi(S, R)) = \phi(O, T')$ e $P \oplus (Q \oplus R) = P \oplus |\phi(O, \phi(Q, R))| = P \oplus |\phi(O, U')| = P \oplus U = \phi(O, \phi(P, U)) = \phi(O, T'')$ é suficiente mostrar que $T' = T''$.

Sejam $C' = L_1 L_2 L_3$, $C'' = M_1 M_2 M_3$, temos que $C'.C = \sum I(P, C' \cap C)P = L_1.C + L_2.C + L_3.C = (P + Q + S') + (S + R + T') + (O + U' + U)$. Todos os pontos de $C' \cap C$ são simples sobre C , pois C é não singular, além disso $C''.C = M_1.C + M_2.C + M_3.C = (O + S' + S) + (Q + R + U') + (P + U + T'')$, então, pela proposição 5.3, temos que $T' = T''$, logo $\phi(O, T') = \phi(O, T'')$ e portanto $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

(iv) Dado P , quero encontrar $(-P)$, tal que $P \oplus (-P) = \phi(O, \phi(P, -P)) = 0$. Seja L_1 a reta tangente a C em O , então, $L_1.C = O + O + R$, e L_2 a reta, tal que $L_2.C = P + R + X$, então $-P = X$. De fato, $P \oplus X = \phi(O, \phi(P, X)) = \phi(O, R) = 0$.

Portanto, $(C, \oplus)$ é grupo abeliano.

Na verdade, dada uma cúbica irredutível C , qualquer, se denotarmos por C^0 o conjunto dos pontos simples de C , $O \in C^0$, então C^0 , com a operação $\oplus$ definida acima, é um grupo abeliano. Se dados $P, Q \in C^0$ tivermos $\phi(P, Q) \in C^0$, como $O \in C^0$, isso implicará que $P \oplus Q = \phi(O, \phi(P, Q)) \in C^0$, e daí a maneira de provar que $(C^0, \oplus)$ é grupo abeliano é semelhante a feita acima.

Seja então $P, Q \in C^0$, mostraremos que $\phi(P, Q) \in C^0$. De fato, suponha inicialmente que $P \neq Q$, então temos uma única reta L , tal que $L.C = P + Q + R$, para $R \neq Q$ e $R \neq P$, temos $L.C = I(P, L \cap C)P + I(Q, L \cap C)Q + I(R, L \cap C)R$, logo $I(R, L \cap C) = 1$, e pela propriedade (5) para número de intersecção, $1 \geq m_R(L).m_R(C) \geq 1 \Rightarrow m_R(C) = 1 \Rightarrow R \in C^0$. Já se $P = Q$, então a reta tangente a C em P , L é tal que $L.C = P + P + R$, logo para $R \neq P$ teríamos $L.C = I(P, L \cap C)P + I(R, L \cap C)R = 2P + I(R, L \cap C)R \Rightarrow I(R, L \cap C) = 1 \geq m_R(L).m_R(C) \geq 1 \Rightarrow m_R(C) = 1 \Rightarrow R \in C^0$. Portanto, $P \oplus Q \in C^0$ e $(C, \oplus)$ é grupo abeliano.

BIBLIOGRAFIA

- 1 ATIYAH, M.F. & MACDONALD, I.G. *Introduction to Commutative Algebra*. London, Addison-Wesley Publishing, 1969. 128p.
- 2 FULTON, W. *Algebraic Curves: An Introduction to Algebraic Geometry*. London, Benjamin/Cummings Publishing, 1969. 226p.
- 3 HARTSHORNE, R. *Algebraic Geometry*. New York, Springer-Verlag, 1987. 496p.
- 4 HEFEZ, A. *Introdução à Geometria Projetiva*. Vitória, Sociedade Brasileira de Matemática, 1989. 76p. Trabalho apresentado a 10.^a Escola de Álgebra, Vitória, 1989.
- 5 MATSUMURA, H. *Commutative Algebra*. London, Benjamin/Cummings Publishing, 1980, 312p.
- 6 REID, M. *Undergraduate Algebraic Geometry*. 2.^a ed. Coventry, University of Warwick, 1988. 111p.
- 7 SHAFAREVICH, I.R. *Basic Algebraic Geometry*. New York, Springer-Verlag, 1974.
- 8 VAINSENCHER, I. *Introdução às Curvas Algébricas Planas*. IN: COLÓQUIO BRASILEIRO DE MATEMÁTICA, 12. Poços de Caldas, 1979. Rio de Janeiro, IMPA, 1979. 174p.