Introdução às Curvas Algébricas Planas

Israel Vainsencher

INSTITUTO DE MATEMÁTICA PURA E APLICADA
Rua Luiz de Camões, 68
20.060 - Rio de Janeiro - RJ

PREFÁCIO

> ..."la première est toujours si astreinte à la considération des figures, qu'elle ne peut exercer l'entendement sans fatiguer beaucoup l'imagination; et on s'est tellement assujetti en la dernière à certaines règles et à certams chiffres, qu'on en a fait un art confus et obscur qui embarrasse l'esprit[43] au lieu d'une science qui le cultive".

Após enunciar este veredito, Descarte propôs-se a tomar o melhor da Geometria e da Álgebra, corrigindo os defeitos de uma pelas virtudes da outra. Nascia a Geometria Analítica Clássica. Dela são sucedâneas a Geometria Diferencial e a Geometria Algébrica.

Apesar da origem comum, é claro o desequilíbrio verificado nos currículos atuais quanto ao tratamento dispensado aos aspectos introdutórios dessas duas disciplinas. O estudante é devidamente apresentado ao triedro de Frenet, torção, curvatura... mas se passa a distância do plano projetivo e curvas algébricas.

Estas notas foram escritas com o objetivo de servir de texto a um curso de 1 semestre, como disciplina eletiva destinada a alunos do 3º/4º ano do Bacharelado, ou ainda como disciplina de iniciação científica.

O teorema de Bezout é o resultado central do curso. Para apresentá-lo com vigor, é necessário empreender uma jornada razoá

vel.

Nosso ponto de partida são as curvas planas usualmente estudadas na geometria elementar, tais como retas, cônicas, conchóides, etc. ... Passamos em seguida a uma revisão crítica do conceito de curva algébrica, formulando uma definição rigorosa, ainda que mais abstrata.

No Capítulo II, iniciamos o estudo da interseção de 2 curvas. Introduzimos a resultante de 2 polinômios e concluimos com um caso particular do teorema dos zeros de Hilbert.

Nos Capítulos III e IV são exploradas as idéias básicas necessárias à demonstração do teorema de Bezout. Para que curvas de graus m e n se intersectem "sempre" em mn pontos, é necessário explicar como alguns desses pontos devem ser contados mais de uma vez, quer seja por tangência quer pelo fato de uma das curvas "passar várias vezes" pelo ponto em questão; por fim, deve-se explicar como alguns outros podem estar no infinito...

No Capítulo V demonstramos o Teorema de Bezout. No capítulo seguinte estudamos mais detalhadamente o índice de interseção de 2 curvas.

O Capítulo VII constitui-se quase que numa revisão da matéria: aplicamos o Teorema de Bezout ao cálculo do número de tangentes inflexionais de uma curva e o de tangentes que passem por um ponto.

No Capítulo VIII ocorre uma certa mudança no objeto de estudo. Até então estivéramos interessados no aspecto conjuntista, analisando propriedades de uma curva como subconjunto do plano; agora

examinamos o seu caráter funcional, i.e., propriedades do corpo de funções racionais.

O último tópico - cúbicas não singulares - tenta mostrar o sabor de coisa inacabada, mal disfarçando a esperança de que o aluno recorra à bibliografia indicada para explorar com mais profundidade o roteiro aqui iniciado.

Gostaria de registrar meus agradecimentos à Comissão Organizadora; ao Yves, Karl Otto e Celso por várias sugestões e, em especial, ao Antonio Carlos pelo espírito crítico com que leu o manuscrito.

Recife, 29/06/1979.

ÍNDICE

Pág.

CAPÍTULO I

DEFINIÇÕES PRELIMINARES E EXEMPLOS

§1. Um pouco de história

A manipulação de expressões do tipo $X^2+Y^2 = 1$ é um fato relativamente recente na história da Matemática, podendo se situar em torno do século XVI. Mas os matemáticos gregos já sabiam efetuar cálculos elaborados, recorrendo a procedimentos geométricos. Por exemplo, para o cálculo do produto de duas quantidades a, b, poderíamos proceder assim:

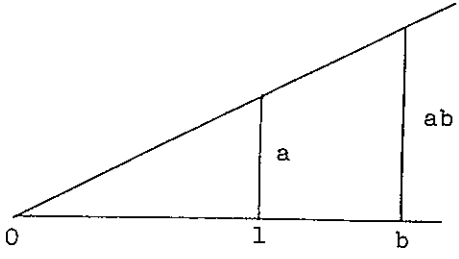


Fig. 1

Neste exemplo, o segmento de comprimento a é traçado perpendicularmente à reta Ob. Esta construção requer somente o desenho de retas e círculos. (Os círculos foram empregados para se obter o ângulo reto).

Com um pouco de imaginação, é possível se descrever métodos para a construção com régua e compasso de expressões do tipo

$$\sqrt{a + \sqrt{ab}}/a^2b \ ,$$

ou mais geralmente, para qualquer elemento do chamado corpo dos números construtíveis[1].

Além das retas e círculos, os matemáticos da Antiguidade estudaram outras curvas, geralmente descritas como o lugar geométrico de pontos satisfazendo a certas condições. Essas curvas especiais eram o recurso empregado na solução de vários problemas, para os quais todas as tentativas com régua e compasso malograram. Alguns desses problemas têm uma história curiosa, em que lenda e fato se misturam. É o caso dos célebres problemas da duplicação do cubo, da trisseção do ângulo e da quadratura do círculo[2]. Veja o Exemplo 6 mais adiante, e o Exercício 1d).

Com a ulterior introdução do método das coordenadas, constatou-se que várias curvas conhecidas desde a Antiguidade podiam ser descritas por equações polinomiais.

1. Definição. Uma curva algébrica plana é o lugar dos pontos cujas coordenadas cartesianas satisfazem a uma dada equação polinomial

$$f(X,Y) = 0 \ ,$$

onde f é um polinômio não constante. (Compare com a Definição 4).

---

1) Veja a discussão no livro "Introdução à Álgebra", de Adilson Gonçalves, pág. 183 e seguintes.

2) Consulte a "História da Matemática" de Carl B. Boyer, tradução de Elza Gomide, pág. 48.

2. Exemplos. Eis aqui uma lista preliminar de curvas algébricas planas. A maioria deve ser bem conhecida do leitor.

1) A reta que passa pelos pontos $(a,b) \neq (c,d)$. Sua equação é

$$\begin{vmatrix} a & c & X \\ b & d & Y \\ 1 & 1 & 1 \end{vmatrix} = 0$$

2) O círculo de raio r e centro (a,b), lugar dos pontos que satisfazem a equação

$$(X-a)^2 + (Y-b)^2 = r^2.$$

3) A elipse, lugar dos pontos cujas distâncias a dois pontos fixos (digamos $(\pm c,0)$) têm soma constante $2a$. A condição imposta escreve-se

$$\sqrt{(X+c)^2 + Y^2} + \sqrt{(X-c)^2 + Y^2} = 2a$$

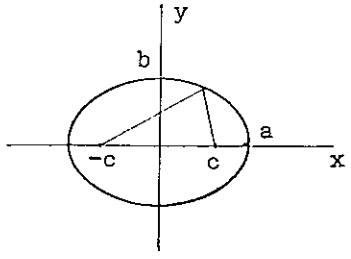


Fig. 2

Esta equação não é polinomial, mas é possível eliminar os radicais e mostrar que toda solução dela é também solução da seguinte

(e vice versa),

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} = 1 \ ,$$

onde $b = \sqrt{a^2-c^2}$.

4) A hipérbole, lugar dos pontos cujas distâncias a dois pontos fixos, chamados focos (digamos $(\pm c,0)$), têm diferença constante 2a. A condição descrita é

$$\sqrt{(X-c)^2 + Y^2} - \sqrt{(X+c)^2 + Y^2} = 2a.$$

Procedendo como no caso da elipse, eliminamos os radicais e obtemos a equação

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1$$

onde $b^2 = c^2-a^2$.

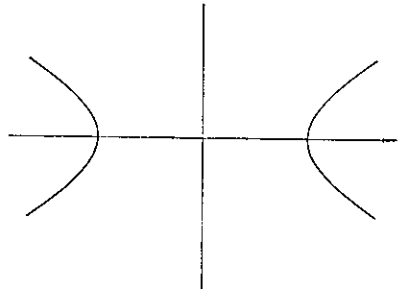


Fig. 3

5) A parábola, lugar dos pontos equidistantes de um ponto fixo (foco, e.g. $(0,b)$, $b > 0$) e de uma reta fixa (diretriz, e.g. $Y = -b$). Sua equação (já simplificada) é,

$$X^2 = 4bY$$

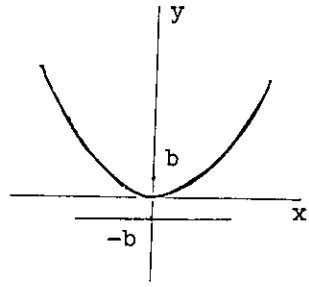


Fig. 4

6) A cissóide de Diocles, lugar dos pés das normais traçadas do vértice de uma parábola às suas tangentes. Dada a parábola de equação $X^2 = 4bY$, a tangente num ponto (x_o, y_o) se escreve

$$x_o X - 4by_o = 2b(Y-y_o) .$$

A normal tomada da origem (que é o vértice) é

$$2bX + x_o Y = 0 .$$

Dessas duas, resulta a equação da cissóide ,

$$bX^2 - Y(Y^2+X^2) = 0 .$$

Note que, em coordenadas polares, essa última equação fornece,

$$r = b \cos \theta \operatorname{cotg} \theta .$$

Daí obteremos uma descrição dinâmica que permite traçar a cissóide. Construa o círculo de diâmetro b e centro $(0, b/2)$.

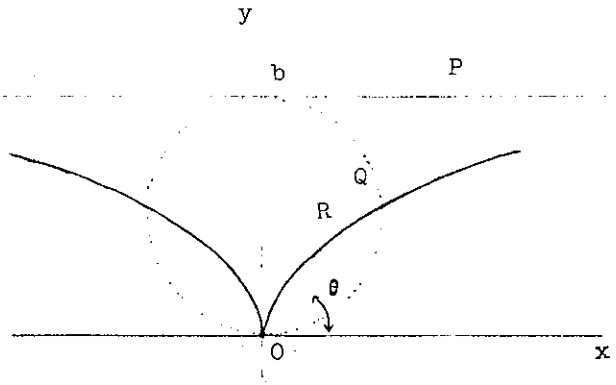


Fig. 5

Considere a reta $Y = b$; para cada um de seus pontos P, trace a reta OP e tome o ponto Q da interseção com o círculo. Finalmente, marque o ponto R tal que $OR = PQ$. Variando P, o ponto R descreve a cissóide. Com efeito, temos

$$PQ = OP - OQ$$

$$= \frac{b}{\operatorname{sen} \theta} - b \operatorname{sen} \theta$$

$$= b \cos \theta \operatorname{cotg} \theta = r \ .$$

A cissóide foi empregada para resolver o problema da duplicação do cubo: dada a aresta de um cubo, construir a aresta do cubo de volume duplo. Em símbolos, procuramos resolver a equação,

$$X^3 = 2b^3 \ ,$$

onde b denota o comprimento da aresta conhecida. Sabe-se que esta equação não é resolúvel por régua e compasso (por exemplo, para $b = 1$). Recorrendo à cissóide como "curva auxiliar", a so-

lução gráfica é obtida com o seguinte procedimento: intersecte a cissóide

$$(b-Y)X^2 = Y^3$$

com a reta

$$b-Y = 2X \ ;$$

obtem-se um ponto (x_o,y_o) com $(y_o/x_o)^3 = 2$. Ligando-o à origem, constrói-se a reta $Y = \sqrt[3]{2}\,X$. Fazendo $X = b$, resulta a quantidade procurada.

Convidamos o leitor a se familiarizar com os exemplos adicionais compilados na lista de exercícios.

Exercícios

1) Esboce as curvas seguintes.

a) Folium de Descartes: $X^3+Y^3 - 3aXY = 0$.

b) Trissectriz de Maclaurin: $X(X^2+Y^2) = a(Y^2-3X^2)$.

c) Caracol de Pascal: $(X^2+Y^2)^2 - 2aX(X^2+Y^2) + (a^2-b^2)X^2 - b^2Y^2 = 0$.

Mostre que em coordenadas polares a equação é

$$r = a\cos\theta \pm b.$$

Distinga os casos $a > b$, $a < b$ e $a = b$. Trata-se da conchóide da circunferência $r = a\cos\theta$ relativa à origem. Em geral, a conchóide de uma curva C relativa a um ponto O e de intervalo

b é construída assim: para cada ponto $P \in C$, marque sobre OP dois segmentos $PA = PA' = b$; os pontos A, A' descrevem a conchóide.

d) Conchóide de Nicomedes: $(X-a)^2(X^2+Y^2) = b^2X^2$. É a conchóide da reta $X = a$, de intervalo b, relativa à origem. Esta curva resolve o problema do cálculo de médias proporcionais: dados os números r, s, encontrar X, Y tais que $X/r = Y/X = s/Y$. A duplicação do cubo e a trisseção do ângulo são problemas desse tipo. A figura abaixo ilustra a construção do ângulo $A\hat{O}P = A\hat{O}B/3$.

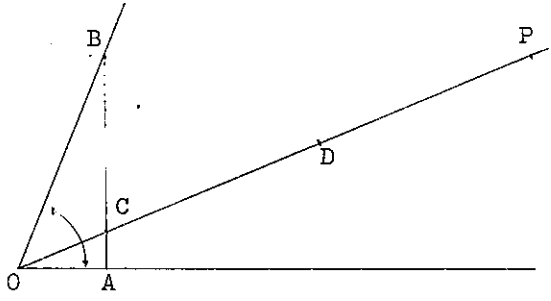


Fig. 6

O ponto P é a interseção da paralela a OA que passa por B, com a conchóide da reta normal BA e intervalo 2OB. Por construção, CP = 2OB. Marcando o ponto médio D de CP, resulta o triângulo isósceles CDB. O leitor não deve ter dificuldade em completar a justificativa da construção.

e) Astróide:

$$X^{2/3} + Y^{2/3} = 1 .$$

Mostre que esta curva é de fato algébrica, dada por uma equação polinomial do sexto grau. Ela é o lugar descrito por um ponto de uma circunferência de raio 1/4 que gira sem deslizar apoiada ao lado interno de uma circunferência unitária centrada na origem. Curvas definidas por esse processo são chamadas de hipociclóides; quando a circunferência se move pelo lado externo, obtem-se uma epiciclóide; elas são algébricas se e só se a razão dos raios é um número racional.

f) Oval de Cassini: $((X-a)^2 + Y^2)((X+a)^2 + Y^2) = b^4$. É o lugar do pontos cujo produto das distâncias aos 2 pontos fixos $(\pm a,0)$ é igual à constante b^2. Se $b^2 < a^2$, a curva consiste de 2 componentes conexas. Se $b^2=a^2$ tem-se a lemniscata de Bernoulli. Para $b^2 > a^2$, tem-se a oval propriamente dita.

2) Mostre que a curva dada parametricamente por

$$x(T) = T^2-T, \quad y(T) = T^3$$

é algébrica, encontrando um polinômio $f(X,Y)$ não constante tal que $f(x(T), y(T)) = 0$.

3) Sejam $x = x(T)$, $y = y(T)$ funções racionais (= quocientes de polinômios em uma variável T). Mostre que existe um polinômio não constante $f(X,Y)$ tal que $f(x,y) = 0$. (Sugestão: seja $k(T)$ o corpo das funções racionais a coeficientes no corpo k. Se $x \in k(T)$ é não constante, então $k(T)$ é uma extensão algébrica do subcorpo $k(x)$ gerado por x, pois se $x = p/q$,

com p,q polinômios então T satisfaz à equação polinomial $p(X) - xq(X) = 0$. Logo, todo $y \in k(T)$ é algébrico sobre $k(x)$).

4) Uma curva é <u>racional</u> se for definida parametricamente por equações

$$X = x(T), \quad Y = y(T),$$

onde as funções de T indicadas são racionais e ao menos uma é não constante. Mostre que toda curva racional é algébrica.

5) <u>Curvas de Lissajous</u>. São dadas parametricamente por

$$x(\theta) = a \operatorname{sen}(m\theta + p), \quad y(\theta) = b \operatorname{sen}(n\theta + q),$$

onde a,b,m,n,p,q são constantes $(abmn \neq 0)$. Curvas desse tipo ocorrem na investigação de fenômenos vibratórios. (a) Esboce a curva, supondo $m = 2$, $n = 3$, $a = b = 1$, $p = 0$, $q = \pi/4$. (b) Mostre que a curva <u>não</u> é algébrica se m/n é irracional. (c) Se m é inteiro, mostre que $x(\theta)$ pertence ao anel A gerado pelas funções $\operatorname{sen}\theta$, $\cos\theta$. (d) Mostre que A é um domínio e que seu corpo de frações é igual a $\mathbb{R}(T)$, onde $T = \operatorname{tg}(\theta/2)$. (e) conclua que uma curva de Lissajous com m/n racional é algébrica. Ache a equação polinomial no caso considerado em (a).

6) Chama-se <u>rosácea</u> uma curva de equação polar

$$r = a \operatorname{sen}(b\theta).$$

(a) Esboce para $a = 1$, $b = 1,2,2/3$. (b) Prove que se $b = m/n$, com m,n inteiros > 0, primos relativos, então a rosácea é algébrica, satisfazendo a uma equação polinomial (em coordenadas car-

tesianas) de grau $m+n$ ou $2(m+n)$ conforme sejam m,n ambos ímpares ou um deles par. Se b é irracional, não é algébrica.

§2. Equação de uma curva algébrica

Reexaminemos a Definição 1. Uma questão que naturalmente se põe é se a equação polinomial $f = 0$ está bem determinada pela curva, i.e., o lugar das soluções. A resposta é não: $f = 0$ e $f^2 = 0$ têm as mesmas soluções. Poderíamos arriscar o palpite de que esse seria o único tipo de indeterminação: se tomássemos f com grau mínimo, talvez todas as outras equações definindo a mesma curva fossem do tipo $f^m = 0$. Mas note que as soluções de $XY = 0$ e $X^2Y = 0$ são as mesmas, desmentindo a proposta. Ah, mas nesse exemplo a curva tem visivelmente 2 "pedaços", e a afirmativa poderia valer para cada um deles. Talvez uma hipótese mais promissora seja esperar que exista uma equação de grau mínimo, as demais sendo múltiplas desta. Mas as curvas (?), ou melhor dizendo, as equações $X^2+Y^2 = 0$ e $2X^2+Y^2 = 0$ têm o mesmo conjunto de soluções reais, desfazendo a esperança.

A escassez de pontos reais nesse último exemplo parece estar na raiz do problema. Com efeito, veremos mais adiante que, se $p(X,Y)$ é um polinômio irredutível e a curva C definida por $p(X,Y) = 0$ é infinita, então a equação de grau mínimo está bem determinada (a menos de fator constante).

Aqui, e em outras situações com que iremos nos defrontar, a bem da simplicidade de uma proposição que desejamos tornar verda-

deira, somos induzidos a repensar os fundamentos, isolar a dificuldade, e resolvê-la "por decreto"[3] .

É o que faremos, passando a admitir pontos cujas coordenadas são números complexos. E, já tomada esta decisão, por que não trabalhar também com polinômios a coeficientes complexos? Na realidade, praticamente em toda a teoria que exporemos, a propriedade decisiva dos números complexos é que estes formam um corpo algebricamente fechado de característica zero. Assim, salvo menção explícita em contrário, doravante, coordenadas de pontos, bem como coeficientes de polinômios, serão tomados em um corpo k algebricamente fechado e de característica zero. Frequentemente, nos exemplos, suporemos $k = \mathbf{C}$.

A perda aparente do recurso à intuição geométrica será amplamente compensada. Já podemos recolher o primeiro benefício.

3. Proposição. Sejam f, g polinômios em 2 variáveis a coeficiente no corpo k. Então $f(X,Y) = 0$ e $g(X,Y) = 0$ têm as mesmas soluções em k^2 se e só se os fatores irredutíveis de f,g são os mesmos.

Demonstração. Seja $p \in k[X,Y]$ um fator irredutível de f. Por hipótese, para cada $(x,y) \in k^2$,

$$p(x,y) = 0 \Rightarrow g(x,y) = 0 .$$

Provaremos que p divide g em $k[X,Y]$. Podemos supor que Y

3) Vale a pena ler a belíssima discussão desse processo de "negação da negação", em "Conceitos Fundamentais da Matemática", de Bento de Jesus Caraça.

ocorre efetivamente em p. Ponhamos $A = k[X]$, $K = k(X)$ (corpo de frações). Assim, $p \in A[Y]$ é não constante. Visto que A é um anel fatorial, sabemos que p é irredutível em $K[Y]$. Se, por absurdo, supusermos $p \nmid g$, então $mdc(p,g) = 1$. Daí, existiria uma relação

$$ap + bg = c ,$$

onde $a,b \in A[Y]$ e $c \in A$, $c \neq 0$. Agora, como p não é constante, exceto para um número finito de valores de x a equação $p(x,Y) = 0$ admite solução. (Aqui usamos o fato de que k é algebricamente fechado). Segue-se que há uma infinidade de valores de x tais que $c(x) = 0$, donde $c = 0$. Esta contradição mostra que $p|g$ em $K[Y]$ e portanto $p|g$ em $A[Y]$.

C.Q.D.

Segue-se da proposição que uma curva algébrica, dada como lugar das soluções de uma equação polinomial não constante $f(X,Y) = 0$, determina (a menos de fator constante) a equação de grau mínimo: tomar o produto dos fatores irredutíveis distintos de f. Este fato nos leva a substituir a Definição 1 pela seguinte, onde passamos a identificar "curva" com sua equação.

4. Definição. Uma curva algébrica plana afim (ou mais abreviamente, curva) é uma classe de equivalência de polinômios não constantes $f \in k[X,Y]$, módulo a relação que identifica dois tais polinômios se um é múltiplo do outro por uma constante $\neq 0$.

Nesse contexto, a equação de uma curva é um qualquer dos po

linômios nessa classe. Dizemos que uma curva está definida sobre o corpo k_o, subcorpo de k, se ela admitir uma equação a coeficientes em k_o.

O traço (resp. traço real...) de uma curva (definida sobre $\mathbb{R}$...) é o conjunto das soluções (resp. soluções reais...) da equação.

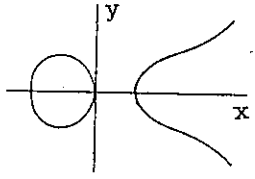
O grau de uma curva f é o grau de sua equação, e será denotado por ∂f. Curvas de grau $1,2,3,\ldots$ são chamadas retas, cônicas, cúbicas...

Usualmente, cometeremos o abuso de designar pelo mesmo símbolo tanto a curva como o seu traço ou uma sua equação. Por comodidade, diremos indistintamente "a curve f" ou "a curva dada pela equação $f = 0$" ou "a curva $f = 0$". O contexto tornará claro quando nos referimos seja ao traço, seja ao polinômio.

Observemos que, agora, as curvas $X^2 = 0$ e $X = 0$, embora tenham o mesmo traço, são consideradas distintas. É sugestivo pensar em X^2 como uma "reta dupla", limite de um par de retas que vêm a coincidir (e.g., $X(X-\varepsilon Y)$, com $\varepsilon \to 0$), ou de elipses que se achatam sobre o eixo (e.g. $X^2 + \varepsilon Y^2 = \varepsilon$).

Uma curva é irredutível se admite uma equação que é um polinômio irredutível. As componentes irredutíveis de uma curva f são as curvas definidas pelos fatores irredutíveis de f. A multiplicidade de uma componente p de f é o expoente com que p ocorre na decomposição de f; quando ≥ 2, dizemos que p é componente múltipla de f.

Intuitivamente, as componentes irredutíveis de uma curva f são os "pedaços" que constituem f e que são também curvas. E de fato, se f contém (o traço de) uma curva irredutível p, então p é uma componente de f. Isto foi demonstrado na Proposição 3. O leitor deve no entanto ser alertado para o fato de que uma curva pode ser irredutível mesmo sendo seu traço real formado por 2 ou mais partes disjuntas. (Veja o Exc.II.3).



$$Y^2 = X(X-1)(X+1)$$

Fig. 7

Na realidade, a determinação do número, bem como da disposição dos circuitos reais de uma curva algébrica plana é uma questão ainda não resolvida por completo[4].

Apesar do aparente contra-senso geométrico, a Definição 4 coloca em definitivo relevo o papel da equação que individualiza uma curva algébrica. Além do mais, frequentemente os argumentos algébricos empregados nas demonstrações de propriedades geométricas se aplicam indistintamente a polinômios sejam eles irredutíveis ou não.

4) Cf. "Problems of Present Day Mathematics", p.50, in Proceedings of Symposia in Pure Math.,Vol. 28, F.E. Browder, Editor (1974).

Exercícios

7) Verifique se as curvas apresentadas no § 1 são irredutíveis.

8) Ache as componentes irredutíveis das curvas:

(a) $Y^3-X^3+X^2Y-XY^2+X^2+Y^2+X-Y-1$

(b) $2X^2Y-2X^3+Y^2-XY+X-Y$

(c) $X^2-5XY+6Y^2$.

9) Seja $f_m = \sum_0^m a_i X^i Y^{m-i}$ um polinômio homogêneo $\neq 0$.

(a) Prove que f_m é o produto de m fatores lineares homogêneos, i.e., $f_m = \prod (b_i X + c_i Y)$, onde b_i , c_i são constantes não ambas nulas e as razões b_i/c_i são bem determinadas. (b) Prove que se f_m, f_{m+1} não têm fator comum, então $f_m + f_{m+1}$ é irredutível.

10) Mostre que $Y^2 - p(X)$ é redutível se e só se $p(X)$ é um quadrado em $k[X]$. Em particular, $Y^2-(X-a)(X-b)(X-c)$ é irredutível para todo $a,b,c \in k$.

11) Mostre que uma cônica $a_{11}X^2 + a_{22}Y^2 + a_{33} + 2a_{12}XY + 2a_{13}X + 2a_{23}Y$ é redutível se e só se $\det(a_{ij}) = 0$.

12) Dado um ponto arbitrário P e duas retas distintas ℓ_1, ℓ_2 contendo P, mostre que o conjunto das retas que contêm P é $\{x_1\ell_1+x_2\ell_2 \mid x_1,x_2$ são constantes não ambas nulas$\}$.

13) Dados 4 pontos não colineares, mostre que existem cônicas f_1, f_2 tais que, a condição necessária e suficiente para que uma cônica f passe pelos 4 pontos é que f seja da forma $x_1f_1+x_2f_2$, com $x_i \in k$, não ambas nulas.

14) Dados 5 pontos arbitrários, existe ao menos uma cônica que os contém; se existirem 2 distintas, então 4 deles são colineares.

15) Mostre que, para todo inteiro $d \geq 1$, existem $\frac{d(d+3)}{2}$ pontos no plano pelos quais passa exatamente uma curva de grau d.

16) Seja C a cúbica $Y = X^3$. Para cada par de pontos $P,Q \in C$, a reta PQ intercepta C num 3º ponto R. Mostre que a correspondência que associa e cada par (P,Q) o simétrico $-R$ de R em relação à origem O dá a C uma estrutura de grupo.

§3. Mudança de coordenadas

As propriedades de curvas planas que estudaremos são aquelas que independem do particular sistema de coordenadas cartesianas empregado. Faremos aqui alguns comentários sobre mudança de coordenadas e daremos a conceituação precisa de "propriedade independente do referencial".

5. Definição. Um referencial ou sistema de coordenadas afim no plano k^2 consiste de um ponto $\mathcal{O} \in k^2$, chamado ori-

gem do referencial, e de uma base $\{v_1,v_2\}$. O referencial canônico é dado por $\mathcal{O} = O(=(0,0))$, $v_1 = (1,0)$, $v_2 = (0,1)$. O vetor coordenadas de um ponto $P \in k^2$ em relação a um referencial $\mathcal{R} = \{\mathcal{O},\{v_1,v_2\}\}$ é o par $(P)_{\mathcal{R}} = (x_1,x_2)$ tal que

$$P = \mathcal{O} + x_1v_1+x_2v_2 \ . \tag{5.1}$$

Uma transformação afim ou afinidade em k^2 é uma aplicação $T: k^2 \to k^2$ composta de uma translação com um isomorfismo linear. A ambiguidade aparente na ordem da composição é irrelevante, pois se L é uma aplicação linear e $P_o \in k^2$, temos $L(P+P_o) = L(P) + L(P_o)$. Isso mostra que uma translação seguida de uma aplicação linear tem o mesmo efeito que a (mesma) aplicação linear seguida de uma (outra) translação. Toda transformação afim é da forma $T(x_1,x_2) = (y_1,y_2)$, onde

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + a_1 \\ y_2 = a_{21}x_1 + a_{12}x_2 + a_2 \end{cases} , \tag{5.2}$$

com $\det(a_{ij}) \neq 0$. O leitor verificará sem dificuldade que as afinidades formam um grupo com a operação de composição. Em particular, a composta de duas afinidades é uma afinidade, e a inversa de uma afinidade também é.

Escrevendo $v_1 = (a_{11},a_{21})$, $v_2 = (a_{12},a_{22})$, $\mathcal{O} = (a_1,a_2)$, podemos interpretar (5.2) como as equações que relacionam $P = (y_1,y_2)$ com $(P)_{\mathcal{R}} = (x_1,x_2)$. E reciprocamente, podemos considerar (5.1) como definindo a afinidade,

$$(x_1,x_2) \mapsto \mathcal{O} + x_1v_1 + x_2v_2 .$$

6. Definição. Dizemos que a afinidade T e o referencial $\mathcal{R}$ são associados se

$$T(P)_{\mathcal{R}} = P \quad (\forall\ P \in k^2).$$

Assim, podemos adotar 2 atitudes diante do processo de mudança de coordenadas: dada uma afinidade T, podemos olhar a relação $(y_1,y_2) = T(x_1,x_2)$ como a expressão que dá as novas coordenadas de um mesmo ponto em termos das antigas; os pontos ficam e as coordenadas movem-se. A outra possibilidade, é a de considerar T agindo sobre os pontos do plano: (y_1,y_2) é a nova posição de (x_1,x_2), com as coordenadas todas tomadas em relação ao referencial canônico.

7. Definição. Uma afinidade $T: k^2 \to k^2$ induz um k-automorfismo do anel de polinômios em 2 variáveis,

$$T_*: k[X_1,X_2] \to k[X_1,X_2]$$

tal que,

$$\forall\ (x_1,x_2) \in k^2, \quad (T_*\ f)(x_1,x_2) = f(T^{-1}(x_1,x_2)).$$

Mais precisamente, se

$$T^{-1}(x_1,x_2) = (b_{11}x_1 + b_{12}x_2 + b_1, b_{21}x_1 + b_{22}x_2 + b_2) ,$$

então

$$(T_*f)(X_1,X_2) = f(b_{11}X_1 + b_{12}X_2 + b_1,\ b_{21}X_1 + b_{22}X_2 + b_2).$$

8. Proposição. Sejam f uma curva e T uma afinidade. Então o traço de $T_{\cdot}f$ é igual à imagem do traço de f por T.

Demonstração. Imediata.

9. Definição - Seja T uma afinidade e seja $\mathcal{R}$ o referencial associado. A equação de uma curva f em relação a $\mathcal{R}$ é $(T_{\cdot})^{-1}f$.

A definição se justifica porque, para cada $P = (x,y)$, temos

$$P \in f \iff f(x,y) = 0$$
$$\iff ((T_{\cdot})^{-1}f)(T^{-1}(x,y)) = 0$$
$$\iff ((T_{\cdot})^{-1}f)((P)_{\mathcal{R}}) = 0 .$$

10. Definição. Dizemos que uma propriedade $\mathcal{P}$ relativa a curvas (ou a configurações planas, tais como conjuntos de pontos, retas, etc. ...) é uma propriedade invariante ou independente do referencial se, para toda afinidade T, uma curva f (ou configuração C) satisfaz $\mathcal{P}$ se e só se $T_{\cdot}f$ (resp. $T(C)$) satisfaz $\mathcal{P}$.

Por exemplo, o grau de uma curva é uma propriedade invariante. A propriedade de 3 retas serem concorrentes, bem como a de um ponto pertencer a uma curva, são invariantes. Já o requerimento de que 2 pontos no plano real sejam equidistantes de um terceiro não é invariante; no entanto, a propriedade de um ponto ser colinear com, e equidistante de 2 outros é invariante! (Leitor: verifique!).

Nos próximos capítulos estudaremos várias propriedades invariantes de curvas algébricas. Enfatizaremos o fato delas serem independentes do referencial apenas quando a verificação a ser feita revelar-se um desafio instrutivo.

Exercícios

17) Ache as coordenadas do ponto (1,2) no referencial $\{(1,1), \{(1,2),(3,5)\}\}$.

18) Prove que 2 triângulos quaisquer são congruentes por uma afinidade, i.e., se $\{P_1,P_2,P_3\}$ e $\{Q_1,Q_2,Q_3\}$ são conjuntos de 3 pontos não colineares existe uma afinidade T tal que $TP_i = Q_i \quad \forall\, i = 1,2,3$. Verifique se 2 quadriláteros são sempre congruentes por uma afinidade.

19) Se L_i (resp. M_i) são 3 retas distintas concorrentes, existe uma afinidade T tal que $T.L_i = M_i$ $(i = 1,2,3)$?

20) Representação matricial. Seja T uma afinidade. Sejam

$$(a_1,a_2) = T(0,0), \quad (a_{11},a_{21}) = T(1,0) - T(0,0),$$
$$(a_{12},a_{22}) = T(0,1) - T(0,0).$$

Definimos

$$M_T = \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{21} & a_{22} & a_2 \\ 0 & 0 & 1 \end{pmatrix}$$

(a) Prove a fórmula

$$[TP] = M_T[P] , \quad \forall\, P \in k^2$$

onde $[(x,y)] = \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$.

(b) Prove que $M_{TT'} = M_T\, M_{T'}$ para todo par de afinidades T,T'.

(c) Mostre que a correspondência $T \mapsto M_T$ é um isomorfismo do grupo das afinidades de k^2 sobre o grupo dos isomorfismos lineares de k^3 que deixam invariante o plano $X_3 = 1$.

21) <u>Cônicas afins</u>. São definidas por um polinômio do 2º grau,

$$f(X_1,X_2) = a_{11}X_1^2+a_{22}X_2^2+a_{33}+2a_{12}X_1X_2+2a_{13}X_1+2a_{23}X_2 ,$$

com ao menos um dos coeficientes dos termos de grau 2 não nulo. Seja $S_f = (a_{ij})$, a matriz simétrica formada pelos coeficientes de f.

(a) Mostre que

$$f(X_1,X_2) = (X_1,X_2,1)\; S_f\; {}^t(X_1,X_2,1) \qquad \text{(produto de matrizes)}$$

onde t significa "transposta".

(b) Mostre que, para toda afinidade T ,

$$S_{T.f} = {}^tM_T^{-1}\; S_f\; M_T^{-1}$$

onde M_T é a matriz definida no exercício anterior.

(c) Supondo $k = \mathbb{R}$, mostre que, dada f, existe T tal que

$$T.f = X_1^2 + b_{22}X_2^2 + b_{33} + 2b_{23}X_2$$

(Sugestão: completar quadrados).

(d) Ainda supondo $k = \mathbb{R}$, mostre que f é congruente a exatamente uma das seguintes: $X_1^2+X_2^2-1$, $X_1^2-X_2^2-1$, $X_1^2-X_2$, $X_1^2+X_2^2+1$, $X_1^2+X_2^2$, $X_1^2-X_2^2$, X_1^2+1, X_1^2-1, X_1^2. Nos 4 primeiros tipos S_f tem posto 3; nos 4 seguintes, o posto é 2 e no último é 1.

(e) Supondo agora $k = \mathbb{C}$, Mostre que esses 9 tipos de cônicas reduzem-se a apenas 5: $X_1^2+X_2^2-1$, $X_1^2-X_2$, $X_1^2-X_2^2$, X_1^2-1, X_1^2.

22) Determine todas as afinidades que deixam invariante a cúbica $f = Y^2 - X(X-1)(X-\lambda)$, onde λ é uma constante. Distinguir os vários casos ($\lambda = 0$, $\lambda = 1$, etc ...)

CAPÍTULO II

INTERSEÇÕES DE CURVAS PLANAS

Vimos em alguns exemplos no Capítulo I a importância atribuída desde a Antiguidade ao estudo da interseção de 2 curvas. Descartes e Newton chegaram a proclamar que o interesse principal das curvas algébricas é o de fornecer soluções geométricas a equações algébricas por meio de interseção de curvas do menor grau possível[1].

Apresentaremos neste capítulo alguns aspectos gerais do problema. Inicialmente, veremos que a interseção de 2 curvas sem componentes em comum é finita. Descrevemos em seguida o processo da resultante para a determinação dos pontos de interseção. Finalizamos dando uma demonstração de um caso particular do Nullstellensatz (teorema dos zeros) de Hilbert, o qual fornece uma condição para que um sistema de equações polinomiais admita solução.

§1. Finitude da interseção

Comecemos destacando o argumento usado na demonstração de (I.3).

---

1) Veja o "Cours de géométrie algébrique" vol. 1 de J. Dieudonné, pag. 17.

1. Lema . Sejam $f,g \in k[X,Y]$ polinômios sem fatores irredutíveis em comum. Então existe uma relação

$$af + bg = c(X) ,$$

onde $a,b \in k[X,Y]$ e c é um polinômio não nulo da variável X. Resultado análogo vale trocando X por Y.

Demonstração. Ponhamos $A = k[X]$, $K = k(X)$. Consideremos f,g como elementos de $K[Y]$. Visto que f,g não admitem fator comum em $A[Y]$, também não o admitem em $K[Y]$ (leitor: por que?). Como $K[Y]$ é um domínio de ideais principais, segue-se uma relação

$$rf + sg = 1 \quad \text{em} \quad K[Y].$$

Eliminando denominadores de r,s, obtemos a relação prometida.

C.Q.D.

Se $f \in k[X]$ é um polinômio não constante, sabemos que a equação $f(X) = 0$ admite no máximo um número finito de soluções. O próximo resultado é uma versão deste fato para polinômios em 2 variáveis.

2. Proposição. O conjunto das soluções de um sistema de 2 equações polinomiais a duas incógnitas sem fator irredutível comum é finito.

Reformulando em linguagem geométrica, temos, equivalentemente:

3. Proposição. A interseção de duas curvas algébricas planas sem componentes em comum é finita.

Demonstração. Apliquemos o Lema 1 aos polinômios $f(X,Y)$, e $g(X,Y)$, onde $f,g \in k[X,Y]$ não admitem fator comum. Obtemos relações

$$af+bg = c(X)$$
$$uf+vg = w(Y)$$

onde $a,b,\ldots,w$ são polinômios, $c(X)$, $w(Y)$ são não nulos e envolvem só a variável indicada. Dessas relações é evidente que toda solução de $f = g = 0$ tem para abscissa uma raiz de $c(X)$ e para ordenada uma raiz de $w(Y)$, todas em número finito. C.Q.D.

Exemplo: Consideremos as interseções da hipérbole $f: XY = 1$ com retas $\ell: aX+bY = c$. A figura abaixo ilustra as possibilidades:

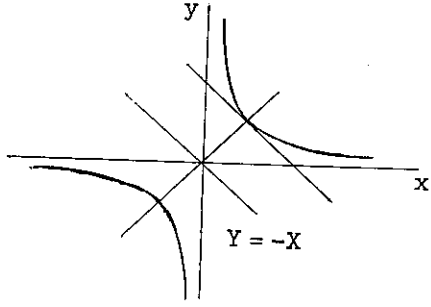


Fig. 8

As retas $X = 0$ e $Y = 0$ não cortam a hipérbole (exceto no infinito...). Em geral, há 2 interseções distintas, reais ou com-

plexas (e.g. $Y = -X$ corta f nos pontos $(i,-i)$, $(-i,i)$). As retas tangentes têm apenas um ponto de contato, que intuitivamente deve ser "contado 2 vezes".

Exercícios

1) Dados $f = X^2-2Y^2+XY-2X+5Y$, $g = X^2+XY+Y-X-2$, encontre polinômios a,b,c tais que $af+bg = c(X)$ como no Lema 1.

2) Seja $f = a_0Y^m+a_1Y^{m-1}+\ldots$, $a_0 \neq 0$, um polinômio a coeficientes em um domínio A. Mostre que, para todo $g \in A[Y]$, existe um inteiro $i \geq 0$ e polinômios $q,r \in A[Y]$ tais que

$$a_0^i g = qf + r, \quad \text{com} \quad r = 0 \quad \text{ou} \quad \partial r < m .$$

Deduza então um algorítmo para construir uma relação $af+bg = c$, onde $a,b \in A[Y]$, $c \in A$, e $c \neq 0$ desde que A seja fatorial e f,g não admitam fator comum não constante. Além disso, a,b podem ser tomados com $\partial a \leq \partial g-1$, $\partial b \leq \partial f-1$.

3) Prove que nenhum dos dois ramos do traço real da hipérbole $XY = 1$ é, em separado, o traço de uma curva algébrica. Mesma questão para a cúbica $Y^2 = X(X-1)(X+1)$. (Veja Fig. I.7).

4) Sejam $f,g \in k[X,Y]$ polinômios sem fator comum não constante. Prove que $k[X,Y]/(f,g)$ é um espaço vetorial de dimensão finita. (Sugestão: existem $r(X)$, $s(Y)$, não nulos, no ideal (f,g). O quociente $k[X,Y]/(r(X),s(Y))$ tem dimensão finita).

§2. A resultante

Como proceder, para achar os pontos de interseção de duas curvas f,g? O método geral mais simples é o de selecionar uma das variáveis, digamos X, para figurar como parte dos coeficientes. Isto é, consideramos f e g como polinômios na variável Y, a coeficientes no anel k[X]. Tentamos então encontrar os valores x de X para os quais f(x,Y) e g(x,Y) admitem raiz comum. Geometricamente, queremos encontrar as projeções, sobre o eixo dos x, dos pontos de $f \cap g$. Este processo, típico da chamada teoria da eliminação, repousa sobre o estudo da resultante de dois polinômios.

4. Definição. Seja A um anel (comutativo, e.g., A = k[X]), e sejam

$$f = a_d Y^d + \ldots + a_o \qquad (d \geq 1)$$

$$g = b_e Y^e + \ldots + b_o \ , \qquad (e \geq 1)$$

polinômios a coeficientes em A. A resultante de f,g é definida por

$$R = R_{f,g} = \begin{vmatrix} a_d & a_{d-1} & \cdots & a_o & & \\ & a_d & \cdots & a_1 & a_o & \\ & & \ddots & & \ddots & \ddots \\ & & & a_d & \cdots & a_o \\ b_e & \cdots & \cdots & b_o & & \\ & b_e & \cdots & b_1 & b_o & \\ & & \ddots & & \ddots & \ddots \\ & & & b_e & \cdots & b_o \end{vmatrix}$$

determinante da matriz $(d+e)\times(d+e)$, com e linhas de a's e d linhas de b's, subentendendo-se que os espaços em branco são preenchidos com zeros.

Nesta definição, os polinômios f,g são considerados <u>formalmente</u> de graus d, e, embora a_d, b_e possam ser nulos. O contexto deixará claro qual o grau formal atribuído; quando não explícito, convencionamos atribuir o grau efetivo, i.e., o maior grau em que Y ocorre efetivamente.

No caso em que estamos mais interessados, os coeficientes a_i, b_j são também polinômios em outras variáveis $X_1, X_2, \ldots$; escreveremos então $R(X_1, X_2, \ldots)$ para enfatizar que R é um polinômio nessas variáveis.

<u>Exemplo:</u> $f = Y^2+X^2-4$, $g = XY-1$.

$$R(X) = \begin{vmatrix} 1 & 0 & X^2-4 \\ X & -1 & 0 \\ 0 & X & -1 \end{vmatrix} = X^4 - 4X^2 + 1$$

Note que um processo "natural" para resolver o sistema

$$\begin{cases} X^2 + Y^2 = 4 \\ XY = 1 \end{cases}$$

seria substituir $Y = 1/X$ na 1ª equação, resultando a equação

$$X^4 - 4X^2 + 1 = 0$$

Ou seja, as interseções do círculo com a hipérbole têm para abscissas as soluções dessa última equação resultante. A coinci-

dência não é acidental.

5. Proposição. Sejam

$$f = a_d(X)\, Y^d + \ldots + a_o(X) ,$$

$$g = b_e(X)\, Y^e + \ldots + b_o(X) ,$$

onde a_i, b_j são polinômios nas variáveis $X_1, X_2, \ldots$. Então, para cada $x = (x_1, x_2, \ldots)$, temos

$R(x) = 0 \iff a(x) = b(x) = 0$ ou $f(x,Y)$, $g(x,Y)$ admitem raiz comum.

Demonstração. Para cada x, a resultante de $f(x,Y)$ e $g(x,Y)$ é obviamente $R(x)$. Por outro lado, $f(x,Y)$ e $g(x,Y)$ admitem uma raiz y em comum se e só se admitirem um fator não constante $Y-y$. Portanto, o teorema resultará do seguinte.

6. Lema. Sejam $f = a_d Y^d + \ldots + a_o$, $g = b_e Y^e + \ldots + b_o$ polinômios a coeficientes em um domínio de fatoração única A (e.g. $A = k$ ou $A = k[X]$). Então $R_{f,g} = 0$ se e só se $a_d = b_e = 0$ ou f,g admitem fator comum não constante.

Demonstração. Digamos $a_d \neq 0$. Então f,g admitem fator comum h não constante se e só se existirem $p,q \in A[Y]$ não ambos nulos, com $\partial p \leq d-1$ e $\partial q \leq e-1$ tais que

$$qf = pg . \tag{6.1}$$

Com efeito, se $f = ph$, $g = qh$, segue-se a relação (6.1). Re

ciprocamente, visto que $A[Y]$ também é fatorial, a relação (6.1) acarreta que algum fator irredutível de f ocorre em g, pois $\partial f > \partial p$.

Escrevendo

$$p = x_o Y^{d-1} + \ldots + x_{d-1} \quad ,$$

$$q = y_o Y^{e-1} + \ldots + y_{e-1} \quad ,$$

a equação (6.1) é equivalente ao sistema linear obtido comparando coeficientes, a saber,

$$\sum_{j=0}^{e-1} a_{d-i-j}\, y_j = \sum_{h=0}^{d-1} b_{e-i-h}\, x_h \quad , \qquad i = 0,\ldots,d+e-1 \quad ,$$

onde convencionamos por $a_m = b_n = 0$ se $m,n < 0$, ou $m > d$, $n > e$. Ora, este sistema admite solução não trivial se e só se é nulo o determinante da matriz dos coeficientes, o qual coincide com R a menos de sinal.

C.Q.D.

Retornando ao problema da interseção de duas curvas f,g, observemos que $R_{f,g}$ é identicamente nulo se e só se f,g admitirem componentes em comum, caso em que $f \cap g$ não é finita.

Quando a interseção é finita, podemos estimar o nº de pontos contando o número de abscissas, que é limitado pelo grau da resultante $R(X)$. Este procedimento é muito grosseiro, pois podem ocorrer vários pontos de interseção com a mesma abscissa.

Exemplo. Sejam $f = X^2+Y^2-2X$, $g = Y^2-X$.

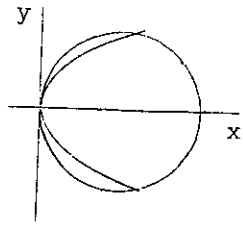


Fig. 9

A resultante é

$$R(X) = \begin{vmatrix} 1 & 0 & X^2-2X & \\ & 1 & 0 & X^2-2X \\ 1 & 0 & -X & \\ & 1 & 0 & -X \end{vmatrix} = X^2(X-1)^2 .$$

Neste exemplo, o mero cálculo da resultante não permite prever o número de interseções. A multiplicidade 2 da raiz $x = 0$ pode ser interpretada, na figura, como causada pela tangência. Já a raiz dupla $x = 1$ é devida ao fato de que há 2 pontos de interseção com a mesma abscissa. Se trocarmos X por Y, eliminando X, obtemos

$$R(Y) = \begin{vmatrix} 1 & -2 & Y^2 & \\ & -1 & Y^2 & \\ & & -1 & Y^2 \end{vmatrix} = Y^2(Y-1)(Y+1) .$$

Agora, os pontos de interseção aparecem fielmente refletidos nas raizes da resultante. A multiplicidade 2 da raiz $y = 0$ persiste, pois ela corresponde a um fenômeno geométrico, que diz respeito à posição das curvas f e g, e não depende do particular sistema de coordenadas empregado. Voltaremos a esta discussão no Capítulo V.

Exercícios

5) Resolva os sistemas:

a) $X(Y^2-X)^2 = Y^5$, $\quad X^4+Y^3 = X^2$.

b) $(X^2+Y^2)^2 = X^2-Y^2$, $\quad X^2+Y^2 = X-4$.

6) Calcule a resultante do par de polinômios

(a) $f(X) = aX^2+bX+c$, $\quad f'(X) = 2aX+b$.

(b) $f(X) = (X-a)(X-b)(X-c)$, $\quad g(X) = (X-d)(X-e)$,
$(a,b,\ldots,e$ constantes).

7) Construa pares de cônicas f_i, g_i irredutíveis tais que $f_i \cap g_i$ consiste de i pontos distintos para $i = 1,2,3,4$. Calcule as resultantes com relação a X e com relação a Y em cada caso.

8) Seja A um anel comutativo com unidade. Mostre que a resultante dos polinômios $f = Y-a$ e $g = b_nY^n +\ldots+ b_o \in A[Y]$ é $(-1)^n g(a)$.

9) Seja $\varphi: A \to B$ um homomorfismo de anéis e denotemos pelo mesmo símbolo o homomorfismo induzido $A[Y] \to B[Y]$ definido por $\varphi(\Sigma a_i Y^i) = \Sigma \varphi(a_i) Y^i$. Prove que $\varphi(R_{f,g}) = R_{\varphi(f),\varphi(g)}$ para todo $f,g \in A[Y]$.

§3. O grau da resultante

Para o cálculo do grau de $R(X)$, introduzimos o conceito de direção assintótica de uma curva f. Intuitivamente, é uma direção limite de retas OP, onde P percorre f afastando-se indefinidamente de O.

7. Definição. Escreva

$$f = f_o + f_1 + \ldots + f_d ,$$

onde cada f_i é homogêneo de grau i, e $f_d \neq 0$. Cada componente $aX+bY$ de f_d é dita uma direção assintótica de f.

Exemplos.

1) $f = 1-XY$ tem as direções assintóticas X e Y.

2) $f = Y^2-X$ tem a direção assintótica Y. (Note que aqui a direção assintótica não é uma assíntota, no sentido da Geometria Analítica).

Calculando a resultante de cada uma dessas curvas com uma reta $\ell = Y-(aX+b)$, o leitor verificará que o grau de $R_{f,\ell}$ é em geral 2, sendo menor somente se ℓ tem a mesma direção assintótica que f.

8. Proposição. O grau da resultante de duas curvas sem direção assintótica em comum é o produto dos graus. Em símbolos,

$$\partial R_{fg} = (\partial f)(\partial g) .$$

A resultante aqui é tomada atribuindo-se a f,g seus graus efetivos com respeito a Y.

Demonstração. Para cada polinômio $f = \sum_{o}^{d} f_i$, com f_i homogêneo de grau i, $f_d \neq 0$, ponhamos

$$f^*(X,Y,Z) = Z^d f_o + Z^{d-1} f_1 + \ldots + Z f_{d-1} + f_d ,$$

onde Z é uma nova variável (independente de X,Y). Observemos que f^* é um polinômio homogêneo de grau $d = \partial f$, e evidentemente $f^*(X,Y,1) = f(X,Y)$.

Reescrevamos f^*, g^* na forma

$$f^* = A_o Y^d + \ldots + A_d$$

$$g^* = B_o Y^e + \ldots + B_e ,$$

onde A_i, $B_j \in k[X,Z]$ são homogêneos e $\partial A_i = i$, $\partial B_j = j$. Calculemos a resultante

$$R(X,Z) = \begin{vmatrix} A_o \cdots\cdots A_d & & \\ & \ddots & \\ & A_o \cdots\cdots A_d & \\ B_o \cdots B_e & & \\ & \ddots & \\ & & B_o \cdots\cdots B_e \end{vmatrix} .$$

9. Lema. O polinômio $R(X,Z)$ acima definido é homogêneo de grau $d.e$, se não for identicamente nulo.

Demonstração. Em geral, se $p \neq 0$ é um polinômio nas n variáveis $X_1,\ldots,X_n$, então p é homogêneo de grau m se e só se

$$p(TX_1,\ldots,TX_n) = T^m p(X_1,\ldots,X_n) \quad \text{em} \quad k[X_1,\ldots,X_n,T],$$

onde T é uma nova variável independente. Com efeito, se p é homogêneo, é imediato que a relação vale. Reciprocamente, suponhamos válida, e escrevamos

$$p = p_o + p_1 + \ldots + p_r ,$$

soma de polinômio homogêneos com $\partial p_i = i$; $p_r \neq 0$. Abreviando $X = (X_1,\ldots,X_n)$, temos

$$p(TX) = p_o + Tp_1 + \ldots + T^r p_r = T^m p$$

donde, (pela definição de igualdade de polinômios!), $m = r$ e $p = p_m$.

Mostremos então que

$$R(TX,TZ) = T^{de} R(X,Z) \quad \text{em} \quad k[X,Z,T] .$$

Ora,

$$R(TX,TZ) = \begin{vmatrix} A_o & TA_1 & \ldots & T^d A_d & & \\ \vdots & & & & & \\ & A_o & \ldots & T^{d-1}A_{d-1} & A^d & A_d \\ & & & \vdots & & \\ B_o & TB_1 & \ldots & T^e B_e & \ldots & \end{vmatrix}$$

Multiplicando a 2ª linha por T, a 3ª por $T^2,\ldots,$a e-ésima por T^{e-1}, a 2ª linha de B's por $T,\ldots,$ a última por T^{d-1}, obtemos

$$T^N R(TX,TZ) = T^M R(X,Z) ,$$

onde

$$N = (1+\ldots+e-1) + (1+\ldots+d-1) , \qquad M = 1 + 2 +\ldots+ d+e-1.$$

Logo,

$$M-N = \frac{(d+e)(d+e-1)}{2} - \frac{e(e-1)}{2} - \frac{d(d-1)}{2} = de$$

C.Q.D.

Para completar a demonstração da Proposição 8 vamos comparar $R(X,Z)$ com $R(X)$. É evidente que $R(X,1)$ é a resultante de f,g considerados formalmente como polinômios em Y de graus d, e. Agora observemos que o coeficiente A_o (resp. B_o) de Y^d (resp. Y^e) em f^* (resp. g^*) é constante, sendo nulo se e só se Y^d (resp. Y^e) não ocorre em f_d (resp. g_e). Esta última condição é equivalente à condição de X ser fator de f_d. Como f,g não têm direções assintóticas em comum, segue-se que, por exemplo, $A_o \neq 0$. Seja j o menor índice tal que $B_j \neq 0$. Desenvolvendo o determinante que define $R(X,Z)$ pelas j primeiras colunas, obtemos

$$R(X,1) = A_o^j R(X).$$

Visto que f,g não têm direção assintótica em comum, em particular não têm componente em comum. Logo $R(X) \neq 0$ e portanto $R(X,Z) \neq 0$. Assim, o grau de $R(X,Z)$ é d.e. Segue-se que

$R(X,1)$ tem grau $d \cdot e$, a menos que $R(X,Z)$ seja múltiplo de Z. Mas neste último caso, $R(1,0) = 0$, acarretando

$$f^*(1,y,0) = g^*(1,y,0)$$

para algum y, donde $f_d(1,y) = g_e(1,y) = 0$ e f,g admitiriam ambos a direção assintótica $yX-Y$, proibido por hipótese.

C.Q.D.

Exercícios

10) Seja $f = f_o + f_1 + \ldots + f_d$, onde cada $f_i \in k[X,Y]$ é homogêneo de grau i e $f_d \neq 0$. Prove que $f(X,aX+b)$ tem grau exatamente igual a d se e só se a reta $Y = aX+b$ tem direção assintótica distinta das de f.

11) Sejam

$$f = a_o X^d + a_1 X^{d-1} Y + \ldots + a_d Y^d ,$$

$$g = b_o X^e + \ldots + b_e Y^e$$

polinômios homogêneos $\neq 0$ a coeficientes em k. Mostre que f,g admitem uma direção assintótica comum se e só se a resultante de $f(1,Y)$ e $g(1,Y)$ é nula.

12) Prove que o grau da resultante de duas curvas sem componente comum é sempre menor do que ou igual ao produto dos graus, com igualdade somente na situação da Proposição 8.

§4. O teorema dos zeros

Finalizamos este capítulo discutindo uma versão particular do célebre Nullstellensatz de Hilbert. Trata-se de elucidar em que condições um sistema de equações polinomiais admite solução.

Observemos inicialmente que, dado um sistema de equações,

$$f_1 = \ldots = f_N = 0,$$

toda solução é também solução de qualquer equação do tipo

$$g_1 f_1 + \ldots + g_N f_N = 0 ,$$

onde os g_i são polinômios arbitrários. Denotemos por $\mathfrak{I}$ o ideal gerado pelos $f_1,\ldots,f_N$, ou seja, o conjunto de todos os polinômios da forma $\Sigma\, g_j f_j$.

Dizemos que um ponto P é um <u>zero do ideal</u> $\mathfrak{I}$ se $f(P) = 0$ para todo $f \in \mathfrak{I}$. É evidente que o conjunto dos zeros de $\mathfrak{I}$ coincide com o conjunto das soluções do sistema proposto.

Por outro lado, se o polinômio constante 1 pertence a $\mathfrak{I}$, é claro que $\mathfrak{I}$ não admite zero. O Nullstellensatz afirma que, reciprocamente, se $\mathfrak{I}$ é um ideal próprio do anel dos polinômios a coeficientes num corpo algebricamente fechado, então $\mathfrak{I}$ admite um zero. Vamos nos ater ao caso de duas variáveis.

Lembremos que um ideal $\mathfrak{I} \subset k[X,Y]$ é próprio se e só se estiver contido em algum ideal maximal. Por exemplo, um ideal de $k[X,Y]$ da forma

$$\underline{m} = (X-x,\ Y-y) \quad ,$$

i.e., gerado por X-x, Y-y, onde x,y são constantes, é maximal, pois é o núcleo do epimorfismo "substituir X = x, Y = y",

$$k[X,Y] \longrightarrow k$$
$$f(X,Y) \longmapsto f(x,y) .$$

Agora observemos que, se $\mathfrak{J}$ estiver contido em (X-x, Y-y) então P = (x,y) é um zero de $\mathfrak{J}$, e reciprocamente. Este argumento mostra que o Nullstellensatz é consequência imediata do seguinte resultado.

10. Proposição. Se k é um corpo algebricamente fechado então todo ideal maximal $\mathfrak{m}$ de k[X,Y] é do tipo (X-x, Y-y) para algum $(x,y) \in k^2$.

(Observemos que é essencial aqui a hipótese de fechamento algébrico. O ideal (X^2+1,Y) de $\mathbb{R}[X,Y]$ é maximal e não admite zero real).

Demonstração. Seja $f \in \mathfrak{m}$ um polinômio não constante. (Leitor: justifique a existência de f). Podemos supor f irredutível porque "maximal ⇒ primo". Sendo k algebricamente fechado, não há dificuldade em se garantir a existência de um zero de f; digamos $f(x_o,y_o) = 0$. Se $\mathfrak{m} = (X-x_o, Y-y_o)$, ponto final. Se não, existe $g \in \mathfrak{m}$ tal que $g(x_o,y_o) \neq 0$. Em particular, f não divide g. Aplicando o Lema 1 obtemos uma relação af + bg = c, onde c é um polinômio não constante de uma só variável, seja X ou Y, à nossa escolha. Visto que $c \in \mathfrak{m}$, concluimos que $\mathfrak{m}$ contém elementos da forma X-x, Y-y. (Este é

outro ponto em que a hipótese sobre k é imprescindível). Tendo em conta que $(X-x, Y-y)$ é maximal, concluimos que $(X-x, Y-y)=\underline{m}$.

C.Q.D.

Exercícios

13) Seja f uma curva e seja $A = k[X,Y]/(f)$. Mostre que os ideais maximais de A estão em correspondência bijetiva natural com os pontos (x,y) tais que $f(x,y) = 0$, i.e., com os pontos do traço de f.

14) Seja S um subconjunto de k^2. Mostre que S é o conjunto das soluções de um sistema de equações polinomiais $f_1(X,Y) = f_2(X,Y) = \ldots = f_r(X,Y) = 0$ se e somente se $S = k^2$ ou $S = \phi$ ou S = união de um nº finito de curvas irredutíveis e de um conjunto finito de pontos.

15) Verifique se a demonstração da Proposição 10 se aplica para concluir um resultado análogo em mais de duas variáveis.

16) Caracterize os ideais maximais de $\mathbb{R}[X,Y]$.

CAPÍTULO III

MULTIPLICIDADES

§1. Interseção de uma curva com uma reta

Seja f uma curva, e seja ℓ uma reta de equação $Y = aX + b$. Os pontos de $f \cap \ell$ podem ser obtidos eliminando Y e resolvendo a equação

$$f_\ell(X) \overset{\text{def.}}{=} f(X, aX+b) = 0 .$$

Eis as possibilidades:

(1) $f_\ell(X)$ é identicamente nulo, caso em que ℓ é uma componente de f;

(2) $f_\ell(X)$ é uma constante $\neq 0$, quando $f \cap \ell = \phi$.

(3) $f_\ell(X)$ é um polinômio não constante, decompondo-se na forma

$$f_\ell(X) = c \prod_{i=1}^{r} (X-x_i)^{m_i},$$

onde c é uma constante e os x_i são as abscissas (2 a 2 distintas) dos pontos de interseção. Procede-se de maneira evidente quando ℓ é da forma $X = cY+d$.

1. Lema. Os inteiros m_i independem do referencial afim.

Demonstração. O processo de substituir $Y = aX+b$ em um polinômio $g(X,Y)$ define um epimorfismo

$$k[X,Y] \longrightarrow k[X]$$

$$g \longmapsto g(X,\ aX+b) \quad ,$$

cujo núcleo é o ideal (ℓ) gerado por $\ell = Y-(aX+b)$. Logo, obtemos um isomorfismo

$$k[X,Y]/(\ell) \xrightarrow{\sim} k[X]$$

tal que a classe $\overline{f}$ de f mod(ℓ) corresponde a f_ℓ. Visto que $k[X]$ é fatorial, à decomposição $\prod (X-x_i)^{m_i}$ de f_ℓ corresponde a (única!) decomposição de $\overline{f}$ em fatores irredutíveis, com o mesmo número r de fatores irredutíveis distintos, o i-ésimo repetido m_i vezes. Agora, se T é uma afinidade, T induz um isomorfismo

$$k[X,Y]/(\ell) \xrightarrow{\sim} k[X,Y]/(T.\ell)$$

tal que $f+(\ell)$ e $T.f + (T.\ell)$ se correspondem, juntamente com as decomposições em fatores irredutíveis.

C.Q.D.

2. Definição. A multiplicidade ou índice de interseção de ℓ, f no ponto P é dada por

$$(\ell,f)_P = \begin{cases} 0 & \text{se } P \notin \ell \cap f \\ \infty & \text{se } P \in \ell \subset f \\ m_i & \text{se } P = (x_i, ax_i+b) \text{ como no caso (3) acima.} \end{cases}$$

Se $\ell \not\subset f$, chamamos o inteiro

$$m_\infty = \partial f - \sum_{i=1}^{r} m_i$$

de multiplicidade de interseção de ℓ, f no ponto impróprio ou ponto no infinito de ℓ.

Deixamos a cargo do leitor a verificação de que m_∞ é positivo se e só se a direção de ℓ é assintótica de f.

O significado intuitivo dessas multiplicidades é que, arbitrariamente próximo à curva f, existem curvas do mesmo grau que cortam ℓ em ∂f pontos distintos, m_i dos quais estão próximos a (x_i, ax_i+b), os m_∞ restantes distanciando-se para ∞ sobre ℓ.

Exemplos.

1) $f = Y-X^2$, $\ell = Y-(aX+b)$. Se $a^2+4b \neq 0$, temos duas interseções distintas. Se $a^2+4b = 0$, temos uma só interseção, com multiplicidade 2.

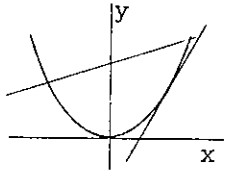


Fig. 10

2) $f = Y-X^3$, $\ell = aX+bY+c$. Se $b \neq 0 = a = c$, temos uma interseção na origem, com multiplicidade 3. Se $a \neq 0 = b$, temos uma interseção a distância finita, com multiplicidade 1, e outra no infinito, com multiplicidade 2. Se $b \neq 0$, podemos ter 1, 2 ou 3 pontos de interseção, todos a distância finita.

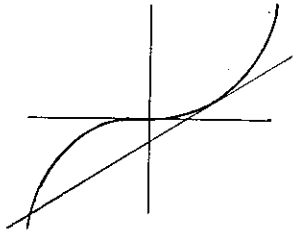


Fig. 11

3) $f = Y^2-X^2(X+1)$, $\ell_a = Y-aX$. A origem O absorve pelo menos 2 interseções. S a = ±1, a multiplicidade de interseção $(\ell,f)_O = 3$.

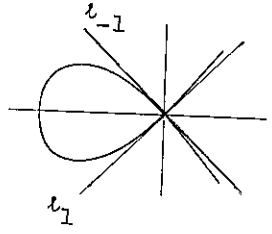


Fig. 12

§2. Pontos múltiplos

3. Proposição. Seja f uma curva e seja P um ponto de f.

Existe um inteiro $m = m_P(f) \geq 1$, tal que, para toda reta ℓ passando por P ,

$$(\ell,f)_P \geq m ,$$

ocorrendo a desigualdade estrita para no máximo m retas e no mínimo uma.

Demonstração. Suporemos, sem perda de generalidade, $P = O$. Escrevemos

$$f = f_m + \ldots + f_d \quad ,$$

com f_i homogêneo de grau i para $m \leq i \leq d$ e $f_m \neq 0$. Tendo em conta que $P \in f$, temos $m \geq 1$. Mudando coordenadas se necessário, podemos também supor que $X \nmid f_m$. O leitor verificará facilmente que $f(0,Y) = Y^m(f_m(0,1) + \ldots + f_d(0,1)\, Y^{d-m})$ e $f_m(0,1) \neq 0$, seguindo-se que $(X,f)_O = m$. Para as demais retas passando por O, ponhamos $\ell_t = Y - tX$. Temos então,

$$f(X,tX) = X^m(f_m(1,t) + f_{m+1}(1,t)X + \ldots + f_d(1,t)X^{d-m}).$$

Segue-se que

$$(\ell_t, f)_O \geq m \quad ,$$

ocorrendo igualdade se e só se $f_m(1,t) \neq 0$. Como $X \nmid f_m$, segue-se que $f_m(1,t)$ é um polinômio em t de grau $m(\geq 1)$ e que portanto se anula para ao menos 1 e no máximo m valores distintos.

C.Q.D.

4. Definição. O inteiro $m = m_p(f)$ descrito na proposição acima é a multiplicidade do ponto P na curva f ou multiplicidade de f em P. Se $P \notin f$, convencionamos $m_p(f) = 0$.

Se $P = (x,y) \in f$, escrevemos

$$f(X+x,\ Y+y) = f_m(X,Y) + \text{(termos de grau } \gneq m).$$

O polinômio homogêneo $f_m(X,Y)$ pode ser decomposto de ma-

neira única,

$$f_m = \prod (a_i X + b_i Y)^{e_i} ,$$

onde os fatores lineares $a_i X + b_i Y$ são retas distintas. As retas

$$\iota_i = a_i(X-x) + b_i(Y-y)$$

são as <u>retas tangentes</u> de f em P; o expoente e_i é a <u>multiplicidade da tangente</u> ι_i .

A demonstração da Proposição 3 mostra que $(\iota,f)_P > m = m_P(f)$ justamente para ι igual a uma das retas tangentes a f em P.

Dizemos que um ponto P de uma curva f é <u>liso</u> ou <u>não singular</u> ou <u>simples</u> em f e que f é <u>lisa</u>, etc. ... em P se $m_P(f) = 1$; <u>singular</u> caso contrário. A curva f é <u>lisa</u> ou <u>não singular</u> se $m_P(f) = 1$ para cada $P \in f$. Se $m_P(f) = 2,3,\ldots,m$, P é dito um ponto <u>duplo</u>, <u>triplo</u>,...,<u>m-uplo</u>. Um ponto m-uplo $P \in f$ é <u>ordinário</u> se f admitir m tangentes distintas no ponto P. Uma <u>cúspide</u> é um ponto duplo com tangentes coincidentes. Um <u>nó</u> é um ponto duplo ordinário.

5. <u>Proposição</u>. (1) Um ponto $P \in f$ é liso se e só se ao menos uma das derivadas parciais f_X, f_Y não se anula em P.

(2) Se $P = (a,b) \in f$ é liso então a (única!) tangente a f em P é dada por

$$f_X(P)(X-a) + f_Y(P)(Y-b) = 0$$

Demonstração. Ambas as afirmativas decorrem facilmente da fórmula de Taylor,

$$f(X+a,\ Y+b) = f(a,b) + f_X(a,b)X + f_Y(a,b)Y + g(X,Y) \quad ,$$

onde todos os termos de g têm grau ≥ 2.

C.Q.D.

Exemplos.

1) A lemniscata $(X^2+Y^2)^2 = X^2-Y^2$ apresenta um nó na origem, com tangentes $Y = \pm X$.

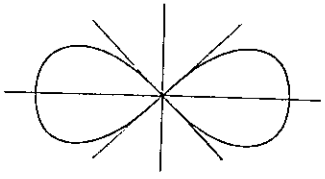


Fig. 13

2) A cissóide $X^2 - Y(Y^2+X^2) = 0$ tem uma cúspide na origem, com tangente vertical $X = 0$.

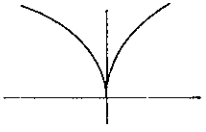


Fig. 14

3) Singularidade tacnodal: $Y^2-3X^2Y-Y^3+X^4 = 0$.

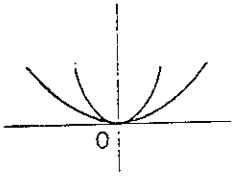


Fig. 15

4) Singularidade real isolada: $X^2+Y^2 = Y^3$

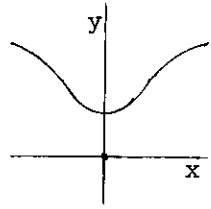


Fig. 16

5) Rosácea de 3 pétalas: $(X^2+Y^2)^2 = Y^3-3X^2Y$; a origem é um ponto triplo ordinário.

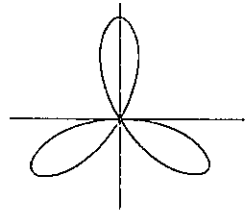


Fig. 17

6. Proposição. Se f é uma curva sem componentes múltiplas, então o conjunto dos pontos singulares de f é finito.

Demonstração. Lembremos que uma componente irredutível p de f é múltipla se $p^2|f$. Pela proposição anterior, o conjunto dos pontos singulares é dado pelas equações

$$f = f_X = f_Y = 0$$

Ora, ao menos uma das parciais, digamos f_X, é não identicamente nula. (Leitor: por que?). Afirmamos que $f = f_X = 0$ admite só

um número finito de soluções. Do contrário, pela Proposição (II.3), existiria componente irredutível p comum a f e f_X. Mas isto acarreta que $p^2 | f$, absurdo.

C.Q.D.

7. Proposição. Seja f uma curva sem componentes múltiplas. Então, para cada ponto P do plano, e para cada reta ℓ contendo P, com excessão de um número finito, ℓ intersecta f fora de P em $\partial f - m_p(f)$ pontos distintos.

(Intuitivamente, um ponto de multiplicidade m absorve m interseções de $\ell \cap f$, as demais sendo, em geral, distintas).

Demonstração. Suponhamos inicialmente f irredutível. Sem perda de generalidade, podemos supor P = (0,0). Ponhamos $m = m_P(f)$, $d = \partial f$ e lembremos a convenção $m = 0 \iff P \notin f$. Temos

$$f = f_m + \ldots + f_d ,$$

com f_i homogêneo de grau i para $m \leq i \leq d$ e $f_m f_d \neq 0$. Seja T uma nova indeterminada. Definamos

$$g(X,T) := X^{-m} f(X,TX) = f_m(1,T) + \ldots + X^{d-m} f_d(1,T).$$

O leitor verificará sem dificuldade que g(X,T) é irredutível em k[X,T]. Em particular, g_X e g não têm componente em comum. Logo, existe um número finito de valores t de T para os quais g(X,t) e $g_X(X,t)$ admitem raiz comum). (Essas são as raízes múltiplas de g(X,t). Evitando o número também finito de valores que anulam $f_m(1,T)\, f_d(1,T)$, concluímos que g(X,t) é um polinômio em X de grau d-m, com esse mesmo número de raízes dis-

tintas, e todas $\neq 0$. Tendo em conta que

$$f(X,tX) = X^m g(X,t) ,$$

concluímos que a reta $Y = tX$ intersecta f conforme anunciado.

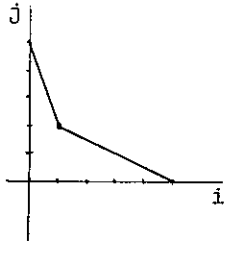
Para o caso geral (f possivelmente redutível), aplicamos a parte já demonstrada para cada componente.

C.Q.D.

§3. Diagrama de Newton

Finalizamos o capítulo descrevendo o diagrama de Newton, um método prático para esboçar o traço real de uma curva na vizinhança de um de seus pontos.

Para cada termo $a_{ij}X^iY^j$ efetivamente presente na equação da curva, marcamos o ponto (i,j) em um novo plano. Traçamos em seguida os segmentos ligando 2 ou mais desses pontos, com a propriedade de que a reta determinada isola os demais pontos no semiplano oposto ao da origem. Antes de prosseguirmos, tomemos por exemplo $X^5-5XY^2+2Y^5 = 0$ para fixar as idéias. A 1ª figura é o diagrama de Newton; a 2ª, um esboço do traço real de f, próximo à origem.



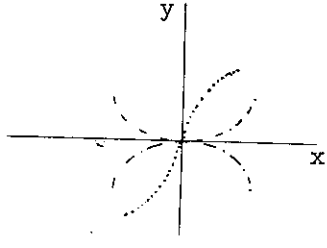


Fig. 18

Os termos correspondentes aos pontos (i,j) em um dado segmento, fatorando-se X ou Y, dão uma boa aproximação da curva próximo à origem.

No exemplo, o segmento que une (0,5) a (1,2) fornece $2Y^5-5XY^2$, do qual retemos $2Y^3-5X$. Esta é a parte do traço de f desenhada em pontilhado. O 2º segmento dá X^5-5XY^2, daí o par de parábolas $X^2 = \pm\sqrt{5}\ Y$ marcadas em traço-ponto.

Outro exemplo: $X^5-X^2Y^2+Y^5 = 0$.

Fig. 19

O 1º segmento dá $X^3 = Y^2$; o 2º dá $Y^3 = X^2$.

Sem entrar em maiores detalhes, o método funciona porque cada segmento do diagrama seleciona termos da equação que são infinitéssimos de mesma ordem, os demais pontos no semiplano oposto ao da origem representando termos de ordem superior [1] .

Exercícios

1) Analise as interseções de $X+Y = 2$ com $XY = 1+\varepsilon$ para $\varepsilon \to 0$.

1) Veja J. Dieudonné, "Calcul Infinitésimal", pag. 106.

2) Determine os pontos singulares com suas respectivas multiplicidades e retas tangentes e esboce as curvas:

a) $X^3-3XY^2+X^4+Y^4+2X^2Y^2 = 0$.

b) $Y^5-5YX^2+2X^5 = 0$

c) $Y^2X-X^2-Y^2+X = 0$

d) Reveja os exemplos e exercícios do Capítulo I.

3) Mostre que se uma cônica é singular, ela é redutível. Vale a recíproca?

4) Mostre que $m_p(f)$ é o menor inteiro m tal que alguma derivada parcial de f de ordem m é $\neq 0$.

5) Dizemos que um ponto P sobre uma curva f é um <u>ponto de inflexão</u> se P é não singular e $(\ell,f)_p \geq 3$. a) Cônicas irredutíveis não admitem pontos de inflexão; b) Escrevendo $f = f_1+f_2+\ldots$ com $f_i \in k[X,Y]$ homogêneo de grau i, mostre que $P = (0,0)$ é um ponto de inflexão se e só se f_1 é uma componente de f_2.

6) Determine os pontos de inflexão das curvas seguintes:

a) $Y = X^3$; b) $Y = YX^2 + X^3$; c) $X^3+Y^3+3XY = 0$; d) $X^3+Y^3+(X+Y+1)^3 + 3XY(X+Y+1) = 0$; e) $(X^2+Y^2)^2 = X^2-Y^2$.

7) Mostre que, se f é uma curva irredutível e $\partial f \geq 2$, então $m_p(f) \leq \partial f-1$ para todo P. Para cada $d \geq 2$, dê um exemplo de curva irredutível de grau d tendo a origem como ponto $(d-1)$-uplo ordinário, e sendo lisa nos demais pontos.

8) Mostre que uma curva redutível é singular em cada ponto de interseção de duas componentes. Dê um exemplo de curva

redutível não singular.

9) Prove que uma curva do tipo $Y^m = p(X)$, onde m é um inteiro ≥ 2 e $p(X)$ é um polinômio de uma variável, é não singular se e só se $p(X)$ não possui raízes múltiplas.

10) Mostre que a condição para que um dado ponto P seja m-uplo para uma curva f de grau $d \geq m$ se expressa por um sistema de $\binom{m+1}{2}$ equações lineares independentes, nos coeficientes de f.

11) Por 3 pontos arbitrários passa sempre uma cúbica que os contém com multiplicidade 2. Se existirem 2 tais cúbicas, então os 3 pontos são colineares e de fato existe uma infinidade.

12) Complete os detalhes da demonstração da Proposição 7 no caso em que f é redutível.

CAPÍTULO IV

PONTOS NO INFINITO

§1. O plano projetivo

As retas paralelas $aX+bY+c$, $aX+bY+c'$ $(c \neq c')$ não se intersectam a distância finita; a parábola $Y = X^2$ e a reta $X = 0$, bem como a hipérbole $XY = 1$ e os eixos coordenados são mais evidência de que essas interseções que estão "faltando", e até o presente vêm sendo tratadas como "direções assintóticas", devem ser melhor estudadas. O desejo de dar um tratamento rigoroso a esses "pontos que deviam estar lá" nos levará a introduzir de maneira sistemática os pontos no infinito. Esses "pontos" serão apresentados inicialmente como entes de natureza aparentemente diversa dos pontos usuais do plano afim. Mas logo veremos ser possível, e mesmo recomendável, eliminar as aspas; os novos pontos não merecerão no final nenhuma distinção especial com relação a seus parceiros atualmente dados a distância finita.

A idéia original de adjuntar ao plano usual uma reta no infinito, constituindo um plano projetivo, é devida a Desargues. Seu livro, publicado em 1639, pretendia dar uma fundamentação matemática aos métodos de perspectiva empregados pelos pintores e arquitetos. A concepção de Desargues do plano projetivo é, em essência, a que vamos descrever.

Consideremos o plano afim mergulhado no espaço tridimensional como o plano $\prod$ de equação $Z = 1$.

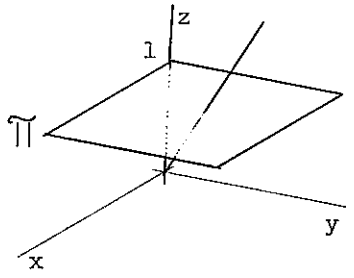


Fig. 20

Cada ponto do plano $\prod$ determina uma reta passando pela origem e pelo dado ponto. Cada reta de $\prod$ determina um plano pela origem. Se as retas $\ell, \ell' \subset \prod$ se intersectam, seu ponto de interseção dá lugar à reta de interseção dos dois planos associados a ℓ, ℓ'. Se as retas ℓ, ℓ' são paralelas, os planos que elas definem ainda se intersectam, desta feita ao longo de uma reta passando pela origem e contida no plano $Z = 0$.

1. Definição. O plano projetivo $\mathbb{P}^2$ é o conjunto das retas do espaço tridimensional passando pela origem.

Do exposto acima, vemos que o plano afim $\prod$ se identifica naturalmente com um subconjunto de $\mathbb{P}^2$ que ainda denotaremos por $\prod$. Os pontos de $\mathbb{P}^2 - \prod$ são chamados de pontos no infinito.

Denotamos por $(x:y:z)$ o ponto de $\mathbb{P}^2$ que representa a reta ligando a origem 0 a um ponto $(x,y,z) \neq 0$. Dizemos que x,y,z são coordenadas homogêneas do ponto $(x:y:z)$ relativas à base canônica $\{(1,0,0), (0,1,0), (0,0,1)\}$.

Por definição, temos que

$$(x:y:z) = (x':y':z') \Leftrightarrow$$

existe constante $t \neq 0$ tal que $(x,y,z) = t(x',y',z')$.

Em geral, fixada uma base qualquer no espaço tridimensional, as coordenadas de um ponto $\neq 0$ relativas a essa base são chamadas de coordenadas homogêneas do ponto correspondente de $\mathbb{P}^2$. Coordenadas homogêneas de um ponto de $\mathbb{P}^2$ (relativas a uma base prefixada) só estão bem definidas a menos de um fator escalar $\neq 0$.

Vamos nos servir da aplicação,

$$q: \mathbb{R}^3 - \{0\} \longrightarrow \mathbb{P}^2$$
$$(x,y,z) \longmapsto (x:y:z)$$

para introduzir uma topologia em $\mathbb{R}^2$, a topologia quociente. Dizemos que um subconjunto $U \subset \mathbb{P}^2$ é aberto se $q^{-1}(U)$ é aberto em $\mathbb{R}^3 - \{0\}$ com sua topologia usual.

Intuitivamente, isso estabelece em $\mathbb{P}^2$ uma noção de vizinhança, segundo a qual dois pontos de $\mathbb{P}^2$ estão "próximos" se as retas associadas em $\mathbb{R}^3$ formam um ângulo "pequeno".

O subconjunto de $\mathbb{P}^2$,

$$\mathbb{A}^2 = \{(x:y:z) | z \neq 0\},$$

é aberto e denso em $\mathbb{P}^2$, pois $q^{-1}(\mathbb{A}^2)$ é o complementar do plano $z = 0$ em $\mathbb{R}^3$ e é evidentemente aberto e denso em $\mathbb{R}^3-\{0\}$. Pode-se mostrar que a aplicação

$$\mathbb{R}^2 \longrightarrow \mathbb{A}^2 \subset \mathbb{P}^2$$
$$(x,y) \longmapsto (x:y:1)$$

é uma bijeção contínua, com inversa também contínua. Desta maneira, passamos a considerar o plano afim $\mathbb{R}^2$ como contido em $\mathbb{P}^2$, identificando-o com $\mathbb{A}^2$.

§2. Espaços projetivos

Considerações análogas se aplicam, mais geralmente, para a definição do espaço projetivo associado a um espaço vetorial V de dimensão arbitrária sobre um corpo k.

3. Definição. O espaço projetivo $\mathbb{P}(V)$ associado a um espaço vetorial V é o conjunto dos subespaços de V de dimensão 1. Se $V = k^{n+1}$, escrevemos $\mathbb{P}^n_k = \mathbb{P}(V)$, ou simplesmente $\mathbb{P}^n$.

As coordenadas homogêneas de um ponto $P \in \mathbb{P}(V)$ relativas a uma base $\{v_0,\dots,v_n\}$ de V são as coordenadas $(x_0,\dots,x_n)$ de um vetor não nulo arbitrário $\Sigma x_i v_i$ pertencente ao subespaço representado por P. Fixada a base, escrevemos $P = (x_0:\dots:x_n)$ para indicar um ponto com essas coordenadas homogêneas.

Para cada $i=0,\dots,n$, , o subconjunto de $\mathbb{P}^n$

$$U_i = \{(x_0:\dots:x_n) \mid x_i \neq 0\} \ ,$$

pode ser identificado com k^n através da bijeção

$$(x_0:\dots:x_n) \longleftrightarrow \left(\frac{x_0}{x_i},\dots,\frac{x_n}{x_i}\right) \quad (\text{omitir } \frac{x_i}{x_i}) \ .$$

Convencionamos escrever $\mathbb{A}^n = U_n$; salvo menção em contrário, identificamos k^n com $\mathbb{A}^n \subset \mathbb{P}^n$.

O complementar de $\mathbb{A}^n$ em $\mathbb{P}^n$ consiste de pontos da forma

$(x_o:\ldots:x_{n-1}:0)$. Desta maneira, $\mathbb{P}^n - \mathbb{A}^n$ identifica-se a um $\mathbb{P}^{n-1}$, que convencionamos chamar hiperplano no infinito. (Veja também o exercício 9,b)).

Em particular, $\mathbb{P}^o$ consiste de um só ponto.

$\mathbb{P}^1$, a reta projetiva, é a reta usual $\mathbb{A}^1$ com um ponto extra no infinito.

Quando $k = \mathbb{R}$, podemos visualizar $\mathbb{P}^1_{\mathbb{R}}$ como a circunferência, com o ponto no infinito indicado na figura:

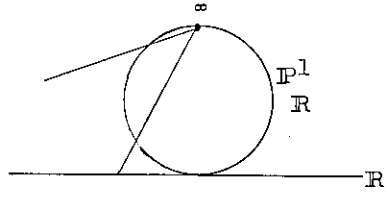


Fig. 21

A reta projetiva complexa pode ser identificada com a esfera, via projeção estereográfica. Mas esta interpretação será ignorada aqui. Preferimos encarar $\mathbb{P}^1_{\mathbb{C}}$ como um objeto uni-dimensional.

§3. Curvas projetivas

Passemos a investigar como se situam as curvas planas afins nesse ambiente mais amplo. Comecemos com as retas.

Para o resultado seguinte, suporemos $k = \mathbb{R}$ (ou $\mathbb{C}$).

4. Proposição - Seja ℓ: $aX + bY + c = 0$ (com a ou $b \neq 0$), e seja $\overline{\ell}$ a aderência de ℓ em $\mathbb{P}^2$. Então temos

$$\overline{\ell} = \ell \cup \{(b:-a:0)\} = \{(x:y:z) \mid ax+by+cz = 0\} .$$

Demonstração. Denotemos por ℓ^* o 2º membro da última igualdade proposta. É imediato que $\ell^* = \ell \cup \{(b:-a:0)\}$. Mostremos que $\overline{\ell} = \ell^*$. Por definição da topologia de $\mathbb{P}^2$, resulta ℓ^* fechado em $\mathbb{P}^2$. Visto que $\ell \subset \ell^*$, segue-se $\overline{\ell} \subset \ell^*$. Resta mostrar que o ponto no infinito $P = (b:-a:0)$ pertence a $\overline{\ell}$. Para isso, basta exibirmos uma sequência de pontos $P_n \in \ell$ com $\lim_{n\to\infty} P_n = P$. Suponhamos, por exemplo, $b \neq 0$. Seja

$$P_n = (bn: -an-c: b) .$$

Temos

$$P_n = (n: (-an-c)/b:1)$$

$$= (b: -a - \frac{c}{n}: \frac{b}{n}) .$$

A 1ª igualdade mostra que $P_n \in \ell$; a 2ª mostra que $P_n \to P$, pois $(b, -a - \frac{c}{n}, \frac{b}{n})$ tende a $(b, -a, 0)$ em $\mathbb{R}^3 - \{0\}$ e $q: \mathbb{R}^3 - \{0\} \to \mathbb{P}^2$ é contínua. C.Q.D.

5. Definição. Seja $f = \sum_0^d f_i$, onde cada $f_i \in k[X,Y]$ é homogêneo de grau i, $f_d \neq 0$. A homogeneização de f é o polinômio homogêneo de grau $d = \partial f$,

$$f^*(X,Y,Z) = \Sigma Z^{d-i} f_i(X,Y)$$

Deixamos a cargo do leitor a verificação de que o resultado anterior se generaliza para uma curva f arbitrária: o subconjunto de $\mathbb{P}^2$,

$$\{(x:y:z) \mid f^*(x,y,z) = 0\}$$

é igual à aderência de f em $\mathbb{P}^2$. Não faremos mais uso deste fato, nem de outras propriedades topológicas de $\mathbb{P}^2$. Incluimos essa discussão apenas para motivar a definição seguinte.

6. Definição. Uma curva plana projetiva é uma classe de equivalência de polinômios homogêneos não constantes, $F \in k[X,Y,Z]$, módulo a relação que identifica dois tais polinômios, F, G, se um for múltiplo constante do outro.

Adotaremos, mutatis mutandis, as definições e convenções feitas no Capítulo I para o caso afim. Deixamos a cargo do leitor a transcrição das definições de traço, equação, componente irredutível e grau dadas em (I.4).

Observemos que, se F é um polinômio homogêneo, a relação

$$F(tx,ty,tz) = t^{\partial F}F(x,y,z)$$

mostra que a condição para que um ponto (x:y:z) pertença ao traço de uma curva projetiva é independente das coordenadas homogêneas.

Curvas de grau 1,2,3,... são, como antes, chamadas retas, cônicas, cúbicas, etc.

A reta $Z = 0$ é usualmente chamada de reta no infinito, mas a escolha é meramente psicológica. Mudando a base de k^3, podemos decretar que qualquer reta de $\mathbb{P}^2$ previamente estipulada seja a reta no infinito. Seu complementar $(Z \neq 0)$, é o plano $\mathbb{A}^2$, cujos pontos são ditos estarem a distância finita.

O fecho projetivo de uma curva afim f é a curva projetiva definida pela homogeneização f^*.

Os pontos a distância finita sobre uma curva F são dados pela equação $F(X,Y,1) = 0$. O polinômio no primeiro membro desta equação é a desomogeneização de F com respeito a Z, denotado F_*. Note que F_* é não constante, a menos que F seja igual a uma potência de Z. (Equivalentemente: o traço de F coincide com a reta no infinito). Observaremos a seguinte

Convenção. Doravante, as curvas algébricas planas afins $f(X,Y) = 0$ serão consideradas implicitamente como a parte que se acha a distância finita sobre a curva projetiva $f^*(X,Y,Z) = 0$. Assim, quando nos referirmos, por exemplo, à parábola $Y = X^2$, estaremos automaticamente pensando em $ZY = X^2$. O termo curva significará curva plana projetiva, salvo menção em contrário.

§4. Mudança projetiva de coordenadas

7. Definição (Compare com (I.7) Seja $T: k^3 \to k^3$ um isomorfismo linear. Visto que uma tal aplicação preserva retas de k^3 passando pela origem, temos definida uma bijeção natural, ainda designada por $T: \mathbb{P}^2 \to \mathbb{P}^2$, chamada uma projetividade ou mudança projetiva de coordenadas em $\mathbb{P}^2$. Mais geralmente, define-se de maneira análoga projetividade em um espaço projetivo $\mathbb{P}(V)$ arbitrário.

Temos também induzido um k-isomorfismo

$$T_*: k[X,Y,Z] \to k[X,Y,Z]$$

tal que, para todo $(x,y,z) \in k^3$ e todo polinômio f,

$$(T_*f)(x,y,z) = f(T^{-1}(x,y,z)).$$

Mais explicitamente, escrevendo $X = X_1$, $Y = X_2$, $Z = X_3$ e designando por (a_{ij}) a matriz de T^{-1} relativa à base canônica de k^3 , temos

$$(T.f)(X_1,X_2,X_3) = f(\Sigma a_{1j}X_j,\ \Sigma a_{2j}X_j,\ \Sigma a_{3j}X_j) \ .$$

A <u>imagem de uma curva projetiva</u> F por uma projetividade T é a curva definida por T.F. As curvas F e T.F são ditas <u>congruentes</u>.

Dizemos que uma propriedade $\mathcal{P}$ relativa a curvas F é <u>invariante ou independente das coordenadas</u> se F satisfaz $\mathcal{P}$ somente se T.F a satisfaz para toda projetividade T. Definição análoga se aplica a propriedades relativas a outras configurações. (Comparar com I.10)).

São exemplos de propriedades invariantes o grau de uma curva projetiva, a colinearidade de pontos, a redutibilidade de uma curva, e várias outras que veremos no decorrer do curso.

8. <u>Proposição</u>. <u>Sejam</u> $\{L_1,L_2,L_3\}$, $\{H_1,H_2,H_3\}$ <u>conjuntos de 3 retas de</u> $\mathbb{P}^2$ <u>não concorrentes</u> (i.e. $\cap L_i = \cap H_j = \emptyset$). <u>Existe uma projetividade</u> T <u>tal que</u> $T.L_i = H_i$ <u>para</u> $i = 1,2,3$.

<u>Demonstração</u>. Cada reta de $\mathbb{P}^2$ corresponde a um plano de k^3 passando pela origem, denotado a seguir pelo mesmo símbolo. Seja u_i (resp. v_i) um vetor não nulo na interseção dos planos L_j, L_k (resp. H_j,H_k) para $\{i,j,k\} = \{1,2,3\}$. Então os u_i (resp. v_i), $i = 1,2,3$ formam uma base de k^3. Assim, existe um isomorfismo linear T definido pela condição $T\,u_i = v_i$, $i = 1,2,3$. Visto que u_i, u_j geram L_k , temos efetivamente

$T.L_i = H_i$. C.Q.D.

Exemplos:

1) Duas retas em $\mathbb{P}^2$ sempre se intersectam porque dois planos passando pela origem em k^3 sempre contêm uma reta em comum. Em particular, as retas afins $aX+bY+c = 0$, $aX+bY+c' = 0$ se intersectam no infinito.

2) A parábola $Y^2 = X$ intersecta $Y = 0$ nos 2 pontos $(0:0:1)$ e $(1:0:0)$.

3) A hipérbole $XY = 1$ intersecta $X = 0$ no ponto $(0:1:0)$. Este se encontra no complementar da reta $Y = 0$. Tomando-a como a nova reta no infinito, desomogeneizando $XY-Z^2$ com relação a Y, obtemos a parábola $X = Z^2$ (que é tangente a $X = 0$).

4) A elipse $\frac{X^2}{a^2} + \frac{Y^2}{b^2} = 1$ é a parte da cônica $\frac{X^2}{a^2} + \frac{Y^2}{b^2} = Z^2$ a distância finita. Escolhendo a reta $X = 0$ como a reta no infinito, obtemos agora, a distância finita, a hipérbole $Z^2 - \frac{Y^2}{b^2} = \frac{1}{a^2}$.

Tente imaginar os 2 ramos de uma hipérbole se encontrando no ∞. Talvez você se convença de que a hipérbole e a elipse são de fato 2 aspectos da mesma curva:

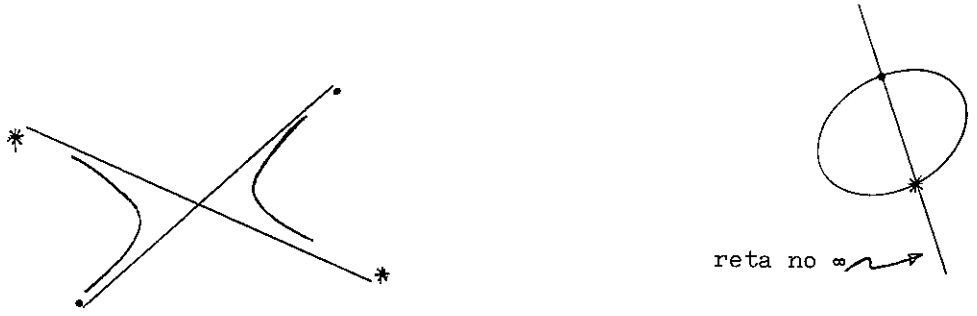


Fig. 22

É por vezes conveniente fazer uma representação gráfica de $\mathbb{P}^2$ desenhando o chamado triângulo de referência formado pelas retas $X = 0$, $Y = 0$ e $Z = 0$ (esta última tomada no ∞):

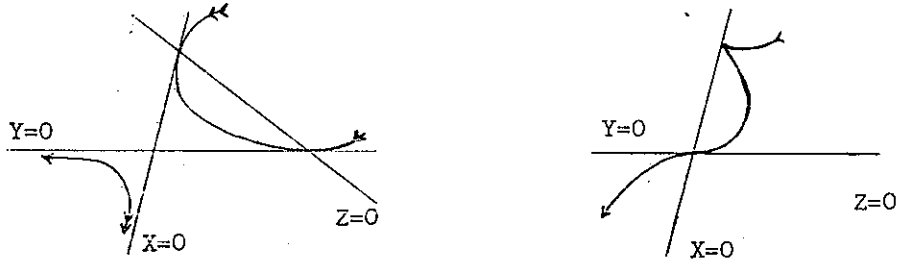


Fig. 23

A primeira figura mostra o ramo positivo da hipérbole $XY = 1$ efetivamente tangenciando os eixos $X = 0$ e $Y = 0$ no infinito, e se prolongando com o ramo negativo.

Na segunda, temos a parábola cúbica $Y = X^3$ exibindo seu ponto cuspidal (ou de reviravolta) no ∞.

Exercícios

1) Construa uma sequência de pontos P_n a distância finita sobre a hipérbole $XY = 1$ tal que $\lim_{n\to\infty} P_n = (0:1:0)$.

2) Mostre que todo ponto de $\mathbb{P}^2 - \mathbb{A}^2$ é aderente a alguma reta afim.

3) Mostre que as direções assintóticas de uma curva afim f estão em correspondência com as interseções de f^* com a reta no infinito $Z = 0$.

4) Prove que f^* é a aderência da curva afim $f \subset \mathbb{A}^2$.

5) Demonstre as fórmulas: a) $(fg)^* = f^* g^*$; b) $(FG)_* = F_* G_*$; c) $(f^*)_* = f$; d) $Z^n (F_*)^* = F$, onde $n = \partial F - \partial F_*$.

6) Prove que um produto de polinômios é homogêneo se e só se cada fator é um polinômio homogêneo. (Este fato foi implicitamente suposto na definição de componente de uma curva plana projetiva).

7) Mostre que uma curva afim f é irredutível se e só se f^* é uma curva projetiva irredutível.

8) Seja F uma curva projetiva irredutível e seja G uma curva projetiva. Mostre que se $F \subset G$ então $F \mid G$.

9) Sejam $P_i = (a_{i1}: a_{i2}: a_{i3}) \in \mathbb{P}^2$, $i = 1,2,3$. Prove que eles são colineares se e só se $\det(a_{ij}) = 0$.

10) Seja V um espaço vetorial. a) Para cada subespaço vetorial $W \subset V$, mostre que $\mathbb{P}(W) \subset \mathbb{P}(V)$; se W' é outro subespaço de V, mostre que $\mathbb{P}(W')=\mathbb{P}(W) \Longleftrightarrow W=W'$. $\mathbb{P}(W)$ é dito um subespaço projetivo de $\mathbb{P}(V)$. b) Suponha $\dim W = \dim V-1$ e seja v_o um ponto de V fora de W. Para cada $v \in V$, seja $[v]$ o subespaço gerado. Mostre que a aplicação $w \longmapsto [w+v_o]$ é uma bijeção de W em $\mathbb{P}(V) - \mathbb{P}(W)$. c) Definimos a dimensão (resp. codimenção) de $\mathbb{P}(W)$ por $\dim \mathbb{P}(W) = \dim W-1$ (rep. $\operatorname{codim} \mathbb{P}(W) = \dim V - \dim W$). Mostre que $\dim \mathbb{P}(W) \geq 0 \Longleftrightarrow \mathbb{P}(W) \neq \phi$. d) Mostre que uma interseção de subespaços projetivos é um subespaço projetivo. e) Mostre que se S_1, S_2 são subespaços projetivos então

$$\operatorname{codim} (S_1 \cap S_2) \leq \operatorname{codim} S_1 + \operatorname{codim} S_2 .$$

f) Uma reta (resp. hiperplano) em $\mathbb{P}(V)$ é um subespaço de dim (resp. codim.) 1. Mostre que toda reta intersecta qualquer hiperplano de $\mathbb{P}(V)$.

11) Seja V_d o espaço vetorial dos polinômios homogêneos $F(X,Y,Z)$ de grau d. a) Mostre que o conjunto das curvas de grau d identifica-se naturalmente com $\mathbb{P}(V_d)$. b) Calcule $\dim \mathbb{P}(V_d)$. c) Mostre que as curvas de grau d que passam por um ponto fixo formam um hiperplano em $\mathbb{P}(V_d)$. c) Mostre que o conjunto das retas de $\mathbb{P}^2$ que passam por um ponto P é uma reta de $\mathbb{P}(V_1)$ (dita a dual do ponto P). d) A reta de $\mathbb{P}^2$ determinada por 2 pontos distintos é representada em $\mathbb{P}(V_1)$ pelo ponto de interseção das 2 retas duais; 3 pontos de $\mathbb{P}^2$ são colineares se e

só se suas retas duais são concorrentes.

12) Sejam $P_1,\ldots,P_5 \in \mathbb{P}^2$ 5 pontos distintos. Seja S_i o conjunto das cônicas que passam por $P_1,\ldots,P_i$. a) Mostre que S_i é um subespaço projetivo de $\mathbb{P}(V_2)$ e que codim $S_i = i$ para $i = 1,2$ ou 3. b) Mostre que dim $S_4 = 1$ se e só se $P_1,\ldots,P_4$ não são colineares. Neste caso, conclua que existem cônicas F_1, F_2 tais que, a condição necessária e suficiente para que uma cônica F contenha $P_1,\ldots,P_4$ é que F seja da forma $x_1F_1+x_2F_2$ para algum $(x_1:x_2) \in \mathbb{P}^1$. c) Investigue sob quais condições os 5 pontos determinam uma única cônica.

13) Prove que o grupo das afinidades de $\mathbb{A}^2$ é isomorfo ao grupo das projetividades de $\mathbb{P}^2$ que deixam a reta no infinito invariante.

14) Dados dois conjuntos $\{P_i\}$, $\{Q_i\}$ de 4 pontos de $\mathbb{P}^2$, 3 a 3 não colineares, mostre que existe uma única projetividade T tal que $TP_i = Q_i$, $i = 1,\ldots,4$. Generalize para $\mathbb{P}^n$.

15) Prove que dois isomorfismos lineares que induzem a mesma projetividade são múltiplo escalar um do outro.

16) Associe a cada cônica,

$$F = a_{11}X^2 + a_{22}Y^2 + a_{33}Z^2 + 2(a_{12}XY + a_{13}XZ + a_{23}YZ),$$

a matriz simétrica $S_F = (a_{ij})$. a) Mostre que

$$F(X,Y,Z) = (X,Y,Z)\, S_F\, {}^t(X,Y,Z).$$

b) Seja $M = (m_{ij})$ uma matriz inversível 3×3 e denotemos pela mesma letra a projetividade associada $(M(x_1:x_2:x_3) = (\Sigma m_{1j}x_j:\Sigma m_{2j}x_j:\Sigma m_{3j}x_j))$. Prove que

$$S_{M.F} = {}^tM^{-1}\, S_F\, M^{-1}$$

c) Mostre que toda cônica é congruente por uma projetividade a exatamente uma das seguintes: $XY = Z^2$, $XY = 0$, $X^2 = 0$. Em particular, do ponto de vista complexo-projetivo, a parábola, a hipérbole e a elipse são congruentes; elas diferem pela posição relativa à reta no infinito.

17) Mostre que a cissóide $X^2 = Y(Y^2+X^2)$ é congruente à cúbica cuspidal $Y^2 = X^3$ (Homogeneizar primeiro). A trissectriz de MacLaurin e o folium de Descartes também são congruentes entre si.

18) Prove que se uma cônica tem 3 pontos colineares ela é redutível.

CAPÍTULO V

INTERSEÇÃO DE CURVAS PROJETIVAS

A motivação originalmente presente na criação do plano projetivo foi o desejo de abolir o paralelismo de retas: em $\mathbb{P}^2$, 2 retas sempre se intersectam. Mas na realidade $\mathbb{P}^2$ é muito mais prodigioso. Veremos que 2 curvas projetivas planas quaisquer sempre se intersectam. Melhor ainda: é possível atribuir, a priori, multiplicidades de interseção de maneira que, o número total de pontos comuns às duas curvas, contados com multiplicidade, seja ou igual ao produto dos graus dessas curvas, ou infinito, este último caso ocorrendo somente se houver componente comum. Este é o enunciado do teorema de Bezout.

§1. Interseção de reta e curva, agora projetivas

Seja L uma reta e seja F uma curva de grau d.

Suponhamos inicialmente $L = X$. Temos então:

$$P = (0:y:z) \in X \cap F \iff F(0,y,z) = 0 .$$

Ora, o polinômio $F(0,Y,Z)$ ou bem é identicamente nulo (caso em que $X \subset F$) ou é homogêneo de grau d, decompondo-se na forma

$$F(0,Y,Z) = \prod (z_i Y - y_i Z)^{m_i} ,$$

onde os pontos $P_i = (0:y_i:z_i)$ são 2 a 2 distintos e constituem $X \cap F$. Chamamos naturalmente o expoente m_i de multiplicidade

de interseção de X,F em P_i. Deixamos a cargo do leitor a verificação de que essas multiplicidades coincidem com as definidas anteriormente (quando comparáveis). Em especial, se $(0:1:0) \in X \cap F$, a multiplicidade aqui definida coincide com aquela no então chamado ponto impróprio da reta.

1. Proposição. Seja L uma reta e seja F uma curva de grau d. Se $L \not\subset F$ então $L \cap F = \{P_1,\dots,P_r\}$, onde $P_i \neq P_j$ para $i \neq j$ e existem inteiros $m_i \geq 1$ bem determinados pela seguinte condição: se T é uma projetividade tal que $T_*L = X$, então

$$(T_*F)(0,Y,Z) = \prod_1^r (z_iY-y_iZ)^{m_i} ,$$

onde $TP_i = (0:y_i:z_i)$ para $i = 1,\dots,r$. Em particular, $\Sigma m_i = d$.

Demonstração. Consideremos o diagrama de homomorfismos de anéis,

$$\begin{array}{ccc} k[X,Y,Z] & \xrightarrow{T_*} & k[X,Y,Z] \\ \downarrow & & \downarrow \\ k[X,Y,Z]/(L) & \xrightarrow{\overline{T}_*} & k[Y,Z] \end{array}$$

A 1ª das flexas verticais é a aplicação quociente $g \longmapsto \overline{g} = g+(L)$; a 2ª é $g(X,Y,Z) \longmapsto g(0,Y,Z)$, e $\overline{T}_*$ é o isomorfismo induzido por T_*. Segue-se que $k[X,Y,Z]/(L)$ é isomorfo ao domínio fatorial $k[Y,Z]$. Portanto, $\overline{F}$ admite fatorização única,

$$\overline{F} = p_1^{n_1} \dots p_s^{n_s} ,$$

onde os p_i são irredutíveis distintos e os expoentes n_i são ≥ 1. Levando em conta que $\overline{T}_*(\overline{F}) = (T_*F)(0,Y,Z)$ e comparando as decomposições, concluimos que $r = s$ e $n_i = m_i$ a menos de reor-

denação. Finalmente, a afirmativa com relação aos TP_i é evidente.

C.Q.D.

2. Definição. A multiplicidade ou índice de interseção da reta L com uma curva F no ponto P é definido por

$$(L,F)_P = \begin{cases} \infty & \text{se } P \in L \subset F \\ 0 & \text{se } P \notin L \cap F \\ m_i & \text{se } P = P_i \end{cases}$$ nas condições da Prop. anterior.

A proposição acima pode ser reenunciada, dizendo que $L \cap F$ consiste de ∂F pontos contados com multiplicidade; é um caso particular do Teorema de Bezout. O caso geral será visto mais adiante.

A mesma proposição revela que, com o emprego de uma projetividade conveniente, podemos sempre supor, para o cálculo de $(L,F)_P$, que P se encontra a distância finita e que L,F são distintos da reta no ∞. Nestas circunstâncias, é imediato que

$$(L,F)_P = (L_*,F_*)_P ,$$

onde o 2º membro é a multiplicidade de interseção definida no caso afim.

Assim, os resultados do Capítulo III podem ser transcritos para as curvas projetivas. Em especial, temos a seguinte

3. Proposição. Seja F uma curva projetiva e seja P um ponto de F. Existe um inteiro $m = m_P(F) \geq 1$ tal que, para toda reta L passando por P,

$$(L,F)_P \geq m$$

ocorrendo desigualdade estrita para no máximo m retas e no mínimo uma.

Demonstração. Movendo F e P com uma projetividade, podemos supor que a reta no infinito não contém P. Assim, reduzimos ao caso afim, quando então a proposição é conseqüência de (III.3).

C.Q.D.

4. Definição. (Comparar com (III.4) O inteiro $m_P(F)$ descrito acima é a multiplicidade de F (resp. P) em P (resp. F). Se $P \notin F$, convencionamos $m_P(F) = 0$. Dizemos que P (resp. F) é simples ou não singular ou liso (a) em F (resp. P) se $m_P(F) = 1$; múltiplo ou singular se $m_P(F) \geq 2$. F é lisa ou não singular se o for em cada um de seus pontos. Se $m_P(F) = 2,3,\ldots,m$ P é dito um ponto duplo, triplo,...,m-uplo. As retas tangentes a F em P são as retas excepcionais destacadas na proposição anterior.

Se f é uma curva afim e $F = f^*$, é imediato que $m_P(F) = m_P(f)$ para cada ponto $P \in \mathbb{A}^2$. Portanto, as definições dadas acima são consistentes com as dadas no Capítulo III.

Para a determinação de $m_P(f)$ e das retas tangentes, reduzimos ao caso afim, desomogeneizando F com relação a uma variável que não se anula em P.

Exemplo. A parábola cúbica $Y = X^3$ é singular no infinito, no ponto $P = (0:1:0)$. Desomogeneizando F: $Z^2Y = X^3$ com

relação a Y (que tomamos como nova reta no infinito) obtemos $Z^2 = X^3$. Segue-se que $m_P(F) = 2$, $(Z,F)_P = 3$ e $(L,F)_P = 2$ para $L \neq Z$ (L = reta passando por P). (Veja Fig. 23).

5. Proposição - Seja F uma curva de grau d e seja $P \in \mathbb{P}^2$. Então:

(1) (Fórmula de Euler) $dF = XF_X + YF_Y + ZF_Z$.

(2) P é um ponto singular de F se e só se

$$F_X(P)X = F_Y(P) = F_Z(P) = 0 .$$

(3) Se F é liso em P então a reta tangente a F neste ponto é

$$F_X(P)X+F_Y(P)Y+F_Z(P)Z = 0.$$

Demonstração.

(1) Sendo ambos os membros lineares como funções de F, é suficiente verificar a fórmula quando F é um monômio $X^i Y^j Z^k$, $i+j+k = d$, o que é imediato.

(2) Suponhamos $P = (a:b:1)$. Por (III.5(1)) P é um ponto singular de F se e só se $(F_*)_X = (F_*)_Y = F_* = 0$ em (a,b). Aplicando (1), concluimos dessas igualdades que $F_Z(P)=0$. Reciprocamente, se $F_X = F_Y = F_Z = 0$ em P, então $F_* = (F_*)_X = (F_*)_Y = 0$ em P. O mesmo argumento se aplica se P é da forma (a:1:b) ou (1:a:b).

(3) Suponhamos, por exemplo, $P = (a:b:1)$. De acordo com (III.5(2)) a reta tangente é dada pelo polinômio (já homogeneizado),

$$(F_*)_X(a,b)(X-aZ) + (F_*)_Y(a,b)(Y-bZ) ,$$

que é igual a

$$F_X(P)X + F_Y(P)Y - Z[aF_X(P) + bF_Y(P)] .$$

Por (1), a expressão entre colchetes coincide com $-F_Z(P)$.

C.Q.D.

Exercícios

1) Para cada inteiro $m \geq 1$, construa uma curva F, de grau m, tal que a origem $0 = (0:0:1)$ seja um ponto liso e a multiplicidade de interseção $(X,F)_0$ seja igual a um. É possível conseguir F lisa (inclusive no infinito)?

2) Mostre que uma cúbica com 2 pontos singulares é redutível.

3) Ache as multiplicidades dos pontos no ∞ e os índices de interseção com a reta no ∞ para cada uma das curvas consideradas nos Capítulos I e III.

4) Mostre que uma curva projetiva $F \subset \mathbb{P}^2$ é não singular se e só se $F(X,Y,1), F(X,1,Z)$ e $F(1,Y,Z)$ são todas não singulares (ou ϕ). Mostre com um exemplo que 2 dessas podem ser não singulares embora F seja singular.

5) Mostre que, para cada curva irredutível F, se $d = \partial F$ então existem $d(d+3)/2$ pontos tais que F é a única curva deste grau que os contém. (Sugestão: existem retas $L_1,\ldots,L_d$, cada qual cortando F em d pontos distintos, e

tais que $L_i \cap L_j \cap L_k = L_i \cap L_j \cap F = \phi$ para i,j,k distintos. Tome $P \in F$ e fora dos L_i's; depois escolha $i+1$ pontos distintos em $L_i \cap F$ $(i = 1,\ldots,d-1)$ e mais d pontos em $L_d \cap F$. Se existisse $G \neq F$ contendo estes pontos, com $\partial G = d$, existiria uma curva H da forma $xF + yG$ (com $(x:y) \in \mathbb{P}^1$) contendo um $(d+1)$-ésimo ponto de L_d. Logo $L_d \subset H$, etc ...).

6) Prove que toda curva projetiva lisa é irredutível. (Compare com Exercício III.2).

§2. O teorema de Bezout

Consideremos agora o problema do cálculo do número de pontos de interseção de duas curvas projetivas F, G de graus arbitrários.

6. Lema. Sejam F,G curvas planas projetivas. Então $F \cap G$ é finita se e só se F,G não admitem componente comum.

Demonstração. Se F,G não admitem fator comum em $k[X,Y,Z]$ então F_*, G_* também não o admitem em $k[X,Y]$. Com efeito, se $F_* = fh$, $G_* = gh$, com $f,g,h \in k[X,Y]$ e h não constante, então $(F_*)^* = f^*h^*$, $(G_*)^* = g^*h^*$. Daí se seguiria que h^* é fator de F,G, contradição. Como F_*, G_* não têm componente comum, segue-se que $F \cap Z$ ou $G \cap Z$ é finita, (senão Z seria componente comum) e portanto $F \cap G$ é finita. A recíproca é trivial.

C.Q.D.

Esclarecida a finitude de $F \cap G$, propomo-nos a calcular seu número de pontos. Note que ainda não apresentamos nenhuma garantia de que $F \cap G$ seja não vazia, em geral. Isto será uma conseqüência do Teorema de Bezout.

7. Definição. Sejam $P_i = (x_i:y_i:z_i)$, $i = 1,\ldots,r$ os distintos pontos de $F \cap G$.

Diremos que F,G estão em boa posição ou bem posicionadas se $P_o = (0:1:0) \notin F \cap G$.

Diremos que F, G estão em muito boa posição ou muito bem posicionadas se $P_o \notin F \cap G$ e se, para cada par P_i, $P_j \in F \cap G$, P_o, P_i, P_j são não colineares. Esta última condição é equivalente à exigência de que $i \neq j$ implique $(x_i:z_i) \neq (x_j:z_j)$.

Suporemos no que segue que F,G não têm componente em comum.

Escrevamos

$$F = A_o Y^d + A_1 Y^{d-1} + \ldots + A_d \ ,$$

$$G = B_o Y^e + \ldots + B_e$$

onde A_i, $B_j \in k[X,Z]$ são homogêneos de graus i,j.

É claro que $(0:1:0) \in F \iff A_o = 0$. Logo, estando F,G bem posicionados, temos A_o ou $B_o \neq 0$. Lembrando o Lema II.9, temos que a resultante $R = R(X,Z)$ de F,G com respeito a Y é homogênea de grau $d \cdot e$.

Por outro lado, levando em conta que A_o ou $B_o \neq 0$, pa-

ra cada $(x:z) \in \mathbb{P}^1$ temos

$$R(x,z) = 0 \iff \exists (x:y:z) \in F \cap G.$$

Supondo F,G muito bem posicionadas, concluimos que R escreve-se na forma

$$R(X,Z) = c \prod_{1}^{r} (z_i X - x_i Z)^{m_i}$$

onde c , é uma constante $\neq 0$, os expoentes m_i são inteiros ≥ 1, $\Sigma m_i = de$, e $P_i = (x_i:y_i:z_i)$, $i = 1,\ldots,r$ são os distintos pontos de $F \cap G$. É natural, portanto, adotarmos a seguinte

8. Definição. A multiplicidade ou índice de interseção de F,G no ponto P é definida por

$$(F,G)_P = \begin{cases} 0 & \text{se } P \notin F \cap G \\ m_i & \text{se } P = P_i \end{cases} \quad \text{nas condições acima.}$$

Observando que $\Sigma m_i = \partial R = (\partial F)(\partial G)$, demonstramos, para o caso em que F,G estão muito bem posicionadas, o importante

9. Teorema de Bézout. Duas curvas planas projetivas F, G sem componente em comum, têm $(\partial F)(\partial G)$ pontos em comum contados com multiplicidade.

Para o caso geral, é necessário definirmos $(F,G)_P$ livre da hipótese de bom posicionamento. É claro que, se $F \cap G$ é finito, existe uma projetividade T tal que T.F, T.G estão em muito boa posição. A sugestão foi lançada:

10. Definição. O índice ou multiplicidade de interseção de F,G (curvas projetivas sem componentes em comum) no ponto $P \in \mathbb{P}^2$ é

$$(F,G)_P = (T.F,\ T.G)_{TP}$$

onde T denota uma projetividade tal que T.F, T.G estejam muito bem posicionadas, e o 2º membro é calculado como na Definição 8.

Exemplo. O círculo F: $X^2+Y^2 = 2X$ e a parábola G: $Y^2 = X$ (Fig. 9) não estão muito bem posicionados: os pontos de interseção (1:1:1) e (1:-1:1) são colineares com (0:1:0). Aplicando a projetividade T que fixa Z e troca X por Y, obtemos

$$T.F = X^2+Y^2-2YZ, \quad T.G = X^2-ZX\ ,$$

que agora estão em muito boa posição. A resultante é $X^2(X-Z)(X+Z)$, indicando as multiplicidades 2 e 1 dos pontos (0:0:1) e (1:±1:1) respectivamente.

O leitor atento objetará de imediato, pois a "definição" acima proposta só é honesta se provarmos que o 2º membro independe de T. Mãos à obra, pois!

11. Proposição. Sejam F,G curvas muito bem posicionadas. Seja T uma projetividade tal que T.F, T.G também estão muito bem posicionadas. Então

$$(F,G)_P = (T.F,\ T.G)_{TP} \quad \forall\ P \in \mathbb{P}^2\ .$$

Demonstração. Usaremos um artifício notável, devido a Seidenberg[1] .

A idéia é provar a igualdade quando T é uma projetividade genérica. Precisamente, sejam W_{ij} $(i,j = 1,2,3)$ 9 indeterminadas, e seja K o fecho algébrico de $k(W_{ij})$, o corpo de funções racionais nessas novas variáveis. O plano projetivo $\mathbb{P}^2_k$ se identifica a um subconjunto de $\mathbb{P}^2_K$, o plano projetivo sobre o corpo K. A projetividade genérica W é a projetividade de $\mathbb{P}^2_K$ definida pela matriz (W_{ij}) ,

$$W(x_1:x_2:x_3) = (\Sigma W_{1j}x_j : \Sigma W_{2j}x_j : \Sigma W_{3j}x_j) \quad .$$

F,G definem curvas em $\mathbb{P}^2_K$, que denotamos por $\overline{F},\overline{G}$. O fato importante a observar é que, mesmo considerando pontos com coordenadas em $K \supset k$, temos

$$\overline{F} \cap \overline{G} = F \cap G = \{P_1,\ldots,P_r\} \quad .$$

Com efeito, as coordenadas de um ponto de $\overline{F} \cap \overline{G}$ são raízes da resultante de F,G com relação a uma variável conveniente, e portanto satisfazem a uma equação algébrica a coeficientes em k. Sendo este algebricamente fechado, vemos que os pontos comuns a $\overline{F},\overline{G}$ em $\mathbb{P}^2_K$ são os que já conhecíamos, em $F \cap G$.

Consideremos agora os "transladados genéricos", $W.\overline{F}$, $W.\overline{G}$. Temos, por definição

$$(W.\overline{F})(X,Y,Z) = \overline{F}(W^{-1}(X,Y,Z))$$

Eliminamos os denominadores desta última expressão, definindo

$$F^W(X,Y,Z) = \det(W_{ij})^{\partial F} F(W^{-1}(X,Y,Z)).$$

---

1) A. Seidenberg, "Elements of the Theory of Algebraic Curves", Addison Wesley, 1968.

F^W é um polinômio a coeficientes em $k[W_{ij}]$, anel dos polinômios nas variáveis W_{ij}. Note que F^W e $W.\overline{F}$ definem a mesma curva em $\mathbb{P}^2_K$, pois diferem por um múltiplo constante.

Para cada projetividade T definida por uma matriz (t_{ij}) a coeficientes em k, é evidente que, o resultado da substituição $W_{ij} \to t_{ij}$ em F^W é $T.F$.

Observemos que F^W, G^W estão muito bem posicionados. Com efeito, se $P_o = (0:1:0)$ pertencesse a $F^W \cap G^W$, teríamos $P_o = W(P)$ para algum $P \in F \cap G$. Daí, especializando (W_{ij}) para a matriz identidade, viria $P_o \in F \cap G$, proibido por hipótese. Analogamente, se existissem $Q, Q' \in F^W \cap G^W$ colineares com P_o, concluiríamos a existência de $P, P' \in F \cap G$ colineares com P_o.

Calculando a resultante de F^W, G^W, encontramos

$$R((W),X,Z) = c(W) \prod_{i=1}^{r} (z_i(W)X - x_i(W)Z)^{n_i} ,$$

onde $c(W)$ é um polinômio $\neq 0$, $n_i = n_i(W)$ é um inteiro ≥ 1 e

$$x_i(W) := W_{11}x_i + W_{12}y_i + W_{13}z_i ,$$

$$z_i(W) := W_{31}x_i + W_{32}y_i + W_{33}z_i ,$$

são coordenadas homogêneas de $W(x_i:y_i:z_i)$, o i-ésimo ponto de $F^W \cap G^W$. A expressão para a resultante está correta porque sabemos que $R((W),X,Z) \in k[W_{ij}][X,Y]$ e que, em $K[X,Z]$, ela é completamente decomponível nos fatores lineares $z_i(W)X - x_i(W)Z$ correspondentes aos pontos de $F^W \cap G^W$.

Agora é claro que, especializando (W_{ij}) para qualquer (t_{ij}) associada a uma projetividade T tal que $T.F$, $T.G$ este-

jam muito bem posicionados, $R(W_{ij},X,Z)$ se especializa na resultante de $T.F$, $T.G$, com cada fator $z_i(W)X-x_i(W)Z$ se transformando no fator correspondente ao ponto TP_i. Segue-se que os expoentes $n_i(W)$ não dependem de W_{ij} , e em particular,

$$(T.F\ ,\ T.G)_{TP} = (F,G)_P\ ,$$ C.Q.D.

Para aplicações do Teorema de Bezout, é importante sabermos como estimar $(F,G)_P$ em termos de dados locais de F,G, separadamente, em torno do ponto P.

13. Proposição. $(F,G)_P \geq m_P(F)\ m_P(G)$, valendo a desigualdade se e só se F e G possuem uma tangente comum em P.

Demonstração. Podemos supor $P = (0:0:1)$ e que F,G estão muito bem posicionados. Ponhamos $m = m_P(F)$, $n = m_P(G)$. Devemos mostrar que X^{mn} divide $R(X,Z)$ em $k[X,Z]$, ou, equivalentemente, que X^{mn} divide $R(X,1)$ em $k[X]$.

Estando F, G bem posicionados, sabemos que $R(X,1)$ é igual a $R(X)$, resultante de $f = F(X,Y,1)$, $g = G(X,Y,1)$, a menos de fator constante $\neq 0$.

Para o cálculo de $R(X)$, escrevemos f, g em potências crescentes de Y (causando apenas uma permutação nas colunas da matriz cujo determinante queremos calcular):

$$f = a_0X^m + a_1X^{m-1}Y + \ldots + a_mY^m + a_{m+1}\ Y^{m+1} + \ldots$$

$$g = b_0X^n + \ldots + b_nY^n + b_{n+1}\ Y^{n+1} + \ldots$$

onde a_i, $b_j \in k[X]$, sendo os m primeiros a's e os n primeiros b's constantes. Temos

$$R(X) = \pm \begin{vmatrix} a_oX^m & a_1X^{m-1} & \cdots & a_m & a_{m+1}\cdots \\ & a_oX^m & \cdots & a_{m-1}X & a_m \\ \hline b_oX^n & b_1X^{n-1} & \cdots & b_n & b_{n+1}\cdots \\ & b_oX^n & \cdots & b_{n-1}X & b_n \cdots \\ & & \vdots & & \end{vmatrix}$$

Multiplicando a 1ª linha de a's por X^n, a 2ª por X^{n-1}, etc..., a 1ª de b's por X^m, etc..., vemos que é possível fatorar $X^{m+n-j+1}$ de j-ésima coluna, $1 \leq j \leq m+n$. Desta maneira, concluímos que $R(X)$ é divisível por X elevado ao expoente

$$\frac{(m+n)(m+n-1)}{2} - \frac{m(m-1)}{2} - \frac{n(n-1)}{2} = mn.$$

Para estudarmos em que caso ocorre igualdade, definamos

$$\tilde{R}(X) = R(X)\, X^{-mn}.$$

Trata-se de um polinômio em X. Ponhamos

$$f_m := a_oX^m + a_1X^{m-1}Y + \ldots + a_mY^m,$$

$$g_n := b_oX^n + \ldots + b_nY^n$$

Precisamos mostrar que

$\tilde{R}(0) = 0 \iff f_m, g_n$ têm fator comum em $k[X,Y]$.

Sem perda de generalidade, podemos supor que X não é fator comum, i.e., a_m ou $b_n \neq 0$. Neste caso, f_m, g_n têm fator comum em $k[X,Y]$ se e só se $f_m(1,Y)$, $g_n(1,Y)$ têm raiz comum.

Examinando com atenção o processo utilizado acima para extrair o fator X^{mn} de $R(X)$, percebemos que $\tilde{R}(0)$ é o determinante de uma matriz que apresenta uma submatriz $(m+n)x(m+n)$ (formada pelas n primeiras linhas de a's e m primeiras de b's) igual à matriz que fornece a resultante de $f_m(1,Y)$, $g_n(1,Y)$; os demais elementos das colunas de ordem maior que $m+n$ e nas mesmas linhas desta submatriz não nulos. Além disso, o bloco complementar da submatriz em questão é justamente a matriz que dá a resultante dos polinômios $\overline{f} = Y^{-m}f(0,Y)$, $\overline{g} = Y^{-n}g(0,Y)$. Desenvolvendo o determinante pelos menores extraídos das $m+n$ primeiras colunas, encontramos

$$\tilde{R}(0) = R_{f_m,g_n} \cdot R_{\overline{f},\overline{g}} \ .$$

Ora, $R_{\overline{f},\overline{g}} \neq 0$, do contrário $\overline{f}(Y)$, $\overline{g}(Y)$ admitiriam raiz comum y, necessariamente $\neq 0$ (porque a_m ou $b_n \neq 0$). Mas então teríamos $(0,y) \in f \cap g$, impedido pela hipótese de que F,G estão muito bem posicionadas e já têm o ponto $(0,0)$ em comum.

Em conclusão, $\tilde{R}(0)$ é zero se e só se R_{f_m,g_n} é zero.

C.Q.D.

14. Corolário. Sejam F, G curvas sem componentes em comum. Então

$$\sum_{P \in F \cap G} m_P(F)\, m_P(G) \leq (\partial F)(\partial G) \ .$$

Demonstração. Pelo teorema de Bezout, sabemos que

$$\Sigma(F,G)_P = (\partial F)(\partial G) \ .$$

Pela proposição anterior, temos cada $(F,G)_p \geq m_p(F)\, m_p(G)$.

C.Q.D.

Exercícios

7) Mostre que as Definições 10 e 2 são consistentes.

8) Calcule as multiplicidades de interseção para os pares de curvas:

a) $Y = X^3$, $Y = X^2$; b) $X^2+Y^2 = 1$, $X^2+Y^2 = 4$;

c) $(X^2+Y^2)^2 = X^2+Y^2$, $X^2+Y^2 = 1$; d) $(X^2+Y^2)^2 = X^2-Y^2$, $X^2+Y^2 = X-Y$.

9) Prove que se F,G são curvas que estão apenas bem posicionadas (não necessariamente muito bem pos.) e se $R_{F,G} = \prod (z_j X - x_j Z)^{n_j}$, com os $(x_j:z_j) \in \mathbb{P}^1$ 2 a 2 distintos, então n_j é a soma das multiplicidades de interseções correspondentes aos pontos $(x:y:z)$ com $(x:z) = (x_j:z_j)$.

10) Sejam f, g curvas planas afins, com f^*, g^* não necessariamente bem posicionados. Seja $R(X) = \prod (X-x_i)^{n_i}$ a resultante. Discuta a relação dos n_i's com multiplicidades de interseção e estude a diferença de $\Sigma\, n_i$ para $(\partial f)(\partial g)$.

11) Mostre que uma quártica com 3 pontos singulares colineares ou com 4 pontos singulares é redutível.

(Sugestão: trace uma cônica pelos 4 pontos e mais um quinto).

CAPÍTULO VI

PROPRIEDADES DO ÍNDICE DE INTERSEÇÃO

Mostraremos neste capítulo que o índice de interseção é caracterizado por uma lista de propriedades naturais. Como primeira consequência, veremos que a fórmula explícita que define $(F,G)_P$ pode ser esquecida, pois as referidas propriedades fornecem um método para o cálculo efetivo. Apresentamos depois uma fórmula alternativa para o índice de interseção, usando séries de potências. Esta nova abordagem dispensa o deslocamento prévio exigido pelo método da resultante e põe em relevo o fato de $(F,G)_P$ só depender do comportamento de F,G em torno de P.

§1. As propriedades características

Inicialmente reescreveremos a Definição V.10 estendendo-a para o caso em que as curvas podem admitir componente comum.

1. Definição. Sejam F,G curvas planas projetivas e seja P um ponto de $\mathbb{P}^2$. Escrevemos $F = F_0H$, $G = G_0H$, com $H = \text{mdc}(F,G)$ (ou seja, H é a reunião das componentes comuns de F,G, tomadas com multiplicidade; F_0, G_0 não têm componente em comum). Os pontos de $F_0 \cap G_0$ fora de H são as interseções isoladas de F,G. Definimos a multiplicidade ou índice de interseção de F,G em P por

$$(F,G)_P = \begin{cases} \infty & \text{se } P \in H \\ 0 & \text{se } P \notin F \cap G \\ (F_o,G_o)_P & \text{se } P \text{ é uma interseção isolada de } F,G. \end{cases}$$

Lembramos que, neste último caso, escolhemos uma projetividade S tal que $S.F_o$, $S.G_o$ estejam muito bem posicionadas. Agora, se $(x:y:z) = S(P)$, então $(F_o,G_o)_P$ é igual ao expoente com que $zX-xZ$ ocorre na resultante de $S.F_o$, $S.G_o$.

Mostramos na Proposição (V.11) que esta definição independe da particular projetividade com que deslocamos F_o, G_o. Se não tivermos o cuidado de eliminar as componentes comuns, a resultante de F,G será nula.

O processo de colocar 2 curvas em muito boa posição é em geral laborioso. O cálculo de $(F,G)_P$ será tremendamente facilitado pela lista de propriedades que descreveremos logo a seguir. De fato, mostraremos que elas fornecem um algorítmo para o cálculo do índice, dispensando completamente a fórmula da resultante. Em particular, qualquer outra fórmula que satisfaça a essas propriedades terá que atribuir o mesmo valor.

2. Proposição. $(F,G)_P$ satisfaz às seguintes propriedades:

(1) $(F,G)_P = (G,F)_P$ é ∞ ou um número inteiro ≥ 0 .

(2) $(F,G)_P = 0 \iff P \notin F \cap G$

(3) $(F,G)_P = \infty \iff P \in H =$ componente comum de F,G.

(4) $(F,G)_P = (T.F,\ T.G)_{TP}$ $\forall$ projetividade $T: \mathbb{P}^2 \to \mathbb{P}^2$.

(5) $(X,Y)_P = 1$ onde $P = (0:0:1)$.

(6) $(F,G+AF)_P = (F,G)_P$ $\forall$ A homogêneo com $\partial A = \partial G - \partial F$.

(7) $(F,G_1G_2)_P = (F,G_1)_P + (F,G_2)_P$.

Antes de escrever a demonstração, vamos ilustrar como essas propriedades podem ser empregadas para o cálculo de $(F,G)_P$, aplicando-as ao seguinte

Exemplo: F: $(X^2+Y^2)^2 = Y^3-3X^2Y$ (rosácea de 3 pétalas)

G: $Y^3 = Y^2-3X^2$ (cúbica nodal)

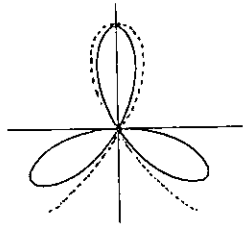


Fig. 24

Temos $F = (X^2+Y^2)^2 - Z(Y^3-3X^2Y)$, $G = Y^3-Z(Y^2-3X^2)$. Logo, empregando as propriedades indicadas na última coluna, vem

$$(F,G)_P = (F-YG,G)_P \qquad ((1),(6))$$

$$= (X^4+2X^2Y^2,G)_P$$

$$= (X^2,G)_P + (X^2+2Y^2,G)_P \qquad ((7))$$

$$= 2(X,Y^2(Y-Z))_P + (X^2+2Y^2,Y^3-7ZY^2)_P \qquad ((6))$$

$$= 4(X,Y)_P + 2(X,Y-Z)_P + 4(X,Y)_P + (X\pm i\sqrt{2}\ Y,Y-7Z)_P.$$

Logo,

$$F \cap G = \{(0:0:1),\ (0:1:1),\ (\pm 7i\sqrt{2}:7:1)\}\ ;$$

no primeiro desses, a multiplicidade de interseção é igual a 8; no 2º é 2; nos 2 últimos é 1.

Demonstração da Proposição 2. As 3 primeiras propriedades dispensam comentários.

A 4ª - invariância por mudança projetiva de coordenadas - decorre essencialmente do fato de que, na Definição (1.1), gozamos de liberdade irrestrita na escolha da projetividade T. Com efeito, se $(F,G)_P = 0$ ou ∞, é óbvio que $(T.F,T.G)_{TP}$ tem o mesmo valor. Se P é uma interseção isolada, escolhemos (com a notação da Definição (1.1) S tal que $S.F_o$, $S.G_o$ estejam muito bem posicionadas e tomamos $U = ST^{-1}$. Temos então

$$(T.F,T.G)_{TP} = (U.(T.F),\ U.(T.G))_{UTP}$$

$$= (S.F,S.G)_{SP}$$

$$= (F,G)_P$$

Verifiquemos (5). Escrevendo $F = 0Y+X$, $G = Y$, calculamos $R_{F,G} = \begin{vmatrix} 0 & X \\ 1 & 0 \end{vmatrix} = -X$. Isto mostra que (0:0:1) ocorre com multiplicade 1.

Para a 6ª propriedade, é suficiente considerarmos o caso em que A é um polinômio da forma $A = A_m Y^{c-m}$, com $c = \partial G - \partial F$ e $A_m(X,Z)$ homogêneo de grau m. Neste caso, é imediato que a

matriz cujo determinante define $R_{F,G+AF}$ é obtida da associada a $R_{F,G}$ somando às linhas dos coeficientes de G, múltiplos das linhas dos coeficientes de F.

A 7ª propriedade é de verificação mais trabalhosa. Ela se baseia nos seguintes resultados da teoria da eliminação.

3. Lema. Seja $A = \mathbb{Z}[X_0, X_1, \ldots, X_m, Y_0, \ldots, Y_n]$ o anel dos polinômios nas indeterminadas X_i, Y_j, a coeficientes inteiros. Sejam

$$\left.\begin{aligned} f &= X_0(Y-X_1)\ldots(Y-X_m) = X_0(Y^m - (\Sigma X_i)Y^{m-1} + \ldots), \\ g &= Y_0(Y-Y_1)\ldots(Y-Y_n) = Y_0(Y^n - (\Sigma Y_i)Y^{n-1} + \ldots) \end{aligned}\right\} \in A[Y]$$

Temos então as seguintes fórmulas para a resultante de f, g:

$$\begin{aligned} R &= X_0^n\, Y_0^m \prod_{i,j}(X_i - Y_j) \\ &= X_0^n \prod_i g(X_i) \\ &= (-1)^{mn}\, Y_0^m \prod_j f(Y_j)\ . \end{aligned}$$

Demonstração. Denotemos por S o 2º membro da 1ª fórmula proposta. É imediato que S satisfaz às 2 outras igualdades. Por outro lado, a definição da resultante mostra que $R = X_0^n\, Y_0^m\, \tilde{R}$, onde $\tilde{R}$ denota um polinômio nas variáveis $X_1, X_2, \ldots, Y_1, Y_2, \ldots$, a coeficientes em $\mathbb{Z}$. Substituindo-se X_i por Y_j, com $i, j \geq 1$, anula-se a resultante; logo $X_i - Y_j$ divide R e portanto S divide R em A. Mas é fácil verificar que S e R têm o mesmo grau em X_i (resp. Y_j), donde R é um

múltiplo inteiro de S. Fazendo $X_o = Y_o = Y_1 = \ldots = Y_n = 1$ e $X_1 = \ldots = X_m = 0$, vê-se de imediato que o referido inteiro é 1, ou seja, R = S.

C.Q.D.

4. Proposição. Seja D um domínio. Dados $f,g,h \in D[Y]$, vale a fórmula

$$R_{f,gh} = R_{f,g}\, R_{f,h}.$$

Demonstração. Escrevamos

$$f = x_o Y^m + \ldots$$

$$g = y_o Y^r + \ldots$$

$$h = z_o Y^s + \ldots ,$$

as reticências indicando termos de grau inferior. Existe uma extensão $E \supset D$ tal que, em $E[Y]$, podemos fatorar

$$f = x_o(Y-x_1)\ldots(Y-x_m) ,$$

$$g = y_o(Y-y_1)\ldots(Y-y_r) ,$$

$$h = z_o(Y-z_1)\ldots(Y-z_s) .$$

(Tomar, por exemplo, um corpo de raízes do produto fgh).

Consideremos o anel $A = \mathbb{Z}[X_o,\ldots,X_m, Y_o,\ldots,Y_r, Z_o,\ldots Z_s]$. Definamos

$$\tilde{f} = X_o(Y-X_1)\ldots(Y-X_m) ,$$

$$\tilde{g} = Y_o(Y-Y_1)\ldots(Y-Y_r) ,$$

$$\tilde{h} = Z_o(Y-Z_1)\ldots(Y-Z_s) .$$

Podemos definir um homomorfismo de anéis,

$$\varphi\colon A \to E$$

mandando X_i em x_i etc..., de sorte que o homomorfismo induzido,

$$A[Y] \to E[Y]$$

aplica $\tilde{f}$ em f, etc. ... Nestas condições, é claro que

$$\varphi(R_{\tilde{f},\tilde{g}\tilde{h}}) = R_{f,gh} .$$

Apliquemos o Lema a $\tilde{f}$, $\tilde{g}\tilde{h}$. Obtemos:

$$R_{\tilde{f},\tilde{g}\tilde{h}} = X_o^{r+s} \prod(\tilde{g}\tilde{h})(X_i))$$

$$= (X_o^r \prod\tilde{g}(X_i))(X_o^s \prod\tilde{h}(X_i)) .$$

$$= R_{\tilde{f},\tilde{g}} R_{\tilde{f},\tilde{h}} .$$

Calculando φ em ambos os membros, resulta a fórmula anunciada.

C.Q.D.

Verifiquemos agora a propriedade (7) dada na Proposição 2:

$$(F,G_1G_2)_P = (F,G_1)_P + (F,G_2)_P .$$

Podemos supor que P é uma interseção isolada de F,G_1G_2, e sem perda de generalidade, supor logo que F,G_1G_2 não têm componente comum e estão muito bem posicionadas. Mas agora a fórmula proposta decorre imediatamente da Proposição 4.

5. Proposição. O índice de interseção $(F,G)_P$ é univocamente determinado pelas propriedades (1),...,(7) listadas na Proposição 2.

Demonstração. É suficiente provar que $(F,G)_P$ é calculável a partir dessas propriedades. E para tanto, basta considerarmos o caso em que F,G não têm componente comum passando por P. Consideremos F,G como polinômios em Z a coeficientes em $k[X,Y]$, escrevendo

$$F = A_o Z^m + \ldots + A_m$$

$$G = B_o Z^n + \ldots + B_n$$

com $A_i, B_j \in k[X,Y]$ homogêneos, $\partial A_i = \partial F + i - m$, $\partial B_j = \partial G + j - n$, $A_o B_o \neq 0$.

Procederemos por indução sobre $\min\{m,n\}$.

Se $m = 0$, então $F = A_o$ é um produto de fatores lineares homogêneos do tipo $aX+bY$, caso em que sabemos calcular $(F,G)_P$ usando as propriedades. Com efeito, por (1) e (7) reduzimos ao caso em que F é uma reta; por (4) podemos supor $P = (0:0:1)$ e $F = X$; por (6) podemos substituir G por $F(0,Y,Z)$; este último é um produto de fatores lineares e então ganhamos, usando (7) e (5) (e possivelmente (4) para transformar em Y um fator linear).

Suponhamos, para a etapa indutiva, $0 < m \leq n$. Sem perda de generalidade, podemos supor F irredutível. Em particular,

A_o e F são primos relativos. Aplicamos o algorítmo da divisão, encontrando, para algum inteiro $r \geq 0$, polinômios $B,\hat{G}$ tais que

$$A_o^r G = BF+\hat{G} , \quad \text{com} \quad \partial_Z \hat{G} \leq m-1.$$

Note que $\hat{G}$ é primo relativo com F. Usando (6), obtemos

$$(F,A_o^r G)_P = (F,\hat{G})_P .$$

Logo,

$$(F,G)_P = (F,\hat{G})_P - (F,A_o^r)_P ;$$

O 1º termo no 2º membro é calculável por indução; o 2º é calculável pois $\partial_Z A_o^r = 0$. Isto completa a demonstração.

C.Q.D.

Exercícios

1) Sejam F: $(X^2+Y^2)^2 = X^2-Y^2$ e C_a: $X^2+Y^2 = a(X-Y)$, onde a é constante arbitrária. (Se $a = \infty$, tome C_∞: $Z(X-Y) = 0$). Para cada a, calcule $(F,C_a)_P$ em cada ponto. Verifique o teorema de Bezout.

2) Mostre que F: $Y^2 = X-X^3$ e G: $3XY^2 = 3X^2-1$ se intersectam em 9 pontos <u>distintos</u>. Se P é qualquer um deles, mostre que o índice de interseção de F com sua reta tangente em P é igual a 3.

3) Prove que $(F,G)_P$ só depende das componentes de F,G que passam por P, usando apenas as propriedades (1),...,(7),

da Proposição 2.

4) Prove que $(F,G)_P \geq m_P(F)\, m_P(G)$ usando apenas (1),...,(7).

5) Refaça o Exercício V-7 sem calcular resultantes.

6) Use o Lema 3 para mostrar que, se $f = a_0Y^m+\ldots+a_m$, $g = b_0Y^n+\ldots+b_n$ são polinômios a coeficientes em um domínio arbitrário A, com $a_0b_0 \neq 0$, então $R_{f,g} = 0$ se e só se f,g admitem raiz comum em alguma extensão do corpo de frações de A.

§2. Séries de potências

No restante deste capítulo, descrevemos uma definição alternativa para a multiplicidade de interseção, empregando séries de potências. Há várias outras alternativas, mas qualquer definição aceitável deverá satisfazer a lista de propriedades naturais dadas na Proposição 2. e conseqüentemente, terá que coincidir com a que adotamos, via resultantes.

Lembramos que uma série de potências na variável X a coeficientes no anel A é uma expressão da forma

$$\sum_{i=0}^{\infty} a_i X^i$$

com os coeficientes $a_i \in A$; duas tais expressões são iguais se e só se os coeficientes correspondentes são iguais. O conjunto $A\langle X\rangle$ das séries de potências a coeficientes em A contém um subconjunto que se identifica naturalmente com o anel dos polinômios

$A[X]$. Definem-se as operações de soma e produto de séries de potências de maneira evidente, de sorte que $A[X]$ se torna um subanel de $A\langle X\rangle$.

Tomando uma nova variável independente Y, o anel das séries de potências em 2 variáveis é definido por

$$A\langle X,Y\rangle = (A\langle X\rangle)\langle Y\rangle \ .$$

Seus elementos se escrevem na forma

$$\sum_{i,j} a_{ij} X^i Y^j .$$

Resumimos na proposição seguinte algumas propriedades básicas das séries de potências. A demonstração é deixada a cargo do leitor.

6. Proposição.

(a) Se A é um domínio (i.e., anel comutativo, com unidade e sem divisores de zero) então $A\langle X\rangle$ também é.

(b) $\Sigma a_i X^i$ é inversível em $A\langle X\rangle$ se e só se o termo constante a_o é inversível em A.

(c) Se α é uma série de potências com termo constante nulo e β é uma série de potências arbitrária, é possível "substituir X por α em β", resultando uma série $\beta(\alpha)$ bem determinada pela seguinte condição: se $\beta_m = \sum_o^m b_i X^i$ é o polinômio "m-ésima soma parcial" de $\beta = \sum_o^\infty b_i X^i$, então $(\beta(\alpha))_m = \beta_m(\alpha)$.

(d) Se α é como acima, a aplicação $\beta \longmapsto \beta(\alpha)$ é um homomorfismo de anéis.

Exemplo: $(1-X)^{-1} = 1+X+X^2+\ldots$. Mais geralmente, se $\alpha \in A\langle X\rangle$ é uma série de potências com termo constante nulo, então $(1-\alpha)^{-1} = 1+\alpha+\alpha^2+\ldots$. Esta expressão tem sentido, pois apenas um nº finito de parcelas contribuem para o coeficiente de cada termo X^i.

Consideremos agora um polinômio $p(X) \in k[X]$. A multiplicidade de uma raiz x de $p(X)$ pode ser detectada substituindo X por $X+x$ e extraindo a maior potência possível de X como fator de $p(X+x)$. Escrevemos então $p(X+x) = X^m u(X)$, onde $u(0) \neq 0$. Logo, $u(X)$ é inversível em $k\langle X\rangle$, e portanto os ideais $(p(X+x))$ e (X^m) são iguais em $k\langle X\rangle$. Segue-se a igualdade dos anéis quocientes:

$$k\langle X\rangle/(p(X+x)) = k\langle X\rangle/(X^m) \ .$$

Ora, este último, considerado como espaço vetorial sobre k, claramente admite para base as classes de $1, X, \ldots, X^{m-1}$ (mod. (X^m)). Vemos então que a multiplicidade da raiz x de $p(X)$ é igual à dimensão do espaço vetorial $k\langle X\rangle/(p(X+x))$.

Daí até inferirmos uma fórmula para a multiplicidade de interseção de duas curvas (digamos, inicialmente, afins) f,g é um pequeno (?) passo:

7. Definição. Dado $P = (x,y) \in \mathbb{A}^2$, ponhamos (provisoriamente! (cf. Proposição 12),

$$[f,g]_P = \dim\{k\langle X,Y\rangle/(f(X+x,Y+y),\ g(X+x,Y+y))\}$$

Exemplo. Suponhamos $f = Y$, g arbitrário, $P = (x,y)$. Se $y \neq 0$, então $P \notin f$, e deveríamos esperar $[f,g]_P = 0$. E de fato, $f(X+x,Y+y) = y+Y$ é inversível em $k\langle X,Y\rangle$, acarretando a nulidade do anel quociente em questão. Se $y = 0$, temos o isomorfismo

$$k\langle X,Y\rangle/(Y,g(X+x,Y)) \xrightarrow{\sim} k\langle X\rangle/(g(X+x,0)) \quad .$$

Do que foi exposto acima, a dimensão deste último quociente é justamente a multiplicidade de x como raiz de $g(X,0)$, em completa concordância com a definição já apresentada para $(f,g)_P$.

Estendemos a definição acima para curvas projetivas F,G, de modo natural:

8. Definição. Se $P = (x:y:1)$ (resp. $(x:1:z)$, resp. $(1:y:z:)$), desomogeneizamos F,G com relação a Z (resp. Y, resp. X) e definimos $[F,G]_P$ aplicando a fórmula dada na Definição 7 com as modificações óbvias.

Há que se fazer a seguinte verificação.

9. Lema. Se $P = (x:y:1) = (1:u:v)$ então

$$\dim k\langle X,Y\rangle/(F(X+x,Y+y,1),\ G(X+x,Y+y,1)) =$$
$$= \dim k\langle Y,Z\rangle/(F(1,Y+u,Z+v),\ G(1,Y+u,Z+v)).$$

(Valendo relação análoga se $(x:y:1) = (u:1:v)$...).

Demonstração. Temos $xv = 1$, $yv = u$. Em particular, $x \neq 0 \neq v$ e portanto $X+x$ é inversível em $k\langle X,Y\rangle$. Sendo F homogêneo, temos

$$F(X+x,Y+y,1) = (X+x)^{\delta F}\, F(1,(Y+y)(X+x)^{-1},\ (X+x)^{-1}) \quad \text{em} \quad k\langle X,Y\rangle.$$

Podemos construir um isomorfismo,

$$\varphi\colon k\langle X,Y\rangle \longrightarrow k\langle Y,Z\rangle$$

tal que

$$\begin{cases} \varphi(X) = (Z+v)^{-1} - x \\ \varphi(Y) = (Y+u)(Z+v)^{-1} - y \end{cases},$$

ou seja, $(X+x)^{-1} \mapsto Z+v$, $(Y+y)(X+x)^{-1} \mapsto Y+u$. Logo,

$$\varphi(F(X+x,Y+y,1)) = (Z+v)^{-\delta F} F(1,Y+u,Z+v),$$

e analogamente para G. Assim, φ induz por passagem ao quociente um isomorfismo entre os espaços cujas dimensões queríamos calcular.

C.Q.D.

Indicaremos mais adiante como proceder para a verificação de que $[F,G]_P$ satisfaz às propriedades características (1),..., (7), provando assim que $[F,G]_P = (F,G)_P$. Antes porém deduziremos uma consequência da nova fórmula.

Se $P = (x,y) \in f$ é um ponto não singular, digamos com $f_Y(P) \neq 0$, e $k = \mathbb{R}$ ou $\mathbb{C}$, sabemos do Cálculo que, próximo a P, a equação $f(X,Y) = 0$ fornece uma função implícita $Y=\varphi(X)$.

Esta função é de fato analítica, i.e., sua série de Taylor converge a $\varphi(X)$ numa vizinhança de x. Se g é uma curva arbitrária, podemos calcular $g(X,\varphi(X))$, obtendo uma série de potências em X. O índice de interseção $(f,g)_P$ deveria refletir a ordem do anulamento desta série para $X = x$.

10. Definição. A ordem (ou ordem de anulamento) da serie $\Sigma\, a_i X^i$ é o ínfimo dos inteiros i tais que $a_i \neq 0$. A ordem da série nula é ∞.

11. Proposição. Seja $P = (x,y)$ um ponto não singular sobre a curva f. Então:

(a) $k\langle X,Y\rangle/(f(X+x,Y+y))$ é k-isomorfo a $k\langle T\rangle$, anel das séries de potências na variável T.

(b) Se g é uma curva arbitrária, então $(f,g)_P$ é a ordem da imagem de $g(X+x,Y+y)$ em $k\langle T\rangle$ através do isomorfismo dado em (a).

Demonstração. Sem perda de generalidade, podemos supor $P = (0,0)$ e f da forma $Y+f_2+\ldots$. Pondo Y em evidência nos termos em que ocorre, temos $f = uY-X^2h$, com u inversível em $k\langle X,Y\rangle$. Visto que f e $u^{-1}f$ geram o mesmo ideal, podemos supor $u = 1$. (Agora h não é mais necessariamente um polinômio. Pouco importa.) Mostraremos que a aplicação

$$k\langle X\rangle \longrightarrow k\langle X,Y\rangle/(f)$$
$$s(X) \longmapsto \overline{s} = s(X) + (f)$$

é um isomorfismo. Esta afirmação é equivalente à seguinte:

$\forall\ g \in k\langle X,Y\rangle$ $\exists$ séries $q(X,Y)$, $r(X)$ tais que

$$g = qf + r.$$

As séries q,r são construídas por aproximações sucessivas. Escrevemos

$$g = g(X,0) + Yq_o = g(X,0) + (Y-X^2h)q_o + X^2hq_o .$$

Ponhamos $r_o = g(X,0)$, e recomecemos com $g_1 = hq_o$ em lugar de g:

$$g_1 = \underbrace{g_1(X,0)}_{r_1} + q_1 f + X^2 h q_1 , \quad \text{etc ...}$$

Desta maneira, construímos seqüências $r_o, r_1, \ldots \in k\langle X\rangle$, $q_o, q_1, \ldots \in k\langle X,Y\rangle$, de sorete que, para cada $m \geq 1$,

$$g = [\sum_o^m X^{2i} r_i + (\sum_o^m X^{2i} q_i) f] + X^{2m+2} hq_m .$$

Definimos $r(X) = \sum_{i\geq 0} X^{2i} r_i$, o que faz sentido, pois cada termo de $r(X)$ é obtido a partir de apenas um nº finito de $X^{2i} r_i$. Similarmente, definimos $q(X,Y) = \sum_{i\geq 0} X^{2i} q_i$.

Por construção, temos $g-r-qf$ múltiplo de X^N para todo N, donde se conclui facilmente

$$g = r+qf .$$

Uma vez demonstrado o isomorfismo

$$k\langle X\rangle \xrightarrow{\sim} k\langle X,Y\rangle/(f) ,$$

se $g \in k\langle X,Y\rangle$ é arbitrário, temos

$$k\langle X,Y\rangle/(f,g) \simeq (k\langle X,Y\rangle/(f))/(\overline{g})$$
$$\simeq k\langle X\rangle/(\gamma) ,$$

onde γ denota a imagem de $\overline{g} = g+(f)$ em $k\langle X\rangle$. Isto completa a demonstração, pois é imediato que a ordem de γ é a dimensão do último quociente. C.Q.D.

Observemos que o isomorfismo $k\langle X\rangle \xrightarrow{\sim} k\langle X,Y\rangle/(f)$ acima construído fornece uma série $\varphi(X)$, imagem de $\overline{Y}$ pelo isomorfismo inverso, tal que

$$f(X,\varphi(X)) = 0 .$$

Isto é uma versão algébrica formal do teorema da função implícita.

12. Proposição. $[F,G]_P$ (Veja Definição 8) satisfaz as propriedades (1),...,(7) do índice de interseção. Em particular, $[F,G]_P = (F,G)_P$ para todo par de curvas planas F,G e todo ponto $P \in \mathbb{P}^2$.

Demonstração. As propriedades (1) (5) e (6) são imediatas.

A propriedade (2) segue-se de que $f(X+x, Y+y)$ é inversível em $k\langle X,Y\rangle$ se e só se $f(x,y) \neq 0$.

Para a 4ª, observemos que se T_1, T_2 são projetividades tais que

$$(\forall F,G,P) \quad [T_i.F,\ T_i.G]_{T_iP} = [F,G]_P ,$$

então o mesmo é válido para a composta T_1T_2. Tendo em conta que toda matriz inversível é um produto de matrizes elementares (aquelas

obtidas da matriz identidade por uma operação elementar sobre as linhas), é suficiente verificar (4) quando T é uma "projetividade elementar". Suponhamos por exemplo $T_*F(X,Y,Z) = F(aX,Y,Z)$ para alguma constante $a \neq 0$; digamos $P = (1:b:c)$. Logo, $TP = (a^{-1}:b:c) = (1:ab:ac)$. Calculamos

$$(T_*F)(1,Y+ab,Z+ac) = F(a,Y+ab,Z+ac) = a^{\partial F}F(1,a^{-1}Y+b,a^{-1}Z+c)$$

Construimos um k-isomorfismo

$$\varphi\colon k\langle Y,Z\rangle \to k\langle Y,Z\rangle$$

tal que

$$\varphi(Y) = Y/a, \quad \varphi(Z) = Z/a\,.$$

Temos então

$$\varphi(F(1,Y+b,Z+c)) = F(1,a^{-1}Y+b,a^{-1}Z+c) = a^{-\partial F}(T_*F)(1,Y+ab,Z+ac)\,,$$

e analogamente para G, mostrando que φ induz um k-isomorfismo entre os anéis quocientes

$$k\langle Y,Z\rangle/(F(1,Y+b,Z+c),G(\ldots)) \simeq$$
$$\simeq k\langle Y,Z\rangle/((T_*F)(1,Y+ab,Z+ac),\ (T_*G)(\ldots).$$

Isto prova que $[F,G]_P = [TF,TG]_{TP}$ no caso considerado. Os demais casos são tratados de maneira similar.

Resta verificar (3) e (7). Em vista de (4), podemos supor $P = (0:0:1)$ e trabalhar com $f = F_*$, etc... Observe que (3) é conseqüência imediata do resultado seguinte.

13. Lema. Sejam $f,g \in k[X,Y]$. São equivalentes:

(i) f,g não admitem componente comum passando pela origem;

(ii) $k\langle X,Y\rangle/(f,g)$ tem dimensão finita;

(iii) f,g são primos relativos (i.e., não admitem fator irredutível) em $k\langle X,Y\rangle$.

Demonstração. (i) ⇒ (ii). Da hipótese, seguem-se relações em $k[X,Y]$,

$$af+bg = r(X)h \neq 0$$
$$cf+dg = s(Y)h \neq 0,$$

onde h denota o $mdc(f,g)$; em especial, $h(0,0) \neq 0$.
Em $k\langle X,Y\rangle$, podemos escrever

$$r(X)h = X^m u \ , \quad s(Y)h = Y^n v \ ,$$

com u,v inversíveis. Segue-se a inclusão de ideais

$$(X^m,Y^n) \subseteq (f,g) \quad \text{em} \quad k\langle X,Y\rangle \ .$$

Obtemos o epimorfismo ,

$$k\langle X,Y\rangle/(X^m,Y^n) \longrightarrow\!\!\!\!\!\rightarrow k\langle X,Y\rangle/(f,g) \ .$$

O 1º desses quocientes é manifestamente de dimensão finita, gerado pelas classes resíduas de X^iY^j mod. (X^m,Y^n) $(i = 0,\ldots,m-1$, $j = 0,\ldots,n-1)$, provando (ii).

(ii) ⇒ (iii) Suponhamos, por absurdo, que exista $h \in k\langle X,Y\rangle$ não inversível tal que $(f,g) \subseteq (h)$ (inclusão de ideais de $k\langle X,Y\rangle$). Levando em conta o epimorfismo

$$k\langle f,g\rangle/(f,g) \longrightarrow\!\!\!\!\!\rightarrow k\langle X,Y\rangle/(h) \ ,$$

deduzimos que $k\langle X,Y\rangle/(h)$ tem dimensão finita. Logo, existe $n \geq 1$ tal que $1,X,\ldots,X^{n-1}$ são linearmente independentes e $1,\ldots,X^n$ são dependentes módulo (h). Portanto, existe uma relação

$$X^n + a_1 X^{n-1} + \ldots + a_n = sh \ ,$$

com a_i's constantes e $s \in k\langle X,Y\rangle$. Mas $h(0,0) = 0$ implica $a_n = 0$, donde $s(0,Y) = 0$ ou $h(0,Y) = 0$. Com a 1ª alternativa, ganhamos, pois concluímos uma relação de dependência para $1,\ldots,X^{n-1}$ (porque X divide s). Com a 2ª, também ganhamos, pois se X divide h, podemos substituir h por X e é óbvio que $k\langle X,Y\rangle/(X) = k\langle Y\rangle$ tem dimensão infinita.

(iii) $\Rightarrow$ (i) Trivial.

C.Q.D.

14. Lema. Sejam $f,g \in k[X,Y]$, primos relativos. Se existir uma relação

$$af = bg \quad \text{em} \quad k\langle X,Y\rangle$$

então existe $c \in k\langle X,Y\rangle$ tal que $a = cg$. Em outras palavras, se $g|af$ em $k\langle X,Y\rangle$ então $g|a$.

Demonstração. Apelando para o fato de que um anel de séries de potências a coeficientes num corpo é fatorial, o resultado é consequência do lema anterior. Mas preferimos dar uma argumentação independente.

Da hipótese, segue-se uma relação

$$rf+sg = d(X) \neq 0 \quad \text{em} \quad k[X,Y] \ .$$

Escrevendo $d(X) = uX^m$ com u inversível em $k\langle X\rangle$, obtemos

$$\alpha f+\beta g = X^m \ , \quad \text{agora em} \quad k\langle X,Y\rangle$$

Multiplicando por a, deduzimos

$$(\alpha b+a\beta)g = aX^m.$$

Seja n o menor expoente ≥ 0 tal que existe uma relação $X^n a = cg$, para algum $c \in k\langle X,Y\rangle$. Mostremos que $n = 0$. Podemos supor que X não é fator comum de a,g em $k\langle X,Y\rangle$, bastando para isso substituir a,g por a/X^i, g/X^i para algum i. Nessas condições, X não divide g, do contrário dividiria af, e portanto dividiria f, impossível. Isso mostra que $n = 0$.

C.Q.D.

Finalmente, para provar a propriedade (7),

$$[F,G_1G_2]_P = [F,G_1]_P + [F,G_2]_P \ ,$$

podemos supor $[F,G_1]_P < \infty$ e como antes, $P = (0:0:1)$. Da inclusão de ideais $I = (f,g_1g_2) \subseteq J = (f,g_1)$, obtemos as aplicações,

$$k\langle X,Y\rangle/(f,g_2) \xrightarrow{\varphi} k\langle X,Y\rangle/I \xrightarrow{\psi} k\langle X,Y\rangle/J$$

$$\overline{p} \longmapsto g_1p+I \ ; \quad h+I \longmapsto h+J.$$

φ e ψ são k-lineares, ψ é sobrejetiva e $\psi\varphi = 0$. É imediato que a imagem de φ coincide com o núcleo de ψ. Mostremos que φ é injetiva. Se existir uma relação

$$g_1p = af + bg_1g_2 \quad \text{em} \quad k\langle X,Y\rangle \ ,$$

segue-se que g_1 divide af em $k\langle X,Y\rangle$. Visto que f,g_1 são primos relativos, segue-se do lema anterior que $g_1c = a$ para al-

gum c. Cancelando g_1, obtemos $p = cf+bg_2$, completando a prova de que φ é injetiva.

Pelo teorema do núcleo e da imagem, segue-se que a dimensão do núcleo de $\psi(= [F,G_2]_P)$, somada à dimensão da imagem de $\psi(= [F,G_1]_P)$, é igual à dimensão do domínio de $\psi(=[F,G_1G_2]_P)$.

C.Q.D.

Exercícios

7) Prove que $k\langle X\rangle$ é um domínio de ideais principais.

8) Prove a Proposição 6.

9) Complete a demonstração do Lema 9 verificando a última afirmação lá enunciada.

10) Denotemos por $\theta(f)$ a ordem de uma série $f \in k\langle X\rangle$. Prove que a) $\theta(fg) = \theta(f) + \theta(g)$; b) $\theta(f)=0 \Leftrightarrow f$ é inversível em $k\langle X\rangle$; c) $\theta(f+g) \geq \min(\theta(f), \theta(g))$, valendo a igualdade se $\theta(f) \neq \theta(g)$.

11) Sejam F,G curvas distintas com o mesmo grau. Seja P um ponto não singular de uma curva H. Mostre que

$$(F+G,H)_P \geq \min\{(F,H)_P, (G,H)_P\}.$$

Se P é singular em H, esta desigualdade pode não valer: considere uma cúbica nodal e as 2 tangentes no ponto singular.

12) Justifique a observação feita logo após o final da demonstração da Proposição 11.

13) Complete os detalhes da demonstração da Proposição 12, verificando a invariância de $[F,G]_p$ pelos tipos de "projetividades elementares" não considerados.

CAPÍTULO VII

FÓRMULAS DE PLUCKER

Vamos aplicar o teorema de Bézout e propriedades do índice de interseção para calcular o número de retas tangentes a uma curva passando por um ponto, e o número de tangentes inflexionais. O resultado é fornecido pelas fórmulas de Plucker.

1. Teorema. $d(d-1) = \check{d} + 2\delta + 3\varkappa$,

$3d(d-2) = i + 6\delta + 8\varkappa$,

onde $d \geq 2$ é o grau de uma curva irredutível F cujas únicas singularidades são δ nós e $\varkappa$ cúspides e onde d e i denotam o número de retas tangentes de F passando por um ponto $P \notin F$ e o número de retas inflexionais, respectivamente.

Supomos ainda que os pontos de inflexão, os nós e as cúspides são todos ordinários, i.e., a(s) reta(s) tangente(s) apresenta(m) contato triplo e não mais, e que o ponto P está fora das tangentes aos pontos singulares, das tangentes inflexionais e das bitangentes.

Exemplos.

(i) Para uma cônica irredutível, temos $d = \check{d} = 2$, $\delta = \varkappa = i = 0$, confirmando o fato de que podem ser traçadas 2 tangentes a uma cônica irredutível por um ponto exterior. Quando a cônica se degenera num par de retas, as 2 tangentes coincidem com a reta que liga o ponto à singularidade, "explicando" a redu-

ção causada por um ponto duplo ordinário ...

(ii) Para uma cúbica irredutível F, há 3 alternativas:

1) $\delta = \varkappa = 0$, quando então F é não singular e $\check{d} = 6$, $i = 9$; 2) $\delta = 1$, $\varkappa = 0$ e 3) $\delta = 0$, $\varkappa = 1$. Note que uma cúbica irredutível não admite bitangentes (por que?) e toda reta tangente inflexional é simples, pois a multiplicidade de interseção não pode exceder 3.

Cada uma das fórmulas no Teorema 1 é obtida intersectando F com uma certa curva auxiliar. Para a 1ª delas, consideremos a seguinte

2. Definição. A curva polar de uma curva F (de grau ≥ 2 e possivelmente redutível) relativa ao ponto $P = (x_o : y_o : z_o)$ é definida por

$$F^P := x_o F_X + y_o F_Y + z_o F_Z \ .$$

Exemplo. A curva polar do círculo $X^2+Y^2 = 1$ com respeito ao ponto (0,2) é a reta $0(2X) + 2(2Y) + 1(-2Z)$, ou ainda, $Y = 1/2$. Note que ela intersecta o círculo nos 2 pontos de contacto das tangentes que passam por (0,2).

3. Proposição - A interseção de uma curva F e sua polar F^P consiste dos pontos singulares de F e dos pontos de contato das tangentes a F passando por P.

Demonstração - Apliquemos a Proposição (VII-5). É óbvio então que todo ponto singular de F está em F^P. Seja agora Q um ponto não singular de F e pertencente a F^P. A re

ta tangente a F em Q é $XF_X(Q) + YF_Y(Q) + ZF_Z(Q)$ a qual, por hipótese, contém P.

C.Q.D.

4. Corolário. Se F é irredutível e $\partial F = d \geq 2$, então por cada ponto do plano passam no máximo, $d(d-1)$ retas tangentes a F.

Demonstração. Visto que $\partial F^P = d-1$, F e F^P não têm componente comum. O corolário resulta do teorema de Bezout.

C.Q.D.

Vamos agora fazer uma análise mais detalhada e calcular a contribuição efetiva em $F \cap F^P$ de cada ponto simples e de cada tipo de ponto singular de F.

5. Lema. A curva polar é invariante por mudança de coordenadas, i.e., se T é uma projetividade, então

$$(T_*F)^{(TP)} = T_*(F^P).$$

Demonstração. Fixados T e P, ambos os membros da igualdade são funções lineares de F. Logo, podemos supor $F = X^iY^jZ^k$, e calcular ambos os membros tomando para T uma projetividade elementar. Alternativamente, pode-se usar a regra da cadeia.

C.Q.D.

6. Lema Seja $Q \in F \cap F^P$. Então, nas condições do Teorema 1, temos

$$(F,F^P)_Q = \begin{cases} 1 & \text{se } Q \text{ é um ponto simples de } F; \\ 2 & \text{se } Q \text{ é um ponto duplo ordinário de } F; \\ 3 & \text{se } Q \text{ é uma cúspide ordinária de } F. \end{cases}$$

Demonstração. Pelo lema anterior, podemos supor $Q = (0:0:1)$.

Suponhamos F lisa em Q. Podemos tomar $Y = 0$ para tangente, i.e., $f = F_*$ da forma $Y + aX^2 + bXY + \ldots$. Segue-se que $P = (x_o:0:z_o)$ com $x_o \neq 0$, pois $P \notin F$. A curva polar é então $2ax_oX + cY + \ldots$ (grau superior). Visto que Y não é tangente inflexional, temos $a \neq 0$. Logo F e F^P têm tangentes distintas na origem, donde o índice de interseção é 1 (V-13).

No 2º caso, podemos supor f da forma

$$XY + (\text{grau superior}).$$

Visto que P está fora das tangentes aos pontos singulares, temos $P = (x_o:y_o:z_o)$ com $x_oy_o \neq 0$. A polar tem então o aspecto

$$x_oY + y_oX + \ldots ,$$

sendo assim transversal às 2 tangentes de F em Q e portanto $(F,F^P)_Q = m_Q(F) = 2$ (por V-13).

Para o 3º caso, escrevemos

$$f = Y^2 + aX^3 + \ldots,$$

com $a \neq 0$ (senão $(Y,f)_0 > 3$). Temos $P = (x_o:y_o:z_o)$, com $y_o \neq 0$. Aplicando uma projetividade que fixe $(0:0:1)$ e $(1:0:0)$ e mande P em $(0:1:0)$, temos que a reta $Y = 0$ é dei-

xado invariante. Logo, f permanece na forma apresentada, e a curva polar é dada por

$$f^P = 2Y + (\text{grau superior}).$$

Empregando com argúcia a propriedade (6) do índice de interseção (VI.2) obtemos, finalmente,

$$(f,f^P)_0 = (aX^3+\ldots,2Y+\ldots)_0 = 3.$$

C.Q.D.

A 1ª fórmula do Teorema 1 decorre da Proposição 2 e do Lema 5.

Para provarmos a 2ª fórmula, consideremos a seguinte.

7. Definição. A curva hessiana de uma curva F de grau ≥ 3 é definida por

$$h(F) = \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{XY} & F_{YY} & F_{YZ} \\ F_{XZ} & F_{YZ} & F_{ZZ} \end{vmatrix}.$$

Exemplos.

1) Se $F = ZY^2-X^3$ (cúbica cuspidal), temos

$$h(F) = \begin{vmatrix} -6X & 0 & 0 \\ 0 & 2Z & 2Y \\ 0 & 2Y & 0 \end{vmatrix} = 24XY^2$$

Temos $F \cap h(F) = \{(0:1:0), (0:0:1)\}$. No 1º ponto, a multiplicidade da interseção é 1 e no 2º é 8. A tangente a F no ponto

$(0:1:0)$ é $Z = 0$, que é inflexional.

2) Se $F = ZY^2-ZX^2+X^3$ (cúbica nodal), temos $h(F) =$
$= -8(Z(X^2-Y^2)+3XY^2)$. O ponto singular de F absorve 6 interseções com $h(F)$. Nos 3 pontos restantes, $(0:1:0)$ e $(12:\pm i4\sqrt{3}: 9)$, o índice de interseção vale 1. As tangentes a F nesses 3 últimos pontos são inflexionais (Leitor: verifique!).

8. Proposição. $F \cap h(F)$ consiste dos pontos singulares e dos pontos de inflexão de F. Nas condições do Teorema 1, se $Q \in F \cap h(F)$ então

$$(F,h(F))_Q = \begin{cases} 1 & \text{se } Q \text{ é um ponto de inflexão ordinário;} \\ 6 & \text{se } Q \text{ é um nó ordinário;} \\ 8 & \text{se } Q \text{ é uma cúspide ordinária.} \end{cases}$$

Demonstração. O procedimento é análogo ao tratamento dado à curva polar: primeiro mostramos que $h(F)$ é invariante por mudança de coordenadas. Com esta liberdade, posicionamos o ponto Q na origem, e escolhemos a(s) tangente(s) como no caso anterior.

Para provar a relação

$$T_*(h(F)) = h(T_*F) \quad ,$$

observamos que a matriz hessiana de T_*F é obtida da matriz hessiana de F multiplicando à esquerda e à direita pela matriz de T^{-1} e sua transposta. Como o determinante de um produto de matrizes é igual ao produto dos determinantes, concluimos que os po

linômios $T_*(h(F))$ e $h(T_*F)$ diferem apenas por um múltiplo constante $\neq 0$, definindo a mesma curva.

Suponhamos agora $Q = (0:0:1) \in F \cap h(F)$. Podemos escrever F na forma

$$AZ^{d-1}Y + Z^{d-2}(BX^2+CXY+DY^2) + \dots .$$

A condição $Q \in h(F)$ é equivalente ao anulamento do determinante

$$\begin{vmatrix} 2B & C & 0 \\ C & 2D & (d-1)A \\ 0 & (d-1)A & 0 \end{vmatrix} = -2(d-1)^2 A^2 B .$$

Logo, ou $A = 0$ - caso em que $(0:0:1)$ é singular em F, ou $A \neq 0$ e $B = 0$ - caso em que $(0:0:1)$ é um ponto de inflexão. Calculemos o índice de interseção em cada caso.

(i) Cúspide ordinária. Escrevemos F na forma

$$Z^{d-2}Y^2 + Z^{d-3}(AX^3+BX^2Y+CXY^2+DY^3) + \dots ,$$

com $A \neq 0$. Procuramos os termos de menor grau de $h = h(F)_*$,

$$h = \begin{vmatrix} 6AX + 2BY + \dots & & \\ 2BX + 2CY + \dots & 2+2cX+6DY + \dots & \\ (d-3)(3AX^2+\dots) & 2(d-2)Y + \dots & (d-3)((d-2)Y^2+(d-4)AX^3+\dots) \end{vmatrix} ,$$

encontrando

$$h = Y^2(aX+bY) + cX^4 + \dots$$

onde as reticências indicam termos irrelevantes, e a,b,c são constantes, com

$$a = 12A(d-2)(d-3) ,$$

$$c = 12A^2(d-3)(d-4) - 18A^2(d-3)^2 .$$

Calculando o índice de interseção, pondo $f = F_*$, $g = h-(aX+bY)f$, vem

$$\begin{aligned}(f,h)_Q &= (f,g)_Q \\ &= (Y^2+AX^3+\ldots,(c-aA)\,X^4+Y(\ldots)+\ldots)_Q \\ &= 2.4 = 8\end{aligned}$$

porque $c \neq aA$ implica que Y não é tangente a g. Note que $c \neq aA$ para $d \geq 4$. O caso $d = 3$ foi essencialmente tratado no exemplo anterior.

(ii) nó ordinário. Temos

$$F = Z^{d-2}XY + Z^{d-3}(AX^3 + BY^3 +\ldots) + \ldots ,$$

com $AB \neq 0$ (senão o contato de uma reta tangente ao nó seria ao menos quádruplo). Calculando $h = h(F)_*$ encontramos

$$h = cXY + aX^3 + bY^3 +\ldots,$$

com

$$\begin{aligned}c &= 2 - (d-2)(d-3) \\ a &= A(6-(d-3)(d-4) \\ b &= B(6-(d-3)(d-4)) .\end{aligned}$$

Pondo $f = F_*$, podemos computar o índice de interseção ,

$$\begin{aligned}(f,h)_0 &= (f,\ h-cf)_0 \\ &= (XY +\ldots,\ (a-cA)\,X^3+(b-cB)Y^3 +\ldots)_0 \\ &= 2.3 = 6 ,\end{aligned}$$

pois $(a-cA)(b-cB) \neq 0$ implica que X,Y não são tangentes a $h-cf$.

(iii) ponto de inflexão ordinário. Fica como exercício para o leitor.

C.Q.D.

Completamos portanto a demonstração das 2 fórmulas de Plücker enunciadas no Teorema 1. A verificação que fizemos para a contribuição de cada tipo de ponto em $F \cap h(F)$ e $F \cap F^P$, sugere que as fórmulas podem ser generalizadas para abranger singularidades mais complicadas. Encorajamos o leitor a calcular alguns outros casos nos exercícios.

Há 2 outras fórmulas de Plücker que gostaríamos de mencionar:

$$\check{d}(\check{d}-1) = d + 2\beta + 3i ,$$

$$3\check{d}(\check{d}-2) = d + 6\beta + 8i ,$$

onde β denota o número de bitangentes. Elas são, de certa maneira, duais das fórmulas do Teorema 1.

Precisamente, associemos à reta $aX+bY+cZ = 0$ o ponto $(a:b:c)$ no plano projetivo dual $\check{\mathbb{P}}^2$. Denotando por A,B,C coordenadas homogêneas em $\check{\mathbb{P}}^2$, vemos que, dualmente, cada ponto $(x:y:z) \in \mathbb{P}^2$ corresponde a uma reta $xA+yB+zC$ em $\check{\mathbb{P}}^2$, justamente a que consiste dos pontos que representam as retas de $\mathbb{P}^2$ contendo $(x:y:z)$ ...

É razoável se esperar, e de fato pode-se demonstrar, que as retas tangentes a uma curva irredutível $F \subset \mathbb{P}^2$ são parametrizadas por uma curva (igualmente irredutível) $\check{F} \subset \check{\mathbb{P}}^2$, chamada curva dual de F. Por exemplo $AX+BY+C$ é tangente à parábola $Y=X^2$

se e só se $A^2-4BC = 0$.

Ora, sabemos que o grau de $\check{F}$ é o número de pontos da interseção de $\check{F}$ com uma reta genérica de $\mathbb{P}^2$; dualmente, isto corresponde ao número $d^\vee$ de retas tangentes a F passando por um ponto genérico de $\mathbb{P}^2$. Demonstra-se também que $(F^\vee)^\vee = F$, e que, na correspondência

$$(\text{tangente de } F) \longleftrightarrow (\text{ponto de } \check{F}),$$

as tangentes inflexionais correspondem às cúspides de $\check{F}$ e as bitangentes aos pontos duplos. Assim, as 2 fórmulas acima podem ser provadas permutando os papéis de $F, \check{F}$.

Os números $d, d^\vee, \delta, \beta, \varkappa, i$ são chamadas de <u>características</u> de Plücker da curva F. As equações de Plucker fornecem uma condição necessária para que 6 números sejam as características de uma curva. Sabe-se que essa condição não é suficiente: não existe curva irredutível com $d = d^\vee = 14$, $\delta = \beta = 0$, $\varkappa = i = 56$. É uma questão ainda não resolvida quais outras condições necessárias viriam garantir que uma lista de 6 inteiros $d, \ldots, \varkappa, i$ ocorra efetivamente como características de uma curva.

<u>Exercícios</u>

1) Verifique as fórmulas de Plücker para a trissectriz Maclaurin, para o folium de Descartes e para a cissóide de Diocles.

2) Mostre que os 3 nós da lemnisc ta não são ordinários. Calcule o nº de interseções absorvidas por cada um desses

nós com a hessiana.

3) Mostre que a curva

$$Y^2-3X(X^2+Y^2) - (X^2+Y^2)^2 = 0$$

tem 2 bitangentes e 4 pontos de inflexão.

4) Mostre que a reta que liga 2 pontos de inflexão de uma cúbica irredutível não cuspidal intersecta a cúbica em um 3º ponto de inflexão.

5) Prove que uma cúbica real não singular possui exatamente 3 pontos da inflexão reais e 3 pares de pontos de inflexão complexo-conjugados.

6) Prove que os pontos de contato de tangentes a uma cúbica não singular por um ponto exterior pertencem a uma cônica. Em que caso é esta cônica degenerada?

7) Investigue os índices de interseção de uma curva com sua polar relativa a um ponto sobre a curva.

8) Prove que um ponto m-uplo ordinário absorve $m(m-1)$ interseções de uma curva com sua polar com respeito a um ponto convenientemente situado.

9) Prove que toda componente comum a uma curva e sua hessiana é uma reta.

10) Investigue a relação entre $h(h(F))$ e F para uma cúbica não singular F.

11) Para cada $d \geq 4$ construa uma curva F não singular cujas tangentes inflexionais são todas ordinárias.

12) Mostre que a dual de uma cônica não degenerada

$$F = a_{11}X^2+a_{22}Y^2+a_{33}Z^2+2(a_{12}XY+a_{13}XZ+a_{23}YZ)$$

é a cônica

$$F = a'_{11}A^2+a'_{22}B^2+a'_{33}C^2+2(a'_{12}AB+a'_{13}AC+a'_{23}BC)$$

onde a matriz simétrica (a'_{ij}) é a inversa de (a_{ij}).

13) Verifique $F = (\check{F})^{\vee}$ para $F = ZY^2-X^3$ e $F = Z(Y^2-X^2)+X^3$.

Estude a correspondência entre os pontos singulares e as tangentes excepcionais.

14) "Se de um ponto P traçam-se tangentes às cônicas de um feixe $F_t := F_0+tF_\infty$, então o lugar dos pontos de contato é uma cúbica". Determine condições precisas sobre o ponto P e o par de cônicas F_0, F_∞ que tornem verdadeira essa afirmação.

15) Qunatas tangentes a uma cúbica F podem ser traçadas por um ponto de F?

CAPÍTULO VIII

CURVAS RACIONAIS

Introduzimos neste capítulo os conceitos de função regular e função racional sobre uma curva. Servimo-nos das curvas racionais como itinerário e motivação. Demonstramos o Teorema de Lüroth e finalizamos estabelecendo um critério numérico de racionalidade.

§1. Curvas racionais afins

1. Definição. Uma curva afim irredutível f é racional se existir um par de funções racionais $x(T)$, $y(T)$, não ambas constantes, tal que $f(x(T), y(T)) = 0$ em $k(T)$. O par $x(T)$, $y(T)$ é chamado uma parametrização racional (ou simplesmente parametrização.)

Exemplos.

1) Toda reta é racional, admitindo parametrização da forma $x(T) = aT+b$, $y(T) = cT+d$, com a ou $c \neq 0$.

2) O círculo $X^2+Y^2 = 1$ é racional, com parametrização obtida da figura:

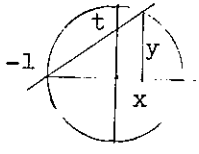


Fig. 25

Intersectamos a reta $Y = t(X+1)$ com o círculo, encontrando o ponto variável $(x(t),y(t))$ onde

$$x(t) = (1-t^2)/(1+t^2)$$

$$y(t) = 2t/(1+t^2) .$$

Intuitivamente, uma curva é racional se for possível desenhá-la sem se levantar o lápis do papel. Por isso, o termo unicursal é também empregado. No entanto, esta descrição é por vezes enganosa. Por exemplo, embora o traço real de $X^4+Y^4 = 1$ admita essa caracterização, podemos mostrar que esta curva não é racional.

Com efeito, admitamos, por absurdo, a existência de uma parametrização

$$x = p(T)/r(T)$$

$$y = q(T)/r(T) ,$$

onde p,q,r são polinômios sem fator comum (aos 3), $r \neq 0$, e digamos q não constante. Derivando a relação

$$x^4 + y^4 = 1 ,$$

vem

$$\dot{x}x^3 + \dot{y}y^3 = 0 .$$

Consideremos o sistema linear

$$\begin{cases} xu + yv = 1 \\ \dot{x}u + \dot{y}v = 0 . \end{cases}$$

Visto que $\omega := x\dot{y}-\dot{x}y \neq 0$ (senão x/y seria constante), o sistema admite a solução única

$$u = \dot{y}/\omega, \quad v = -\dot{x}/\omega .$$

Mas $u = x^3$ e $v = y^3$ são soluções. Daí vem

$$\dot{y} = \omega x^3, \quad \dot{x} = -\omega y^3.$$

Substituindo em termos de $p,q,r,$ e simplificando, vem

$$r^3(r\dot{q} - q\dot{r}) = (p\dot{q} - q\dot{p})p^3$$

$$r^3(r\dot{p} - p\dot{r}) = -(p\dot{q} - q\dot{p})q^3.$$

Daí se deduz que r^3 divide $p\dot{q} - q\dot{p}$. Dividindo e estimando graus, obtemos

$$3\partial p \leq \partial r + \partial q - 1$$

$$3\partial q \leq \partial r + \partial p - 1$$

$$3\partial r \leq \partial p + \partial q - 1$$

$$0 \leq \partial p + \partial q + \partial r \leq -3 , \quad \text{absurdo!}$$

Exercícios

1) Seja $f = f_m + f_{m+1}$ uma curva afim irredutível, onde f_i é homogêneo de grau i. Mostre que f é racional. Obtenha uma parametrização para $X^2Y(X-Y) + (X+Y)^2(X-2Y)^2(X+2Y)$ empregando um feixe conveniente de retas.

2) Seja C uma cônica definida sobre o corpo dos números racionais. Prove que se C admitir um ponto com coordenadas racionais então existirá uma infinidade de tais pontos. Determine todas as soluções inteiras da equação $X^2+Y^2 = Z^2$. Idem para $X^2+Y^2 = 3Z^2$.

3) Mostre que $X^m+Y^m = 1$ é racional se e só se $m = 1$ ou 2.

§2. Funções regulares e funções racionais

Quando uma curva é racional, a cada valor do parâmetro (salvo um número finito que anula o denominador) corresponde um ponto bem definido da curva. Mas pode ocorrer que cada ponto da curva seja atingido por valores distintos do parâmetro, e.g., $x = T^2$, $y = 1/T^2$ (repete 2 vezes cada ponto da hipérbole). Neste exemplo, vemos que é possível substituir T por outra variável. Fazendo $U = T^2$, obtemos a nova parametrização $x = U$, $y = 1/U$. Mostraremos mais adiante que é sempre possível escolher uma boa parametrização, para a qual a correspondência

(valor do parâmetro) $\longleftrightarrow$ (ponto da curva)

é bijetiva, salvo um nº finito de exceções. Para isto, será conveniente introduzir algumas definições.

2. Definição. Seja $C \subset \mathbb{A}^2$ uma curva afim irredutível, de equação $f = 0$. Uma aplicação $\varphi: C \to \mathbb{A}^1$ é chamada regular ou polinomial se for igual à restrição de uma função polinomial $\mathbb{A}^2 \to \mathbb{A}^1$, i.e., se existir um polinômio $p(X,Y)$ tal que $\varphi(x,y) = p(x,y)$ para $(x,y) \in C$.

O conjunto das funções regulares de C forma um anel, que denotamos por $A(C)$. Por definição, temos um epimorfismo

$$k[X,Y] \to A(C)$$

que associa a cada polinômio, considerado como função $\mathbb{A}^2 \to \mathbb{A}^1$, a sua restrição a C.

Usualmente denotaremos pelo mesmo símbolo 3 coisas distintas: 1º) o polinômio $p \in k[X,Y]$; 2º) a função polinomial $p: \mathbb{A}^2 \to \mathbb{A}^1$; e 3º) a sua restrição a C. Não há confusão possível para as 2 primeiras, pois sendo k um corpo infinito, um polinômio é determinado pela função associada. Se necessário, escreveremos $\overline{p}$ para distinguir a restrição a C.

3. Lema. $A(C)$ é um domínio isomorfo a $k[X,Y]/(f)$.

Demonstração. Um polinômio se anula sobre a curva C somente se for múltiplo de f (Proposição II.1). Assim, o núcleo do epimorfismo de restrição é justamente o ideal (f), o qual é um ideal primo pois f é irredutível e $k[X,Y]$ é fatorial.

C.Q.D.

Exemplos.

1) Se ℓ é uma reta, então $A(\ell)$ é isomorfo a um anel de polinômios em uma variável. Precisamente, se ℓ é dada por $Y = aX+b$, a aplicação

$$\begin{aligned} k[X,Y] &\to k[X] \\ h &\mapsto h(X,aX+b) \end{aligned}$$

é um epimorfismo com núcleo (f), onde $f = Y-(aX+b)$. Logo,

$$A(\ell) \simeq k[X,Y]/(f) \simeq k[X].$$

2) Se C é a hipérbole $XY = 1$, temos

$$A(C) \approx [X^m p(X) \mid m \in \mathbb{Z} \ , \ p(X) \in k[X]];$$

Isto é, A(C) se identifica com o anel B das funções racionais cujos denominadores são potências de X. Com efeito, temos um homomorfismo

$$k[X,Y] \longrightarrow k(X)$$

$$h(X,Y) \longmapsto h(X,1/X)$$

cuja imagem é justamente o anel B acima descrito, e cujo núcleo é (XY-1). (Leitor: verifique!).

4. Definição. O corpo das funções racionais de uma curva afim irredutível C é o corpo de frações K(C) do domínio A(C).

Cada elemento de K(C) pode ser escrito na forma $\overline{p}/\overline{q}$, onde $\overline{p},\overline{q}$ denotam funções polinomiais restritas a C com $\overline{q} \neq 0$. Duas tais expressões $\overline{p}/\overline{q}$, $\overline{r}/\overline{s}$ representam a mesma função racional em K(C) se e só se a função regular $\overline{p}\,\overline{s}-\overline{q}\,\overline{r}$ é nula em C, ou equivalentemente, o polinômio ps-qr é múltiplo de f.

Dizemos que a função racional $\varphi \in K(C)$ é regular ou que está definida no ponto $P \in C$ se φ admitir uma representação p/q, com $p,q \in A(C)$ e $q(P) \neq 0$.

Denotemos por C_φ o conjunto dos pontos de C onde φ é

regular. Temos então definida uma aplicação, ainda denotada $\varphi: C_\varphi \to \mathbb{A}^1$, justificando a nomenclatura "função racional" com que designamos os elementos de $K(C)$. Observemos que, em geral, C_φ é o complementar de um subconjunto finito de C. (Leitor: justifique).

Uma função regular obviamente é uma função racional que está definida em todos os pontos de C. A recíproca é o conteúdo da seguinte

5. Proposição. *Se $\varphi \in K(C)$ é uma função racional regular em cada ponto de C então $\varphi \in A(C)$, i.e., φ é regular.*

Demonstração. Seja

$$I = \{q \in A(C) \mid q\varphi \in A(C)\}.$$

Pretendemos mostrar que a função constante 1 está em I. É fácil ver que I é um ideal de $A(C)$. Portanto, supondo, por absurdo, que $1 \notin I$, então I tem que estar contido em algum ideal maximal de $A(C)$. Ora, cada ideal maximal de $A(C) = k[X,Y]/(f)$ corresponde a um ideal maximal de $k[X,Y]$ que contém f. Pelo Nullstellensatz, concluiríamos que existe $P \in C$ tal que $q(P) = 0$ para todo $q \in I$, contradizendo a regularidade de φ em P.

C.Q.D.

Exemplo. Seja C o círculo $X^2+Y^2 = 1$, e seja $\varphi = \frac{\overline{Y}-1}{\overline{X}}$. Esta função é certamente regular em cada $(x,y) \in C$ com $x \neq 0$. No ponto $(0,1)$, φ também é regular, pois temos a nova

representação $\frac{\overline{X}}{\overline{Y}+1} = \frac{\overline{Y}-1}{\overline{X}}$. Mas no ponto $(0,-1)$ φ não é regular. (Leitor: por que?).

Este exemplo mostra que uma função racional pode não admitir representação na forma p/q que funcione em toá s os pontos em que ela é regular. A propriedade da fatorização única em $A(C)$ é o critério responsável pela existência de uma tal representação. No exemplo acima, $A(C)$ não é um domínio fatorial.

6. Proposição. C é uma curva racional se e somente se seu corpo de funções racionais $K(C)$ é k-isomorfo a um subcorpo de $k(T)$ (= corpo das funções racionais na variável T).

Demonstração. Suponhamos $K(C) \subset k(T)$. Sejam $x(T)$, $y(T)$ as imagens de $\overline{X},\overline{Y} \in K(C)$ em $k(T)$. Se $x(T)$ for constante, então $\overline{X}$ também é, acarretando $X-a \in (f)$ para alguma constante $a \in k$. Daí, visto que f, a equação de C, é irredutível, concluimos que $f = X-a$ (a menos de fator constante). Logo, $\overline{Y}$ não é constante, mostrando que $x(T)$ ou $y(T)$ é não constante. Por fim, visto que f é zero em $A(C)$, concluimos que $f(x(T),y(T)) = 0$ em $k(T)$, ou seja, obtivemos uma parametrização de C.

Reciprocamente, dada uma parametrização $x(T)$, $y(T) \in k(T)$, temos definido um k-homomorfismo

$$k[X,Y] \longrightarrow k(T)$$

$$h(X,Y) \longmapsto h(x(T),y(T))$$

que anula f. Afirmamos que o núcleo I coincide com (f). Com

efeito, se existe $g \in I$ não divisível por f, por (II-1) deduzimos a existência de polinômios $c(X)$, $d(Y)$ em I, não nulos. Daí $k[X,Y]/(c,d)$ tem dimensão finita, e portanto sua imagem $k[X,Y]/I \approx k[x(T), y(T)]$, a k-subálgebra de $k(T)$ gerada por $x(T)$, $y(T)$, também é um k-espaço vetorial de dim-finita. Em particular, $1, x = x(T), x^2, \ldots, x^n$ são linearmente dependentes/k para algum inteiro $n \geq 1$. Logo, x é algébrico sobre k, e portanto $x \in k$. Analogamente, $y(T) \in k$, contradizendo a hipótese de que ao menos uma dessas funções era não constante.

C.Q.D.

Suponhamos que a curva C seja racional. A inclusão de corpos,

$$K(C) \subset k(T)$$

fornecida pela proposição anterior é dada pela substituição $X \mapsto x(T)$, $Y \mapsto y(T)$ em $\varphi(X,Y) = p(X,Y)/q(X,Y)$, elemento de $K(C)$. Esta substituição produz a função racional $p(x(T), y(T))/q(x(T), y(T))$ em $k(T)$, a qual está bem definida porque o denominador é $\neq 0$ uma vez que f não divide q.

Exercícios

4) Mostre que toda função regular não constante $\varphi \in A(C)$ admite no máximo um número finito de zeros, i.e., pontos $P \in C$ onde $\varphi(P) = 0$.

5) Seja C o gráfico de uma função polinomial $Y = p(X)$. Mostre que $A(C)$ é isomorfo a $k[X]$. Reciprocamente, se

$A(C)$ é k-isomorfo a um anel de polinômios $k[T]$, será C igual ao gráfico de uma função polinomial, a menos de uma mudança de coordenadas?

6) Mostre que $k[X,Y]/(XY-1)$ (o anel das funções regulares da hipérbole) não é isomorfo a $k[X]$.

7) Mostre que, se C é uma cônica irredutível afim, então $A(C)$ é k-isomorfo a $k[X,Y]/(XY-1)$ ou a $k[X]$. A qual desses corresponde o círculo $C: X^2+Y^2 = 1$?

8) Seja C uma curva irredutível e seja $\varphi \in K(C)$ uma função racional não constante. Mostre que o homomorfismo $k[T] \to K(C)$ definido por $p(T) \longmapsto p(\varphi)$ é injetivo e se estende a um isomorfismo do corpo das funções racionais $k(T)$ sobre o subcorpo $k(\varphi) \subset K(C)$.

§3. O teorema de Lüroth

7. Definição. Dizemos que a parametrização $x(T)$, $y(T)$ da curva C é boa se a inclusão

$$K(C) \subset k(T)$$
$$\varphi(X,Y) \longmapsto \varphi(x(T), y(T))$$

é sobrejetora.

Isto equivale a requerer que exista $\psi(X,Y) \in K(C)$ tal que

$$\psi(x(T),y(T)) = T \ .$$

Exemplo. A parametrização do círculo obtida anteriormente,

$$x(T) = (1-T^2)/(1+T^2)$$

$$y(T) = 2T/(1+T^2)$$

é boa, pois tomando $\psi = Y/X+1$ calculamos $\psi(x(T),y(T)) = T$.

8. Proposição. Toda curva racional admite uma boa parametrização.

Este resultado é consequência do

9. Teorema de Lüroth. Seja K um subcorpo de $k(T)$. Se K contém uma função não constante (i.e. $K \neq k$) então existe $T' \in k(T)$ tal que $K = k(T')$.

Em outras palavras, existe uma função $T' = T'(T)$ tal que cada elemento de K é da forma $\varphi(T')$ para alguma $\varphi \in k(T)$.

Antes de procedermos com a demonstração do Teorema de Lüroth, é instrutivo examinar, por exemplo, o subcorpo $K = k(T^4,T^6)$ gerado pelas funções T^4,T^6. Tomemos $T' = T^6/T^4 = T^2 \in K$. Agora note que $T^4 = (T^2)^2$, $T^6 = (T^2)^3$, donde $K = k(T^2)$.

Demonstração do Teorema de Luroth. Observemos que $k(T)$ é uma extensão algébrica de K. Com efeito, se $\varphi = a(T)/b(T) \in K$ é não constante, com $a,b \in k[T]$, vemos que T é raiz do polinômio $a(X)-\varphi b(X) \in K[X]$. Logo, T é algébrico/K. Seja

$$p(X,T) = a_o(T)X^m + \ldots + a_m(T) ,$$

o polinômio mínimo de T sobre K, onde $a_j \in k[T]$, $a_o \neq 0$,

$a_j/a_o \in K$. Podemos supor $mdc(a_o,\ldots,a_m) = 1$. Seja i tal que

$$n = \partial a_i(T) \geq \partial a_j(T) \quad \text{para} \quad j = 0,\ldots,m \ .$$

Escolha j tal que $a_i/a_j \notin k$. Definamos $T' = a_i/a_j$. Note que o polinômio

$$T' \, a_j(X) - a_i(X) \in K[X]$$

anula T e é de grau n. Logo, podemos estimar o grau da extensão,

$$[k(T): k(T')] \leq n.$$

Seja agora

$$q(X,T) = a_j(X) \, a_i(T) - a_j(T) \, a_i(X) \ .$$

Temos $q(T,T) = 0$. Segue-se que $p(X,T)$ divide $q(X,T)$ em $k[X,T]$, digamos

$$p(X,T) \, r(X,T) = q(X,T) \ .$$

Comparando graus com respeito à variável T,

$$\partial_T p = n \leq \partial_T p + \partial_T p + \partial_T r \leq n.$$

Logo, r independe de T. Agora, $r = r(X)$ divide $q(X,T)$; por simetria (vide definição de q!) $r(T)$ também é fator de $q(X,T)$. Portanto, $r(T)$ divide $p(X,T)$. Mas por construção, $mdc(a_o,\ldots,a_m) = 1$, donde $r(T)$ é constante. Logo $m = n$ e concluimos a demonstração observando as desigualdades,

$$n \geq [k(T): k(T')] \geq [k(T):K] = m \ ,$$

donde $k(T') = K$.

C.Q.D.

Para obtermos uma boa parametrização a partir de uma dada, $x(T)$, $y(T)$, basta aplicar o Teorema de Lüroth ao subcorpo $k(x(T), y(T)) \subset k(T)$. Deduzimos $k(x(T), y(T)) = k(T')$ e tomamos T' como novo parâmetro.

Exercícios

9) Determine a equação da curva parametrizada por $x(T) = T^6-T^2+1$, $y(T) = T^2/(1+T^2)$. Ache $T' \in K = k(x(T),y(T))$ tal que $K = k(T')$.

10) Sejam $x,y \in k(T)$, não ambos constantes. Mostre que existem $u,v \in k(T)$ tais que a aplicação $t \longmapsto (u(t),v(t))$ é injetiva e sua imagem coincide com a imagem de $t \longmapsto (x(t),y(t))$, exceto para um número finito de pontos. Se x,y são polinômios, é possível encontrar u,v polinômios?

§4. Curvas racionais projetivas

Observemos que a parte inicial da demonstração do Teorema de Lüroth mostra, mais geralmente, que se $x(T),y(T) \in k(T)$ não são ambas constantes, então existe um polinômio $f(X,Y)$ não constante tal que $f(x(T),y(T)) = 0$. É claro que podemos supor tal f irredutível. Seja ψ a aplicação dada por $\psi(t) = (x(t),y(t))$. Esta aplicação está definida no complementar de um número finito

de pontos de $\mathbb{A}^1$. A imagem de ψ está contida na curva definida por f, podendo porém omitir alguns pontos.

Exemplo. Consideremos a parametrização do círculo,

$$\psi(t) = \left(\frac{1-t^2}{1+t^2}\ ,\ \frac{2t}{1+t^2}\right) .$$

O ponto $(-1,0)$ está fora da imagem. (Verifique!). Se $k = \mathbb{R}$ ou $\mathbb{C}$, podemos imaginar $t \to \infty$, e é claro que $\lim_{t\to\infty} \psi(t) = (-1,0)$. Mas em qualquer caso, temos um procedimento algébrico para fazer $t \to \infty$: consideramos $\mathbb{A}^1 \subset \mathbb{P}^1$, como de hábito, identificando t com $(t:1)$, e procedemos analogamente para $\mathbb{A}^2 \subset \mathbb{P}^2$. Eis agora o passe de mágica: a aplicação

$$\tilde{\psi}: \mathbb{P}^1 \longrightarrow \mathbb{P}^2$$

$$(t:u) \longmapsto (u^2-t^2: 2tu: u^2+t^2)$$

coincide com ψ no domínio comum, e fornece o valor

$$\tilde{\psi}(\infty) \overset{\text{def}}{=} \tilde{\psi}(1:0) = (-1:0:1).$$

Observe que $\tilde{\psi}$ extende ψ também aos pontos $t = \pm\sqrt{-1}$, em que ambas as coordenadas de $\psi(t)$ não estavam definidas.

10. Definição. Uma aplicação $\psi: \mathbb{P}^m \to \mathbb{P}^n$ é dita regular ou polinomial se existirem polinômios homogêneos do mesmo grau, $\psi_0,\ldots,\psi_n \in k[X_0,\ldots,X_m]$ tais que, $\forall\ P = (x_0:\ldots:x_m) \in \mathbb{P}^m$,

$$\psi(P) = (\psi_0(P):\ldots:\psi_n(P)).$$

Note que, em particular, os polinômios $\psi_0,\ldots,\psi_n$ são

proibidos de admitir zero comum $P \in \mathbb{P}^m$. O requerimento de que sejam homogêneos e do mesmo grau se justifica para garantir que $(\psi_o(P):\ldots:\psi_n(P))$ independe das coordenadas homogêneas de P.

Deixamos a cargo do leitor a demonstração da proposição seguinte, generalizando a discussão feita acima.

11. Proposição. Sejam $x_1(T),\ldots,x_n(T)$ funções racionais. Seja $u \subset A^1$ o maior subconjunto em que estão todas definidas. Então existe uma única aplicação polinomial $\psi: \mathbb{P}^1 \to \mathbb{P}^n$ tal que

$$\psi(t:1) = (x_1(t):\ldots:x_n(t):1) \quad \forall\, t \in u\ .$$

Este resultado mostra que o conceito de parametrização racional de uma curva plana pode ser substituído, com vantagem, pelo conceito de aplicação polinomial (não constante) $\mathbb{P}^1 \to \mathbb{P}^2$. Com efeito, com este último ponto de vista, por um lado desaparecem as restrições impostas à variação do parâmetro e, por outro, a imagem agora é completa no seguinte sentido:

12. Proposição. A imagem de uma aplicação polinomial $\psi: \mathbb{P}^1 \to \mathbb{P}^2$ não constante é uma curva projetiva irredutível.

Demonstração. Sejam ψ_o, ψ_1, $\psi_2 \in k[X_o,X_1]$ coordenadas de ψ. Se $\psi_2 = 0$, mostremos que $\psi(\mathbb{P}^1)$ é igual à reta no infinito $Z = 0$. Com efeito, dado $Q = (y_o:y_1:0) \in \mathbb{P}^2$, o polinômio $y_1\psi_o - y_o\psi_1$ admite raiz $P = (x_o:x_1) \in \mathbb{P}^1$, i.e., $y_1\psi_o(x_o:x_1) = y_o\psi_1(x_o:x_1)$, donde $\psi(P) = Q$.

Suponhamos agora $\psi_2 \neq 0$. Ponhamos

$$x(T) := \psi_0(T,1)/\psi_2(T,1)$$

$$y(T) := \psi_1(T,1)/\psi_2(T,1) \ .$$

Ao menos uma delas é não constante. Seja f a curva racional que elas parametrizam (cf. observação na pág. 133. Seja $F = f^*$. Provaremos que $F = \psi(\mathbb{P}^1)$.

Seja

$$\tilde{F}(T,U) = F(\psi_0(T,U),\ \psi_1(T,U),\ \psi_2(T,U)) \ .$$

É fácil ver que $\tilde{F}(T,U)$ é um polinômio homogêneo nas indeterminadas T,U. Como $\tilde{F}(T,1) = 0$, segue-se que $\tilde{F}(T,U) = 0$, ou seja, F contém $\psi(\mathbb{P}^1)$.

Para completar a demonstração, analisemos a condição para que um ponto $(y_0:y_1:y_2) \in \mathbb{P}^2$ esteja em $\psi(\mathbb{P}^1)$. Supondo $y_2 \neq 0$, a condição

$$(y_0:y_1:y_2) = (\psi_0(t,u):\ \psi_1(t,u):\ \psi_2(t,u))$$

se exprime na existência de uma solução $(t:u) \in \mathbb{P}^1$ para o sistema de equações

$$\begin{cases} y_2\psi_0(T,U) - y_0\psi_2(T,U) = 0 \\ y_2\psi_1(T,U) - y_1\psi_2(T,U) = 0 \end{cases}$$

Ponhamos $G_i = Y_2\psi_i - Y_i\psi_2$, $i = 0,1$. Temos 2 polinômios homogêneos nas variáveis T,U, da forma

$$G_0 = a_0T^m + a_1T^{m-1} + \ldots + a_mU^m$$

$$G_1 = b_0T^m + \ldots + b_mU^m \ ,$$

onde os a_i, b_j são polinômios homogêneos de grau 1 nas novas variáveis Y_o, Y_1, Y_2.

Esta é uma situação típica da teoria da eliminação: procuramos condições sobre os coeficientes de 2 polinômios para que admitam um zero comum. (No caso em pauta, G_o, G_1 são homogêneos, mas o zero comum trivial $t = u = 0$ não interessa). Consideremos a resultante $R = R(Y_o, Y_1, Y_2)$ de $G_o(T,1)$, $G_1(T,1)$. Sabemos então que, para cada $y = (y_o, y_1, y_2)$,

$$R(y) = 0 \iff (a_o(y) = b_o(y) = 0 \quad \text{ou} \quad G_o(T,1), G_1(T,1) \text{ admitem raiz comum } t)$$

Ora, se $a_o(y) = b_o(y) = 0$, temos $G_o(1,0) = G_1(1,0) = 0$. Concluímos que

$$R(y) = 0 \iff (G_o(t,u) = G_1(t,u) = 0 \text{ para algum } (t:u) \in \mathbb{P}^1.)$$

Em resumo, a argumentação acima mostra que

$$(y_o:y_1:1) \in \psi(\mathbb{P}^1) \iff R(y_o, y_1, 1) = 0 \ .$$

Em particular, $\psi(\mathbb{P}^1)$ contém a curva afim $R(Y_o, Y_1, 1) = 0$.

Lembrando que F é irredutível e $\psi(\mathbb{P}^1) \subset F$, concluímos que

$$(y_o:y_1:1) \in \psi(\mathbb{P}^1) \iff (y_o:y_1:1) \in F.$$

Repetindo o argumento com y_o ou y_1 no lugar de y_2, concluímos $\psi(\mathbb{P}^1) = F$.

C.Q.D.

13. Definição. Uma curva projetiva à racional se for igual à imagem de uma aplicação polinomial não constante $\mathbb{P}^1 \to \mathbb{P}^2$..

O leitor deve verificar que esta definição é consistente com a Definição 1. Precisamente, deixamos como exercício a prova da seguinte

14. Proposição.

(i) Seja f uma curva afim. Então f é racional se e só se seu fecho projetivo f^* é racional.

ii) Seja F uma curva projetiva. Então F é racional se e só se F_* é racional (ou vazia!).

Exercícios

11) Demonstre as Proposições 11 e 14.

12) Sejam $\psi_0, \psi_1, \psi_2 \in k[X,Y]$ polinomios homogêneos de grau 2, linearmente independentes. Mostre que não admitem fator comum, e que a imagem da aplicação polinomial que definem de $\mathbb{P}^1$ em $\mathbb{P}^2$ é uma cônica não singular. Toda cônica não singular é imagem de uma tal aplicação.

13) Toda cúbica singular irredutível é racional.

14) Toda aplicação polinomial bijetiva $\mathbb{P}^1 \to \mathbb{P}^1$ é do tipo $(x:y) \to (ax+by:cx+dy)$ com a,b,c,d constantes tais que

$ad-bc \neq 0$.

15) Sejam $p,q,r \in k[T]$ tais que $mdc(p,q,r) = 1$ e p/r, q/r é uma boa parametrização da curva racional f. Mostre que $\partial f = \max\{\partial p, \partial q, \partial r\}$. (Sugestão: Se A,B,C são indeterminadas, então $Ap+Bq+Cr$ é irredutível em $k[A,B,C,T]$; conclua que as raízes de $ap+bq+cr$ são todas distintas para "quase todo" $(a:b:c) \in \mathbb{P}^2$).

16) A multiplicidade de um ponto de uma curva racional é igual ao número de valores do parâmetro que lhe correspondem numa parametrização do tipo descrito no Exercício anterior, contando esses valores com multiplicidades convenientemente definidas.

§5. O gênero virtual

O próximo resultado nos fornecerá um critério numérico para que uma curva seja racional.

15. Definição. O gênero virtual de uma curva projetiva F sem componentes múltiplas é o número inteiro

$$g_v = g_v(F) = \frac{(d-1)(d-2)}{2} - \sum_f m_f(m_P-1)/2 \ ,$$

onde $d = \partial F$ e $m_P = m_P(F)$.

O somatório é finito pois $m_P = 1$ exceto para o número finito de pontos singulares de F.

Exemplos.

1) O gênero virtual de uma reta ou de uma cônica irredutível é zero.

2) Se F é a cúbica $Y^2 = X^3$, temos $g_v = 0$.

3) Considere a curva $Y^2 = X^5$. Os pontos singulares são $(0:0:1)$ e $(0:1:0)$ com respectivas multiplicidades iguais a 2, 3. Logo, $g_v = \frac{(5-1)(5-2)}{2} - 1 - 3 = 2$.

16. Proposição. Seja F uma curva irredutível. Então

(i) $g_v(F) \geq 0$

(ii) $g_v(F) = 0 \Rightarrow F$ é racional.

Observemos que a recíproca de (ii) não é válida, pois no 3º exemplo acima a curva é evidentemente racional (fazer $x=T^2$, $y=T^5$), mas $g_v = 2 > 0$. Na realidade, o gênero virtual é apenas uma aproximação grosseira do mais importante número associado a uma curva, o gênero geométrico. Este último coincide com $g_v(F)$ quando as singularidades de F são apenas pontos múltiplos ordinários. Deixamos como exercício (18) uma recíproca parcial, mostrando que $g_v = 0$ se F é racional e seus pontos singulares são todos ordinários.

Demonstração da Proposição 16. Examinemos inicialmente um caso simples. Uma cúbica irredutível não admite ponto triplo, pois teria que conter a reta que une qualquer outro de seus pontos ao ponto triplo; similarmente, também

não admite 2 pontos duplos distintos. Por outro lado, se a cúbica admitir um ponto duplo P_o, consideremos o feixe das retas que passam por P_o. Se L_o, L_∞ são 2 dessas, as demais retas do feixe são da forma $L_t = L_o + tL_\infty$ para um valor conveniente de t. O ponto P_o absorvendo 2 interseções, cada L_t destaca sobre a cúbica um único ponto adicional, cujas coordenadas se expressam como função racional de t.

Para o caso geral, devemos considerar curvas de grau suficientemente grande passando por todos os pontos singulares de F.

Precisamente, seja $d = \partial F$. Os casos $d = 1,2$ dispensando maiores comentários, suponhamos $d \geq 3$. Sejam $P_1,\ldots,P_s$ os distintos pontos singulares de F, com $m_i = m_{P_i}(F) \geq 2$.

Vamos estudar a coleção das curvas de um certo grau n que passam por cada P_i com multiplicidade $\geq m_i - 1$. Denotemos por $\mathcal{S}_n$ o conjunto de todas as curvas projetivas planas de grau n. Podemos identificar $\mathcal{S}_n$ com um espaço projetivo $\mathbb{P}^N$, com $N = n(n+3)/2$, associando a cada curva $G = \Sigma\, a_{ij}\, X^i\, Y^j\, Z^{n-i-j}$ o ponto $(a_{oo}:a_{01}:\ldots:a_{n0})$, os índices i,j satisfazendo a $i,j \geq 0$, $i+j \leq n$, ordenados de alguma maneira. Seja

$$\mathcal{S}_n^o = \{G \in \mathcal{S}_n \mid m_{P_i}(G) \geq m_i - 1, \quad i = 1,\ldots,s\} .$$

Ora, a imposição de que um dado ponto seja m-uplo sobre uma curva traduz-se num sistema de $\binom{m+1}{2}$ equações lineares homogêneas nos coeficientes do polinômio que define a curva. Assim, $\mathcal{S}_n^o$ identifica-se a um subespaço projetivo de $\mathbb{P}^N$, com a dimen-

são

$$\dim s^o_n \geq N - \Sigma\binom{m_i}{2} =: N_n \ .$$

Tomando $n = d-1$, calculamos

$$\begin{aligned} N_{d-1} &= (d-1)(d+2) - \Sigma\, m_i(m_i-1) \\ &= 2g_v + 4(d-1) \\ &\geq d(d-1) - \Sigma\, m_i(m_i-1) \ . \end{aligned}$$

Esta última quantidade é ≥ 0. Com efeito, aplicando o Teorema de Bezout a F, F_X, encontramos

$$d(d-1) = \Sigma(F,F_X)_P \ .$$

Mas é fácil ver que $m_{P_i}(F_X) \geq m_i - 1$, donde $(F,F_X)_{P_i} \geq m_i(m_i-1)$.

Tendo verificado que N_{d-1} é ≥ 0, podemos concluir que existe uma curva de grau $d-1$, $G \in s^o_{d-1}$, satisfazendo ainda às condições adicionais de passar por N_{d-1} pontos de F, distintos dos P_i. Aplicando Bezout, resulta

$$d(d-1) \geq \Sigma\, m_i(m_i-1) + N_{d-1} \ .$$

Daí vem

$$\begin{aligned} g_v &= N_{d-1} - 2(d-1) \\ &\leq (d-1)(d-2) - \Sigma\, m_i(m_i-1) = 2g_v \end{aligned}$$

donde $g_v \geq 0$, completando a demonstração (q).

Suponhamos agora $g_v = 0$. Fazendo $n=d-2$, calculamos

$$N_{d-2} = d-2.$$

Escolhamos $d-3$ novos pontos $Q_j \in F$, e consideremos

$$\mathcal{S}' = \{G \in \mathcal{S}^{o}_{d-2} \mid Q_j \in G, \quad j = 1,\ldots,d-3\} ,$$

que é obtido a partir de $\mathcal{S}^{o}_{d-2}$ pela imposição de $d-3$ novas equações lineares. Temos então

$$\dim \mathcal{S}' \geq 1.$$

Afirmamos que $\dim \mathcal{S}' = 1$.

Com efeito, se $\dim \mathcal{S}' \geq 2$, então poderíamos forçar algum $G \in \mathcal{S}'$ a passar por mais 2 pontos de F, distintos dos pontos fixos já considerados. Contando os pontos de $G \cap F$, obteríamos

$$d(d-2) \geq \Sigma\, m_i(m_i-1) + d-3 + 2$$

donde

$$0 = (d-1)(d-2) - \Sigma\, m_i(m_i-1) \geq 1 \;!!!$$

Em resumo, existem $G_o, G_1 \in \mathcal{S}'$ tais que todo elemento de $\mathcal{S}'$ é da forma $x_o G_o + x_1 G_1$, para algum $(x_o:x_1) \in \mathbb{P}^1$, i.e., é um feixe de curvas, i.e., uma família a 1 parâmetro. Vamos mostrar que é possível parametrizar F empregando esse feixe de curvas.

Seja C' o complementar de $G_o \cap F_*$ na curva afim $C = F_*$. (Em particular, C' exclui os pontos P_i, Q_j). Seja φ a função racional definida por

$$\begin{aligned} \varphi\colon C' &\longrightarrow \mathbb{A}^1 \\ P &\longmapsto \varphi(P) = -\, G_1(P)/G_o(P). \end{aligned}$$

Por construção, $\varphi(P)\ G_0+G_1$ é a única curva de grau $d-2$ que passa por P, pelos Q_j, e por cada P_i com multiplicidade $\geq m_i-1$.

Observemos que φ é injetiva, do contrário existiria $G \in \mathcal{G}'$ contendo 2 pontos além dos já fixados. Em particular, φ é não constante, acarretando que o subcorpo $k(\varphi)$ de $K(C)$ gerado por φ é isomorfo ao corpo das funções racionais de uma variável (veja o Exercício 8). Para concluirmos que C, e portanto F, é racional, é suficiente provarmos que $K(C) = k(\varphi)$.

17. Lema. Seja φ uma função racional não constante de uma curva irredutível C. Seja $m = [K(C): k(\varphi)]$. Então, exceto para um número finito de valores $t \in k$, a equação $\varphi(P) = t$ admite exatamente m soluções distintas. Em particular, se C admitir uma função racional injetiva então C é racional.

Demonstração. Lembremos que $K(C)$ é gerado sobre k pelas restrições $\overline{X},\overline{Y}$, ou seja, $K(C) = k(\overline{X},\overline{Y})$. Sem perda de generalidade, podemos supor $\overline{X} \notin k$.

Mostremos que $\overline{X},\overline{Y}$ são algébricas/$k(\varphi)$.

Com efeito, φ não é algébrico/k, pois k é algebricamente fechado e $\varphi \notin k$. Se, por absurdo, $\overline{X}$ não fosse algébrico sobre $k(\varphi)$, então para todo $p \in k(\varphi)[T]$, $p \neq 0$, teríamos $p(\overline{X}) \neq 0$. Equivalentemente, para todo $p \in k[T,U]$, se $p \neq 0$ então $p(\varphi,\overline{X}) \neq 0$. Assim, φ não seria algébrico sobre $k(\overline{X})$. Visto que $\overline{Y}$ é algébrico sobre $k(\overline{X})$ (já que $f(\overline{X},\overline{Y}) = 0$, onde f denota a equação de C), deduziríamos que φ não é algébrico so-

bre $k(\overline{X},\overline{Y})$, contradição.

Concluimos que $k(\overline{X},\overline{Y})$ é uma extensão algébrica finita de $k(\varphi)$.

Apliquemos o teorema do elemento primitivo: existe $\psi \in k(\overline{X},\overline{Y})$ tal que

$$k(\overline{X},\overline{Y}) = (k(\varphi))(\psi) = k(\varphi,\psi)$$

Em particular, existem funções racionais α,β de 2 variáveis tais que

$$\overline{X} = \alpha(\varphi,\psi), \quad \overline{Y} = \beta(\varphi,\psi).$$

Escrevamos o polinômio mínimo de ψ sobre $k(\varphi)$ na forma

$$g(T,U) = a_o(T)U^m + \ldots + a_m(T), \quad a_i \in k[T], \quad a_o \neq 0 .$$

Assim, $g(\varphi,\psi) = 0$, e o grau m coincide com o grau da extensão $k(\overline{X},\overline{Y}) = k(\varphi,\psi)$ sobre $k(\varphi)$.

Seja D a curva definida no plano (t,u) pela equação $g(T,U) = 0$.

Por construção de D, o k-homomorfismo de $k[T,U]$ em $k(\overline{X},\overline{Y})$ definido por $h(T,U) \longrightarrow h(\varphi,\psi)$ induz uma inclusão do anel de funções regulares $A(D)$ em $k(\overline{X},\overline{Y})$ e por fim, o k-isomorfismo $k(\overline{T},\overline{U}) \xrightarrow{\sim} k(\overline{X},\overline{Y})$. Este último isomorfismo associa a $\overline{X},\overline{Y}$ as funções $\alpha(\overline{T},\overline{U})$, $\beta(\overline{T},\overline{U})$ respectivamente.

Sejam C_o e D_o os maiores subconjuntos de C e D em que φ,ψ e α,β estão todas definidas. Consideremos as aplicações

$\pi\colon C_o \longrightarrow D$ $\qquad\qquad$ $\chi\colon D_o \longrightarrow C$

$(x,y) \longmapsto (\varphi(x,y),\varphi(x,y))$ e $(t,u) \longmapsto (\alpha(t,u),\beta(t,u))$.

Desprezando mais um número finito de pontos, podemos supor que $\pi(C_o) \subset D_o$ e $\chi(D_o) \subset C_o$. Lembrando a definição do isomorfismo $K(D) \tilde{\to} K(C)$, verifica-se facilmente que π e χ são inversas uma da outra. Em particular, observamos que $\varphi(\chi(t,u)) = t$ para todo $(t,u) \in C_o$. Desta maneira, resolver a equação $\varphi(x,y) = t$ com $(x,y) \in C_o$ é agora equivalente a resolver a equação

$$g(t,U) = 0 \quad .$$

Descontando os valores de t que anulam $a_o(T)$ ou que ocorrem em pontos de interseção de $g(T,U)$ com $g_U(T,U)$, obtemos m soluções distintas.

C.Q.D.

Um comentário: o teorema do elemento primitivo nos permite substituir a curva C por outra D, com o mesmo corpo de funções racionais, de tal sorte que a função φ é substituída pela projeção $D \ni (t,u) \longmapsto t$.

Exemplo. Consideremos a lemniscata $C\colon (X^2+Y^2)^2 = X^2-Y^2$. Seus pontos singulares são $(0:0:1)$ e $(1:\pm i:0)$, todos duplos. Logo, $g_v = 0$. Apliquemos o procedimento da demonstração para construir uma parametrização. Devemos considerar o feixe das cônicas passando por esses 3 pontos e por um 4º ponto adicional, e.g. $(1:0:1)$. Sejam $G_o = XZ$, $G_1 = X^2+Y^2-XZ$. Então o feixe $x_oG_o + x_1G_1 = 0$ $((x_o:x_1) \in \mathbb{P}^1)$ é a totalidade das cônicas que

contém os 4 pontos. A parametrização procurada será obtida achando a função inversa de

$$\varphi(x,y) = (x-x^2-y^2)/y, \quad (x,y) \in C_\varphi .$$

Substituimos $x-x^2-y^2 = ty$ na equação da lemniscata. Desprezando soluções provenientes dos pontos fixos, encontramos

$$y = 2tx/(t^2+1)$$
$$x = (t^4-1)/((t^2+1)^2+4t^2),$$

que dá a parametrização procurada.

§6. Aplicação ao cálculo integral.

Finalizamos este capítulo mencionando uma aplicação da propriedade característica das curvas racionais ao cálculo de integrais de certas funções algébricas.

Dizemos que uma função $y = \varphi(x)$ definida e contínua numa vizinhança da de um ponto $x_o \in k (k = \mathbb{R}$ ou $\mathbb{C})$ é algébrica se existir um polinômio não constante f tal que $f(x,\varphi(x)) = 0$ no domínio de φ. (por exemplo, $\varphi(x) = \sqrt{x}$ é algébrica). Tomando f irredutível, o polinômio fica bem determinado a menos de fator constante e dizemos então que f é a equação de φ, ou que φ é definida por $f(X,Y) = 0$.

Eis a questão que queremos abordar: sob que condições é a integral $\int\varphi(x)dx$ exprimível por funções elementares?

Não é nosso objetivo aqui explorar em profundidade esse problema. Vamos nos contentar com a discussão de um caso simples.

De início, esclareçamos o significado de "função elementar". Chamaremos de <u>função elementar da função algébrica</u> $\varphi(x)$ a uma combinação linear de funções do tipo $\psi(x,\varphi(x))$ ou $\log(\psi(x,\varphi(x))$, onde ψ denota uma função racional de 2 variáveis.

18.<u>Proposição</u>. <u>Seja</u> $y = \varphi(x)$ <u>uma função algébrica definida pela equação polinomial</u> $f(X,Y) = 0$. <u>Se a curva definida por</u> f <u>é racional, então</u> $\int \chi(x,\varphi(x))dx$ <u>é uma função elementar de</u> $\varphi(x)$ <u>para toda função racional</u> χ.

<u>Demonstração</u>. Seja $x(T)$, $y(T)$ uma boa parametrização de f. Logo, salvo um número finito de exceções, cada ponto $(a,b) \in f$ é da forma $a = x(t)$, $b = y(t)$ para um único valor t. Segue-se que $\varphi(x(t)) = y(t)$ para quase todo t em que o 1º membro está definido. Assim, podemos calcular $\int \varphi(x,\varphi(x)dx$ por substituição, fazendo $x = x(T)$, $dx = \dot{x}dT$. A integral se transforma numa do tipo $\int \frac{p(T)}{q(T)}\, dT$, onde p,q são polinômios. Se $q(T) = (T-c_1)^{m_1}\ldots(T-c_s)^{m_s}$, onde os $c_i \in \mathbb{C}$ são 2 a 2 distintos, é possível se escrever

$$\frac{p(T)}{q(T)} = r(T) + \sum_{i=1}^{s} \sum_{j=1}^{m_i} a_{ij}(T-c_i)^{-j} ,$$

onde $r(T)$ é um polinômio e os a_{ij} são constantes. A integral de uma função desse tipo é claramente da forma $\psi(T) + \Sigma\, a_{il} \log(T-c_i)$, onde $\psi(T)$ é racional. Lembrando que $T = \xi(x(T),y(T))$ para alguma função racional ξ, vemos que é possível expressar o resultado final em termos de uma função elemen-

tar de $\varphi(x)$. C.Q.D.

Exemplo. Calcular $\int \frac{\varphi(x)}{x+1}\,dx$, onde $\varphi(x)$ é definida por $Y^2-X^2+X^3 = 0$.

Temos a parametrização

$$x(T) = T^2-1$$

$$y(T) = T(T^2-1).$$

Logo,

$$\int \frac{\varphi(x)}{x+1}\,dx = \int \frac{(T^2-1)T}{T^2-1+1}\cdot 2T\,dT =$$

$$= 2\int (T^2-1)\,dT = 2\left(\frac{T^3}{3} - T\right) =$$

$$= \frac{2}{3}\left(\left(\frac{\varphi(x)}{x}\right)^3 - 3\,\frac{\varphi(x)}{x}\right).$$

Exercícios

17) Ache uma parametrização para $(X^2+Y^2)^2 = XY$.

18) O objetivo deste Exercício é provar que, se F é uma curva projetiva racional cujas singularidades são apenas pontos múltiplos ordinários, então $g_v(F) = 0$.

a) Mostre que existem $x,y,z \in k[T]$ com $mdc(x,y,z) = 1$, $F(x,y,z) = 0$ em $k[T]$ e tal que $t \mapsto P_t =$ $= (x(t):y(t):z(t))$ é uma bijeção do complementar $u \subset \mathbb{A}^1$ de um número finito de pontos sobre o complementar $C \subset F$ de um número finito de pontos.

b) Desprezando mais um número finito de pontos, prove que a equação da reta tangente a F em P_t é, para $t \in u$,

$$\begin{vmatrix} X & Y & Z \\ x(t) & y(t) & z(t) \\ \dot{x}(t) & \dot{y}(t) & \dot{z}(t) \end{vmatrix} = 0 .$$

(Sugestão: use a fórmula de Euler e derive $F(x,y,z)$ com relação a t para mostrar que F_X, F_Y, F_Z (calculadas em P_t) são proporcionais aos menores das 2 últimas linhas).

c) Seja $P = (x_o : y_o : z_o)$ um ponto fora das tangentes aos pontos singulares de F e das tangentes aos pontos correspondentes a valores excepcionais de t (i.e., $t \notin u$). Mostre que $F \cap F^P$ contém, além dos pontos singulares, os pontos P_t em que t é raiz do polinômio

$$\begin{vmatrix} x_o & y_o & z_o \\ dx-t\dot{x} & dy-t\dot{y} & dz-t\dot{z} \\ \dot{x} & \dot{y} & \dot{z} \end{vmatrix} , \quad \text{onde} \quad d = \partial F.$$

d) Mostre que o grau deste último polinômio é no máximo $2d-2$.

e) Use o Exercício VII.8 para concluir a relação

$$d(d-1) \leq \Sigma\, m_Q(F)(m_Q(F)-1)+2d-2 ,$$

e daí, $g_v = 0$.

19) Mostre que toda curva racional projetiva de grau ≥ 3 é singular. No entanto, existem curvas racionais afins não singulares de grau arbitrário.

CAPÍTULO IX

CÚBICAS NÃO SINGULARES

§1. Conexões inesperadas

Este último tópico é um notável ponto de confluência de ramos da Matemática tão diversos como a Álgebra, a Geometria, a Análise e a Aritmética.

O fato central na geometria de uma cúbica não singular F reside na estrutura de grupo definida a partir da correspondência que associa a cada par de pontos $P,Q \in F$, o 3º ponto de interseção da reta PQ com F. Essa estrutura de grupo sintetiza uma grande riqueza de informações. Dela podemos deduzir, por exemplo, que a reta que liga 2 pontos de inflexão intersecta a cúbica num 3º ponto de inflexão. Utilizamos este fato para mostrar que a classe de congruência de F (i.e., a coleção das cúbicas obtidas de F por uma projetividade) é determinada por uma certa constante, chamada o módulo de F.

Quando $k = \mathbf{C}$, a estrutura de grupo está intimamente ligada à teoria das funções elíticas. Embora o estudo desse aspecto analítico fuja aos nossos propósitos, não resistimos ao impulso de, ao menos mencionar, de passagem, algumas das conexões mais surpreendentes. (O aluno com bom espírito de iniciativa encontrará os detalhes nas referências bibliográficas). (1) Associada a cada cúbica não singular F: $Y^2 = X^3+aX+b$, existe uma função meromor-

fa não constante $\wp(z)$, satisfazendo à equação diferencial

$$\wp'(z)^2 = \wp(z)^3+a\wp(z)+b \ .$$

(2) $\wp(z)$ é uma função elítica, i.e., existe um subgrupo $\langle w_1,w_2\rangle \subset \mathbb{C}$ gerado por 2 números complexos w_1,w_2 linearmente independentes/$\mathbb{R}$ tal que $p(z+w) = \wp(z)$ se e só se $w \in \langle w_1,w_2\rangle$. Diz-se então que $\wp(z)$ é duplamente periódica, com períodos $m_1w_1+m_2w_2$, $m_i \in \mathbb{Z}$ (3) A aplicação $z \mapsto (\wp(z):\wp'(z):1)$ induz um isomorfismo do grupo aditivo $\mathbb{C}/\langle w_1,w_2\rangle$ sobre F. (4) Topologicamente, $\mathbb{C}/\langle w_1,w_2\rangle$ é isomorfo a $\mathbb{R}^2/\mathbb{Z}^2 = (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z}) = S^1xS^1$, produto de 2 círculos. Assim, uma cúbica não singular se identifica com um toro! (5) O módulo de F, mencionado acima, expressa-se como função dos períodos de $\wp(z)$.

Quando a cúbica F é definida por uma equação a coeficientes inteiros (e.g., a cúbica do "último teorema de Fermat", $X^3+Y^3 = Z^3$), é natural perguntar se existem pontos racionais, i.e., com coordenadas homogêneas números racionais (ou equivalentemente, números inteiros). Infelizmente, não se conhece nenhum critério para decidir, em geral, se uma cúbica possui ou não pontos racionais. Há exemplos em que não ocorre nenhum tal ponto. Pelo lado mais positivo, pode-se mostrar que, se F possui um ponto racional, então F é congruente a uma cúbica (ainda definida sobre $\mathbb{Z}$) com um ponto de inflexão racional. Tomando-se um tal ponto de inflexão como elemento para a estrutura de grupo (cf. Proposição 12), o conjunto dos pontos racionais forma um subgrupo

de F (Teorema de Mordell)[1].

Bem, aqui vamos nos restringir apenas à classificação projetiva e às propriedades mais simples ligadas à estrutura de grupo de uma cúbica não singular. Procuramos dosar a necessidade de introduzir novos conceitos gerais com aplicações diretas ao estudo dessas curvas.

§2. Forma normal.

Duas retas quaisquer são congruentes por uma projetividade. Similarmente, é um fácil exercício mostrar que, a menos de projetividade, só há um tipo de cônica não degenerada. Também só há um tipo de cúbica nodal e outro cuspidal. Para as cúbicas não singulares, porém, a classificação é bem diferente, existindo um tipo para cada elemento do corpo k! Precisamente, mostraremos neste parágrafo que a cada cúbica F não singular está associado um invariante $J \in k$, o qual determina a classe de congruência de F.

1. Proposição. Toda cúbica não singular é congruente por uma projetividade a uma cúbica do tipo

$$ZY^2 = X(X-Z)(X-\lambda Z)$$

para alguma constante $\lambda \in k$, $\lambda \neq 0,1$.

Demonstração. Sabemos, em vista das fórmulas de Plucker, que uma cúbica não singular F admite pontos de inflexão

1) Existem umas notas fascinantes escritas por J. Tate, "Rational points on elliptic curves" contendo uma demonstração deste teorema; não nos consta que tenham sido publicadas em forma de livro, mas há cópias nas bibliotecas da UFPE e do IMPA.

(9 ao todo). Tomamos (0:1:0) como um deles, com tangente $Z = 0$. Podemos ainda supor que $(0:0:1) \in F$, com tangente $X = 0$. Temos então F já na forma

$$F = X^3 + Z(aX^2 + bXY + cY^2) + dZ^2X \ ,$$

com $d \neq 0 \neq c$ (senão F seria divisível por X). Substituindo Y por $Y/\sqrt{c}$, podemos supor $c = 1$. Substituindo Y por $Y - bX/2$, podemos supor $b = 0$. Assim, já temos F na forma

$$F = X^3 + Z(Y^2 + aX^2) + bXZ^2$$

com novos a, b, este último $\neq 0$ (senão $(0:0:1)$ seria um ponto singular). Seja α uma raiz de X^2+aX+b. Substituindo X por αX vem

$$F = ZY^2 + \alpha^3 X(X-Z)(X-\lambda Z) \ .$$

Finalmente, substituindo Y por $(-\alpha)^{3/2} Y$ e cancelando, obtemos a forma normal enunciada.

C.Q.D.

Quão bem determinado é o parâmetro λ?

Ponhamos, para cada $\lambda \neq 0,1$,

$$F_\lambda = ZY^2 - X(X-Z)(X-\lambda Z) \ ,$$

$$\Lambda(\lambda) = \{\lambda, \tfrac{1}{\lambda}, 1-\lambda, \tfrac{1}{1-\lambda}, \tfrac{\lambda-1}{\lambda}, \tfrac{\lambda}{\lambda-1}\} \ .$$

2. <u>Proposição</u>. <u>Duas cúbicas</u> F_λ, F_μ <u>são congruentes se e somente se</u> $\Lambda(\lambda) = \Lambda(\mu)$.

Demonstração. Mostremos inicialmente que existem projetividades S,T tais que

$$S_{\cdot}F_{\lambda} = F_{1-\lambda} \quad \text{e} \quad T_{\cdot}F_{\lambda} = F_{1/\lambda} \cdot$$

Com efeito, basta definir $S_{\cdot}$, $T_{\cdot}$ pelas condições:

$$S_{\cdot} : \begin{cases} X \longmapsto X-Z \ , \\ Y \longmapsto \sqrt{-1}\, Y \ , \\ Z \longmapsto -Z \ , \end{cases} \quad \text{e} \quad T_{\cdot} : \begin{cases} X \longmapsto \lambda X \ , \\ Y \longmapsto \lambda^{3/2}\, Y, \\ Z \longmapsto Z \ . \end{cases}$$

Substituindo λ por $1-\lambda$ ou $1/\lambda$, segue-se que para cada $\mu \in \Lambda(\lambda)$, conseguiremos obter uma projetividade que leve F_{λ} em F_{μ}.

Para a recíproca, seja U uma projetividade tal que $U_{\cdot}F_{\mu} = F_{\lambda}$. O ponto de inflexão $(0:1:0) \in F_{\mu}$ é transformado em um ponto de inflexão $U(0:1:0) \in F_{\lambda}$. Admitamos, por um momento, conhecido o seguinte

Fato: Se P,Q são pontos de inflexão de uma cúbica não singular F então existe uma projetividade M tal que $M_{\cdot}F = F$ e $MP = Q$.

Continuando com a argumentação, podemos supor então que $U(0:1:0) = (0:1:0)$. Agora os 3 pontos de contato das retas tangentes a F_{μ} passando por $(0:1:0)$ são transladados sobre os respectivos de F_{λ}. Isto é: U aplica $\{(0:0:1),(1:0:1),(\mu:0:1)\}$ sobre $\{(0:0:1), (1:0:1), (\lambda:0:1)\}$. Além disso, U deixa invariante a tangente inflexional $Z = 0$, bem como a reta $Y = 0$.

Identificando esta última com $\mathbb{P}^1$, obtivemos uma projetividade de $\mathbb{P}^1$ (i.e., uma aplicação da forma $(x:y) \mapsto (ax+by:cx+dy)$ que fixa o ponto no infinito $(1:0)$ (identificado com a interseção de $Y = 0$ e $Z = 0$), e que aplica $\{(0:1),(1:1),(\mu:1)\}$ sobre $\{(0:1),(1:1),(\lambda:1)\}$. Nessas circunstâncias, o leitor não terá dificuldade em concluir que $\mu \in \Lambda(\lambda)$. Isto completa a demonstração, a menos da justificativa do Fato acima, a qual será feita oportunamente (Corolário 14).

C.Q.D.

3. Definição. O módulo da cúbica $F_\lambda = ZY^2 - X(X-Z)(X-\lambda Z)$ é dado por

$$J(\lambda) = \frac{27}{4} \frac{(1-\lambda+\lambda^2)^2}{\lambda^2(1-\lambda)} \quad .$$

O leitor deve verificar que J é constante sobre cada $\Lambda(\lambda)$ e que, de fato, $J(\lambda) = J(\mu) \Leftrightarrow \Lambda(\lambda) = \Lambda(\mu)$. Em conclusão, segue-se que 2 cúbicas não singulares são projetivamente equivalentes, (i.e., congruentes por uma projetividade) se e só se elas têm o mesmo módulo!

Na realidade, o módulo de uma cúbica é um invariante mais fino. Pode-se demonstrar que 2 cúbicas não singulares têm o mesmo módulo se e somente se seus corpos de funções racionais são k-isomorfos.

Exercícios

1)Reduza $X^3+Y^3+Z^3 = 0$ à forma normal da Proposição 1.

2) Ache a equação de uma cúbica F tal que $(0:1:0)$ é um ponto de inflexão com tangente $Z = 0$ e tal que os pontos $(-1:0:1), (0:0:1)$ e $(1:0:1)$ são os pontos de contato das retas tangentes a F passando por $(0:1:0)$.

3) Mostre que $\Lambda(\lambda)$ (veja Proposição 2) consiste de 6 elementos distintos, exceto se $\lambda \in \{-1, \frac{1}{2}, 2\}$ ou se $\lambda^2-\lambda+1 = 0$. Mostre que $J(\lambda) = J(\mu) \Leftrightarrow \Lambda(\lambda) = \Lambda(\mu)$.

4) Seja C um conjunto de 9 pontos distintos com a propriedade de que a reta que une 2 quaisquer contém um e só um 3º. Mostre que existe uma projetividade que leva C no conjunto dos pontos.

$$(0:1:-1),\ (-1:0:1),\ (1:-1:0)$$

$$(0:1:a),\ (a:0:1),\ (1:a:0)$$

$$(0:1:b),\ (b:0:1),\ (1:b:0),$$

onde a,b são as raízes de X^2-X+1. (O grupo das simetrias dessa configuração é discutido nos livros "Traité des Substitutions" de Camille Jordan, e "Theory and applications of finite groups" de Miller, Blichfeldt e Dickson).

5) Mostre que toda cúbica é congruente a uma do tipo $G_c = X^3+Y^3+Z^3+3cXYZ$. Mostre que G_c contém os 9 pontos acima definidos e que G_c é singular se e só se $c = \infty, -1, a$ ou b, quando então ela se degenera na união de 3 retas.

§3. Funções racionais

As propriedades mais interessantes de uma cúbica não singular estão diretamente relacionadas com sua estrutura de grupo mencionada na introdução. Para estudá-las, será conveniente fazer uma digressão, introduzindo mais alguns conceitos importantes.

4. Definição. O anel homogêneo de uma curva projetiva F é definido por

$$A(F)_h = k[X,Y,Z]/(F) .$$

Denotamos por $\overline{G}$ a classe de $G \in k[X,Y,Z]$ módulo (F).

Suporemos no que segue que F é irredutível. Assim, $A(F)_h$ é um domínio; denotamos por $K(F)_h$ seu corpo de frações.

Seja $K(F)$ o subconjunto de $K(F)_h$ formado pelas frações do tipo $\overline{G}/\overline{H}$ com G,H homogêneos do mesmo grau. É fácil ver que $K(F)$ é um subcorpo de $K(F)_h$, chamado corpo das funções racionais de F. Esta designação se justifica pelo seguinte

5. Lema. Se F é o fecho projetivo da curva afim irredutível f então $K(F)$ é k-isomorfo a $K(f)$(Def. VIII.4).

Demonstração. Considere o homomorfismo

$$\varphi: k[X,Y] \longrightarrow K(F)_h$$
$$g(X,Y) \longmapsto g(\overline{X}/\overline{Z},\ \overline{Y}/\overline{Z}) .$$

Observando a fórmula

$$g^*(X,Y,Z) = Z^{\partial g}\, g(X/Z,Y/Z) \quad \text{em} \quad k[X,Y,Z] ,$$

deduz-se facilmente que o núcleo de φ é igual a (f). Obtêm-se então os homomorfismos induzidos,

$$\begin{array}{ccc} K[X,Y]/(f) & \hookrightarrow & K(F)_h \\ \uparrow & \nearrow & \\ K(f) & & \end{array} .$$

Observando que $K(F)$ é gerado por $\overline{X}/\overline{Z}$, $\overline{Y}/\overline{Z}$, os quais estão na imagem de $K(f)$, concluimos $K(F) \approx K(f)$.

C.Q.D.

Exercício

6) Seja $F = f^*$ o fecho projetivo de uma curva afim irredutível f. Mostre que $K(F)_h$ é a extensão de $K(F)$ gerada por $\overline{Z}$.

§4. Ciclos e equivalência racional

6. Definição. Um ciclo em uma curva F é uma expressão do tipo

$$n_1P_1 + \ldots + n_rP_r \quad ,$$

onde os n_i são inteiros e os P_i são pontos de F. Mais precisamente, um ciclo é um elemento do grupo abeliano livre gerado pelos pontos de F; este grupo é chamado o grupo dos ciclos de F.

Trata-se simplesmente de uma maneira cômoda de lidar com conjuntos de pontos de F afetados de multiplicidades.

Definimos o grau de um ciclo pela fórmula

$$\partial(\Sigma\, n_i P_i) = \Sigma\, n_i .$$

Evidentemente, se D, D' são ciclos, temos

$$\partial(D+D') = \partial D + \partial D' .$$

Seja agora G uma curva distinta de F. Definimos o ciclo de interseção de G com F pela fórmula

$$(G) = (G)_F = \Sigma (F,G)_P P .$$

Observemos que, pelo Teorema de Bezout, temos

$$\partial(G)_F = (\partial G)(\partial F) .$$

Seja $\varphi \in \bar{K}(f)$ uma função racional $\neq 0$. Suponhamos

$$\varphi = \bar{G}_o/\bar{H}_o = \bar{G}_1/\bar{H}_1 ,$$

com G_i, H_i homogêneos, $\partial G_i = \partial H_i$ e $\bar{H}_o \bar{H}_1 \neq 0$. Temos então

$$G_o H_1 = H_o G_1 + AF , \quad \text{para algum } A \in k[X,Y,Z] .$$

Daí é imediato que

$$(G_o H_1)_F = (H_o G_1)_F$$

e portanto,

$$(G_o)_F - (H_o)_F = (G_1)_F - (H_1)_F$$

por propriedade do índice de interseção.

Podemos então definir o ciclo associado à função racional

$\varphi \neq 0$ pela fórmula

$$(\varphi) = (\varphi)_F = (G)_F - (H)_F ,$$

onde $\varphi = \overline{G/H}$ é uma representação de φ como quociente de classes de polinômios homogêneos do mesmo grau.

Exemplo. Seja $F = ZY^2 - X(X-Z)(X-\lambda Z)$. Temos

$$(Z)_F = 3(0:1:0)$$

$$(Y/X)_F = (0:0:1) + (1:0:1) + (\lambda:0:1) - 2(0:0:1) - (0:1:0)$$

$$= (1:0:1) + (\lambda:0:1) - (0:0:1) - (0:1:0).$$

7. Definição. Sejam D, D' ciclos de uma curva F (suposta irredutível). Dizemos que D é racionalmente equivalente a D' se existir uma função racional $\varphi \in K(F)$ tal que

$$D - D' = (\varphi) ;$$

Escrevemos

$$D \equiv D'$$

para denotar equivalência racional.

8. Lema. Equivalência racional à uma relação de equivalência compatível com a adição de ciclos. Em símbolos:

(1) $D \equiv D$ ($\forall$ ciclo D)

(2) $D \equiv D' \Rightarrow D' \equiv D$ ($\forall$ ciclos D, D')

(3) $D \equiv D'$, $D' \equiv D'' \Rightarrow D \equiv D''$ ($\forall$ ciclos D,D',D'').

(4) $D \equiv D' \Rightarrow D+D'' \equiv D'+D''$ ($\forall$ ciclos D,D',D'').

Demonstração. Sejam D,D',D'' ciclos e sejam φ,ψ funções racionais $\neq 0$.

(1) Temos $D-D = 0 =$ ciclo da função constante 1.

(2) Se $D-D' = (\varphi)$, então $D' - D = (\varphi^{-1})$.

(3) Se $D-D' = (\varphi)$, $D'-D'' = (\psi)$, temos evidentemente

$$(\varphi\psi) = (\varphi) + (\psi) = D-D'+D'-D'' = D-D'' .$$

(4) Fica como exercício para o leitor.

C.Q.D.

9. Proposição. Seja F uma curva irredutível não singular. Se existirem $P \neq Q$ em F racionalmente equivalentes, então F é racional.

Demonstração. Sejam G_o, G_1 curvas projetivas do mesmo grau tais que

$$(G_1)-(G_o) = P-Q.$$

Temos então

$$(G_1) = P + \Sigma\, m_i\, P_i ,$$

$$(G_o) = Q + \Sigma\, m_i\, P_i ,$$

com $m_i \geq 1$ e $P_i \in F$, dois a dois distintos.

Visto que cada P_i é um ponto não singular de F, sabemos por (VI-11) que o índice de interseção $(F,G)_{P_i}$ é igual à ordem de anulamento de G sobre F em P_i. Daí concluimos que, para cada $(x_o:x_1) \in \mathbb{P}^1$, vale

$$(x_oG_o+x_1G_1,F)_{P_i} \geq m_i.$$

Trocado em miúdos, construimos um feixe de curvas $\{x_oG_o+x_1G_1\}$, do qual cada membro corta F nos pontos P_i pelo menos m_i vezes.

Lembrando que $1 + \Sigma\, m_i = (\partial F)(\partial G_o)$, vemos que, por cada ponto distinto dos já fixados passa justamente <u>um</u> membro do feixe. Segue-se que a função racional G_1/G_o é injetiva (veja VIII-17 e o parágrafo que lhe antecede), e portanto F é racional.

C.Q.D.

Exercícios

7) Seja F a reta $X = 0$. Mostre que os ciclos

$$(0:0:1) + (0:1:1) \quad \text{e} \quad (0:1:0) + (1:1:0)$$

são racionalmente equivalentes sobre F.

8) Seja $F = YZ-X^2$. Mostre que os (ciclos que se reduzem aos) pontos $(0:0:1)$ e $(0:1:1)$ são racionalmente equivalentes.

9) Prove que 2 ciclos racionalmente equivalentes têm o mesmo grau.

10) Se F é uma reta, mostre que 2 ciclos com o mesmo grau são racionalmente equivalentes. O mesmo é válido se F é uma cônica ou uma cúbica singular, ou mesmo a lemniscata...

11) Seja $F = Z(X^2-Y^2) + X^3$ e seja $\varphi = \frac{X+Y}{X-Y} \in K(F)$. Calcule (φ).

12) Seja F uma curva não singular e seja $\varphi \in K(F)$ uma função racional não constante. Prove que $(\varphi)_F \neq 0$.

13) Prove que o conjunto dos ciclos racionalmente equivalentes a zero sobre uma curva F é um subgrupo do grupo dos ciclos de F.

§5. A estrutura de grupo

Necessitaremos do seguinte resultado preliminar. Observemos que ele é conseqüência de um resultado mais geral, proposto como Exercício VIII.19. Mas vamos apresentar uma prova direta, por desencargo de cosciência.

10. Proposição. *Se F é uma cúbica não singular então F não é racional.*

Demonstração. Podemos supor F na forma normal (leitor: por que?):

$$Y^2 = X(X-1)(X-\lambda), \quad \text{com } \lambda \neq 0,1.$$

Procederemos por redução ao absurdo, supondo F racional. Assim, existem

$$a,b,c,d \in k[T]$$

tais que

$$x = a/c, \quad y = b/d$$

constituem uma boa parametrização. Naturalmente, podemos supor que

$$mdc(a,c) = mdc(b,d) = 1.$$

Substituindo na equação acima, resulta

$$c^3b^2 = d^2a(a-c)(a-\lambda c) \quad \text{em} \quad k[T].$$

Por unicidade da fatoração, segue-se que c^3 e d^2 são associados. Simplificando e absorvendo a constante c^3/d^2 em b, vem

$$b^2 = a(a-c)(a-\lambda c) \ . \tag{10.1}$$

Admitamos por um momento que $\partial b = 3$, $\partial a = 2 \geq \partial c$. Escrevamos $b = b_1b_2b_3$ com $\partial b_i = 1$. Notando que a, a-c, a-λc são 2 a 2 primos relativos, deduzimos que o mesmo ocorre com os b_i e que

$$b_1^2 = a, \ b_2^2 = a-c, \ b_3^2 = a-\lambda c$$

(a menos de reordenação ou fator constante). Daí concluimos

$$c = (b_1-b_2)(b_1+b_2), \quad (1-\lambda)c = (b_3-b_2)(b_3+b_2)$$

Segue-se que b_1-b_2 é associado a $b_3 \pm b_2$. Sem perda de generalidade, podemos escrever relações

$$b_1-b_2 = \alpha(b_3-b_2)$$

$$b_1+b_2 = \beta(b_3+b_2) \ ,$$

com $\beta-\alpha \neq 0$, permitindo concluir, finalmente, que b_2 e b_3 são associados. Mas isto é absurdo, pois a-c e a-λc são primos relativos!

Resta justificar por que $\partial b = 3$ e $\partial a = 2 \geq \partial c$.

Ora, quase toda reta horizontal $Y = y_o$ corta F em 3 pontos distintos. Como a parametrização é suposta boa, esses pontos são de forma $(x(t), y_o)$ para justamente 3 valores do parâmetro. Estes valores são dados pela condição

$$y(t) = \frac{b(t)}{d(t)} = y_o$$

Assim, o polinômio $b(T) - y_o d(T)$ admite exatamente 3 raízes distintas (para quase todo y_o). Logo, $\partial b \leq 3$. Se $\partial b < 3$, então $\partial d = 3$ e daí $\partial c = 2$ (pois c^3/d^2 é constante). Observando (10.1), deduz-se $\partial b = 2$ e $\partial a = 0$ ou 2. Escreve-se $b = b_1 b_2$ e procede-se como antes, chegando a uma contradição. Se $\partial b = 3$, então $\partial d \leq 3$, acarretando $\partial c \leq 2$. Lembrando (10.1) outra vez, vê-se que necessariamente $\partial a = 2$.

C.Q.D.

Tendo em vista a Proposição 9, concluimos imediatamente o seguinte

11. Corolário. Se F é uma cúbica não singular e $P, Q \in F$ então P é racionalmente equivalente a Q somente se $P = Q$.

Vejamos agora como é definida a estrutura de grupo.

Fixemos um ponto $\mathcal{O} \in F$.

Para cada par de pontos P, Q em F, consideremos a interseção de F com reta L que os contém. Se $P = Q$, tomamos $L =$ tangente. Podemos escrever

$$(L) = P+Q+R$$

para algum R em F, bem determinado pelo par P,Q. Seja H a reta definida pelo par $R,\mathcal{O}$, e seja finalmente $P\dot{+}Q$ o 3º ponto de interseção de H com F, de sorte que

$$(H) = R+\mathcal{O}+(P\dot{+}Q) .$$

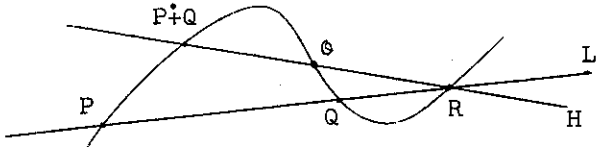


Fig. 26

Observemos que, pondo $\varphi = L/H \in K(F)$, temos

$$(\varphi) = (P+Q+R) - (R+\mathcal{O}+(P\dot{+}Q)) ,$$

e portanto,

(11.1) $$P\dot{+}Q \equiv P+Q-\mathcal{O} .$$

Pelo Corolário 11, esta última fórmula determina completamente $P\dot{+}Q$. É o <u>único</u> ponto de F racionalmente equivalente ao ciclo $P+Q-\mathcal{O}$.

12. <u>Proposição</u>. <u>Seja</u> F <u>uma cúbica não singular e seja</u> $\mathcal{O} \in F$ <u>um ponto de inflexão</u>. <u>A lei de composição</u>

$(P,Q) \longmapsto P \dot{+} Q$ acima descrita estabelece uma estrutura de grupo abeliano em F. O elemento neutro é o ponto $\mathcal{O}$. O inverso aditivo de um ponto $P \in F$ é o 3º ponto de interseção da reta $\mathcal{O}P$ com F, denotado $\dot{-} P$.

Demonstração. É claro que temos $P \dot{+} Q = Q \dot{+} P$. Levando em conta a fórmula (11.1) é fácil ver que $\mathcal{O}$ funciona como elemento neutro e $\dot{-}P$ como inverso de P.

Verifiquemos o axioma da associatividade. Dados $P,Q,R \in F$, temos

$$\begin{aligned}(P \dot{+} Q) \dot{+} R &\equiv (P \dot{+} Q) + R - \mathcal{O} \\ &\equiv (P+Q-\mathcal{O}) + R - \mathcal{O} \\ &= P+(Q+R-\mathcal{O}) - \mathcal{O} \\ &\equiv P+(Q \dot{+} R) - \mathcal{O} \\ &\equiv P \dot{+} (Q+R)\end{aligned}$$

C.Q.D.

13. Proposição.

(i) $P \dot{+} Q \dot{+} R = \mathcal{O} \Leftrightarrow$ Existe uma reta H tal que $(H)_F = P+Q+R$.

(ii) Os 9 pontos de inflexão formam um subgrupo isomorfo a $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$.

(iii) A reta que une 2 pontos de inflexão intersecta F num 3º ponto de inflexão.

Demonstração.

(i) Seja L a tangente (inflexional!) de F em $\mathcal{O}$. Assim,

temos $(L)_F = 3\mathfrak{O}$. Por outro lado,

$$P\dot{+}Q\dot{+}R \equiv P+Q+R \equiv 3\mathfrak{O} \ ;$$

Portanto, o 1º membro é igual a $\mathfrak{O}$ se e só se valer $P+Q+R \equiv \mathfrak{O}$. Suponha válida esta última relação; seja H a reta determinada pelo par P,Q. Escrevamos $(H) = P+Q+R$. O quociente L/H fornece uma função racional cujo ciclo é $3\mathfrak{O}-(H)$. Concluimos que $R \equiv R'$ e portanto pelo Corolário 11, $R = R'$ como desejávamos. A recíproca deixamos para a distração do leitor.

(ii) Tendo em vista (i), é claro que P é um ponto de inflexão se e só se $3\cdot P = \mathfrak{O}$. Logo, o conjunto dos 9 pontos de inflexão coincide com o subgrupo formado pelos elementos de ordem 3. Que este grupo é isomorfo a $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$ segue-se facilmente: é o único grupo não cíclico de ordem 9.

(iii) Se $P+Q+R$ é o ciclo de interseção de F com uma reta, e se P, Q são pontos de inflexão, deduzimos primeiro que $P\dot{+}Q\dot{+}R = \mathfrak{O}$, e então, $3P \dot{+} 3Q \dot{+} 3R = \mathfrak{O}$, donde $3R = \mathfrak{O}$ e R é um ponto de inflexão.

C.Q.D.

14. Corolário. Se P,Q são pontos de inflexão de uma cúbica não singular F então existe uma projetividade M tal que $M.F = F$ e $MP = Q$.

Demonstração. Seja R o 3º ponto de inflexão colinear com P,Q. Procedendo como na demonstração da Proposição 1, podemos supor $R = (0:1:0)$ e F na forma $ZY^2 - X(X-Z)(X-\lambda Z)$. Se T

é a projetividade definida por

$$(x:y:z) \longmapsto (x:-y:z) \quad ,$$

é imediato que $T.F = F$. Por outro lado, P e TP são colineares com R. Visto que F não possui nenhum ponto de inflexão sobre $Y = 0$, segue-se que $P \neq TP$, e portanto $TP = Q$. (Veja a Fig. 7, na pág. 15).

C.Q.D.

Exercícios

14) Sejam $F = ZY^2 - X(X-1)(X+1)$, $\mathcal{O} = (0:1:0)$, $P = (0:0:1)$, $Q = (1:0:1)$, $R = (-1:0:1)$. Mostre que $\{\mathcal{O},P,Q,R\}$ é um subgrupo de F isomorfo a $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

15) Seja $F = ZY^2 - (X^3-43XZ^2+166Z^3)$, $P = (3:8:1)$. Calcule nP para cada inteiro n. ($\mathcal{O} = (0:1:0)$).

16) Mostre que a Proposição 12 subsiste mesmo se $\mathcal{O}$ não é um ponto de inflexão, modificando convenientemente a construção do inverso aditivo.

17) Mostre que a estrutura de grupo de uma cúbica não singular é independente do ponto escolhido para elemento neutro.

Nos exercícios seguintes, F denota uma cúbica não singular e $\mathcal{O} \in F$ é um ponto de inflexão escolhido para elemento neutro.

18) Se G é uma curva $\neq F$, então $(G)_F \equiv (\partial G)\mathcal{O}$.

19) Todo ciclo de F de grau 1 é racionalmente equivalente a um (único) ponto de F.

20) Sejam G,H curvas de grau d, distintas de F. Se $(G)_F = P + \sum_2^{3d} P_i$, $(H)_F = Q + \sum_2^{3d} P_i$, então $P = Q$. Em particular, qualquer cúbica passando por 8 dos 9 pontos de interseção de F com outra cúbica, conterá o 9º ponto.

21) Mostre que os elementos de ordem 2 de F são justamente os pontos de contato das tangentes a F passando por $\mathcal{O}$. O grupo gerado por esses elementos é isomorfo a $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

22) Seja $D = \sum_1^6 P_i$ um ciclo de grau 6 sobre F. Mostre que $D \equiv 6\mathcal{O}$ se e só se existir uma cônica C tal que $(C)_F = D$. Generalize!

23) As soluções da equação $6.P = \mathcal{O}$ consiste dos 9 pontos de inflexão juntamente com os 27 pontos de contato das retas tangentes passando pelos pontos de inflexão. Resulta um grupo isomorfo a $\mathbb{Z}/(6) \times \mathbb{Z}/(6)$.

BIBLIOGRAFIA

Além das referências anotadas no texto, sugerimos os seguintes títulos para leitura adicional. A ordem de apresentação corresponde aproximadamente à facilidade.

Os dois primeiros são uma ótima introdução à teoria das curvas algébricas:

- R.J. Walker, "Algebraic Curves", Dover (1962).
- W. Fulton, "Algebraic Curves, an introduction to Algebraic Geometry", W. A. Benjamin (1969).

Os três seguintes são livros básicos sobre variedades algébricas:

- I.R. Shafarevich, "Basic Algebraic Geometry", Springer-Verlag (1974).
- R. Hartshorne, "Algebraic Geometry", Springer-Verlag (1977).
- P. Griffiths, J. Harris, "Principles of Algebraic Geometry" Wiley - Interscience, 1978.

Informações sobre funções elíticas:

- L.V. Ahlfors, "Complex Analysis" Mc Graw-Hill (1966).
- A. Simis, "Introdução às funções algébricas e funções abelianas" IMPA (1975).

Para ler o prefácio:

- A. Grothendieck, J. Dieudonné, "Elements de Geómetrie Algébrique" Springer-Verlag (1971).

Miscelânea:

- S. Abhyankar, "Historical ramblings in Algebraic Geometry and related Algebra", American Math. Monthly 83 p. 409 (1976).
- J. Dieudonné, "Algebraic Geometry", Advances in Math. 3 p. 233 (1969).