

UNIVERSIDADE DE ÉVORA  
Departamento de Matemática

# Cúbicas Irredutíveis

Uma dissertação apresentada por  
*Olga Maria de Sousa da Silva Pinho*



Orientador da dissertação:  
Professor Doutor A. J. Franco de Oliveira

Esta dissertação não inclui as críticas e sugestões feitas pelo júri.

— 2003 —

UNIVERSIDADE DE ÉVORA  
Departamento de Matemática

# Cúbicas Irredutíveis

Uma dissertação apresentada por  
*Olga Maria de Sousa da Silva Pinho*



143818

Orientador da dissertação:  
Professor Doutor A. J. Franco de Oliveira

Esta dissertação não inclui as críticas e sugestões feitas pelo júri.

— 2003 —

512.77

# Resumo

Nesta tese vai ser apresentada uma classificação de um conjunto de curvas algébricas planas reais — as cúbicas irredutíveis. Para isso, é feita a caracterização destas curvas, através da identificação de pontos particulares nelas contidos, a que chamamos pontos singulares e flexões. Este estudo é feito no plano projectivo real, recorrendo a coordenadas homogéneas, sendo fundamentado na multiplicidade de intersecções entre cúbicas e rectas tangentes em pontos específicos, que nos é dada formalmente pela independência de polinómios.

Com a caracterização destas curvas, e recorrendo a resultados que envolvem o determinante da matriz hessiana de uma cúbica, classificamos todas as cúbicas irredutíveis. Com essa finalidade, necessitamos, no entanto, de alguns teoremas importantes, dos quais destacamos o Teorema de Bézout.

Juntamente a este estudo, é apresentado um percurso histórico da geometria algébrica, sendo também introduzida uma pequena selecção de curvas algébricas que, pelas suas características, ficaram famosas na história.

# Abstract

## Irreducibles Cubics

In this thesis, it is presented a classification of a set of real plane algebraic curves — the irreducibles cubics. Bearing this aim, the characterization of these curves is made through the identification of particular points contained in them, that we call singular points and flexes. This study is made in the real projective plane, using homogeneous coordinates, being based on the intersection multiplicities between cubics and tangent lines in specific points, that are formally given by the independence of polynomials.

By means of the characterization of these curves, and also using some results that involve the determinant of the hessian matrix of a cubic, we classify all the irreducibles cubics. For this purpose, however, we need some important theorems of which we emphasize Bézout's Theorem.

In addition, we present a brief historical survey of algebraic geometry, and a small selection of algebraic curves that, because of their properties, have become famous in the history of the subject.

# Agradecimentos

Desejo agradecer em especial ao meu orientador Professor Doutor A. J. Franco de Oliveira, a ajuda dispensada, dedicação, paciência e profissionalismo que sempre mostrou.

Quero também agradecer a duas pessoas que marcaram o meu percurso académico na área da geometria. A primeira pessoa que me despertou para a geometria no primeiro ano da minha licenciatura, o Professor Doutor Paulo Almeida, pelo entusiasmo com que trata a geometria. Ao Doutor Eduardo Veloso que tive a sorte de conhecer e ser presenteada com alguns dos seus cursos de geometria, pela forma como me motivou para o estudo das curvas algébricas.

Gostaria também de agradecer à minha família e aos meus amigos, que sempre me incentivaram e apoiaram durante todo este período.

## Prefácio

O estudo das curvas sempre exerceu um fascínio muito especial sobre os matemáticos, tendo sofrido o seu maior desenvolvimento no século XIX. Desde então, tem sido fonte de interesse e discussão, devido às propriedades que as curvas possuem e que nos permitem compreender muitas das lacunas existentes nas diversas áreas da ciência.

Nesta tese é feita uma classificação de um conjunto de curvas especiais que denominamos de cúbicas irredutíveis. Tendo como base a intersecção destas cúbicas com rectas e outras curvas, definimos pontos particulares, que nos permitem a sua caracterização. Com este objectivo definimos quatro capítulos. No primeiro capítulo, são introduzidos os fundamentos necessários para a compreensão do todo este estudo, dos quais destacamos a construção do plano projectivo real a partir do espaço euclidiano real através da adição de pontos no infinito. Aqui, é também apresentado o conceito de coordenadas homogéneas e definidos os vários tipos de rectas no plano projectivo real. São também tratados vários exemplos de curvas que ficaram famosas na história, devido a propriedades singulares que possuem.

No segundo capítulo é apresentado o percurso histórico da geometria algébrica, salientando os momentos mais notáveis e decisivos na evolução desta área. As curvas algébricas sempre tiveram interligadas com muitas outras áreas. Por esse motivo, no final deste capítulo, é dado especial relevo à importância da geometria algébrica na teoria dos números, através de um tema que muita polémica levantou — O Último Teorema de Fermat.

No capítulo III iniciamos o estudo da multiplicidade de intersecções entre curvas em pontos específicos. Em primeiro lugar é feita uma abordagem intuitiva e, posteriormente, é dada uma definição formal baseada na independência de polinómios.

Por fim, o capítulo IV é dedicado às cúbicas, nas quais são identificados pontos com características próprias. Estes pontos são definidos com base na intersecções destas curvas com rectas particulares. É através deles que fazemos a caracterização destas curvas, sendo esta a base da nossa classificação. Para isso necessitamos de resultados muito importantes, tais como o Teorema de Bézout, ao qual dedicamos uma secção. Por último, e através da matriz hessiana de uma cúbica, podemos chegar a resultados fundamentais que nos permitem concluir que temos classificadas todas as cúbicas irredutíveis.

# Índice

Capítulo I. Introdução.....	1
§1.1 Curvas algébricas.....	1
§1.2 Plano Projectivo.....	7
Capítulo II. Sinopse histórica da Geometria Algébrica.....	15
§2.1 «Pré-história» (circa 400 a.C.–1630 d.C.).....	16
§2.2 Explorando (1630–1795).....	17
§2.3 A idade de ouro da geometria projectiva (1795–1850).....	19
§2.4 Geometria de Riemann (1850–1866).....	21
§2.5 Desenvolvimento até aos dias de hoje (1866–...).....	24
Capítulo III. Intersecções.....	29
§3.1 Intersecção entre duas curvas na origem.....	29
§3.2 Intersecção em coordenadas homogéneas.....	39
§3.3 Independência e geradores.....	48
Capítulo IV. Cúbicas.....	69
§4.1 Tangentes, pontos singulares e flexões.....	70
§4.2 Cúbicas irredutíveis.....	79
§4.3 Teorema de Bézout.....	90
§4.4 Hessiana.....	96
Referências Bibliográficas.....	107

# Capítulo I | INTRODUÇÃO

Neste capítulo vamos apresentar os fundamentos necessários sobre os quais vamos trabalhar nos capítulos seguintes. Assim, vamos, numa primeira secção, definir curva algébrica e apresentar exemplos de algumas curvas que ficaram famosas pelas suas características. Numa segunda secção, construímos o plano projectivo real a partir do espaço euclidiano. Definimos o conjunto de pontos do plano projectivo e consequentemente introduzimos o conceito de coordenadas homogéneas. Por fim, definimos os vários tipos de rectas existentes no plano projectivo real. Antes de terminarmos, apresentamos dois teoremas fundamentais, um relativo à intersecção de duas rectas e um segundo relativo à existência e unicidade de rectas, dados dois pontos.

## §1.1 Curvas algébricas

Além da definição explícita usual  $y = f(x)$ , existem duas formas de se definir uma curva no plano real  $\mathbb{R}^2$ . A distinção é muito importante.

- Uma curva pode ser definida *parametricamente*, na forma  $x = x(t)$ ,  $y = y(t)$ , onde  $t$  é o parâmetro. A parametrização dá uma imagem dinâmica à estrutura, sendo possível calcular um vector tangente  $(x'(t), y'(t))$ , cujo valor representa a velocidade da curva em função do parâmetro  $t$ .

- Uma curva pode ser definida *implicitamente*, como o conjunto dos pontos  $(x, y)$  no plano que satisfazem uma equação  $f(x, y) = 0$ , onde  $f(x, y)$  é uma função de  $x$  e de  $y$ .

De um modo geral, o estudo das curvas parametrizadas está representado numa grande área da matemática chamada *Geometria Diferencial*, enquanto as curvas definidas implicitamente estão representadas numa outra área, a *Geometria Algébrica*. É nesta última que o nosso estudo vai incidir.

## I. Introdução

Uma curva algébrica em  $\mathbb{R}^2$  é definida implicitamente pela equação da forma  $f(x, y) = 0$ , em que  $f(x, y)$  é um *polinómio real* a duas variáveis  $x$  e  $y$ ,

$$f(x, y) = \sum_{i,j} a_{ij} x^i y^j,$$

sendo esta soma finita e os coeficientes  $a_{ij}$  números reais não todos iguais a zero.

O *grau da curva* é o grau de  $f(x, y)$  que é dado pelo máximo valor de  $i + j$ , onde  $i$  e  $j$  são os índices cujo coeficiente associado  $a_{ij}$  é diferente de zero. Curvas de graus 1, 2, 3, ... são chamadas rectas, cónicas, cúbicas, ..., sendo estas últimas objecto do nosso estudo.

Muitas vezes é necessário estender este conceito para situações onde os coeficientes  $a_{ij}$  pertençam a um corpo mais geral como, por exemplo, o corpo dos complexos  $\mathbb{C}$ .

Dado um polinómio  $f(x, y)$ , podemos definir o conjunto dos zeros de  $f$ , também denominado *variedade de  $f$* , como sendo

$$V_f = \{(x, y) \in \mathbb{R}^2 : f(x, y) = 0\}.$$

O conjunto dos zeros (e o seu grau) não se altera quando multiplicamos  $f$  por um escalar diferente de zero. Daí podermos concluir que “uma curva algébrica é um polinómio  $f$  real diferente de zero, a menos da multiplicação por um escalar diferente de zero”.

Desta forma, consideramos uma curva algébrica real como sendo uma classe de equivalência de polinómios para a relação de equivalência  $\sim$  definida do seguinte modo:  $f \sim g$  se e só se existe um escalar  $\lambda$ , diferente de zero, tal que  $f = \lambda g$ . Trivialmente se verifica que  $\sim$  goza das propriedades inerentes a uma relação de equivalência. É reflexiva ( $f \sim f$ ), simétrica (se  $f \sim g$ , então  $g \sim f$ ) e transitiva (se  $f \sim g$  e  $g \sim h$ , então  $f \sim h$ ).

### Exemplos Introdutórios de Curvas Algébricas

Vamos apresentar alguns exemplos de curvas algébricas reais, muitos dos quais tiveram especial importância na antiguidade.

Começemos por destacar a *Concóide de Nicomedes* (225 a.C.). Para se desenhar uma concóide é necessário uma curva genérica  $l$ , um segmento de recta de comprimento  $k$  e um ponto fixo  $O$ . Normalmente  $l$  diz-se a *curva base* e  $O$  o *polo da curva* resultante. Para se obter a concóide traçam-se rectas passando por  $O$  e marcam-se sobre cada uma dessas rectas pontos  $Q_1$  e  $Q_2$  que distam  $K$  «unidades» da intersecção da recta com a curva  $l$ , como mostra a Fig.1. A curva resultante vai ser o lugar geométrico dos pontos  $Q_1$  e  $Q_2$ .

## I. Introdução

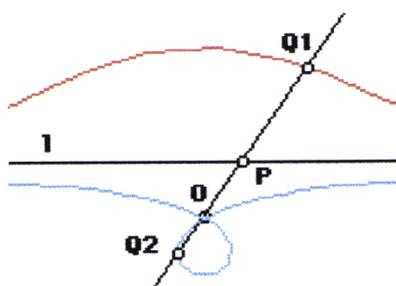


Fig. 1 — *Concóide de Nicomedes*

A *concóide* mais famosa é a de Nicomedes. Com ela, Nicomedes resolveu o problema da *trisseção do ângulo*. Na *concóide* de Nicomedes,  $l$  é uma recta e  $O$  é um ponto não pertencente a  $l$ , como mostra a figura anterior. Podemos observar que a *concóide* tem um ponto de intersecção  $O$  com características particulares que denominamos de *nó*.

A *concóide* de uma curva varia consoante o ponto fixo escolhido. Algumas escolhas particulares para o ponto fixo conduziram a resultados especialmente interessantes. Assim, a *concóide* de uma circunferência em relação a um ponto fixo que se situa sobre ela é a conhecida *limaçon* de Pascal Fig. 2. Esta curva foi descoberta por Étienne Pascal e denominada assim por Roberval em 1650 quando a usou para o seu método de desenhar tangentes. O nome *limaçon* vem do latim *limax* que significa caracol.

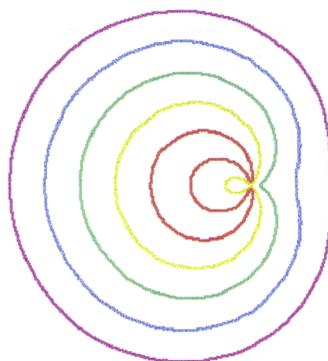


Fig. 2 — *Limaçon de Pascal*

Na *limaçon* de Pascal considera-se um segmento de recta  $AB$  de comprimento fixo, movendo-se de tal modo que a recta que o suporta passe sempre por um ponto fixo situado sobre uma circunferência e o ponto médio do segmento  $AB$  se situe sempre sobre ela. Os extremos do segmento descrevem a *limaçon*. Se o comprimento do segmento for igual ao dobro do diâmetro da circunferência, a *limaçon* reduz-se à *cardióide*.

## I. Introdução

Algumas destas curvas podem ser geradas por um ponto fixo a uma circunferência, que roda sem escorregar, circulando em torno de uma outra com o mesmo diâmetro. Por esse motivo chamam-se a estas curvas de *roulettes*. Duas das classe mais estudadas das roulettes são as conhecidas hipociclóides e epiciclóides. Em ambos os casos temos duas circunferências que designamos por  $b$  e  $c$  e  $P$  é um ponto pertencente a uma delas, no entanto, nas hipociclóides, a circunferência que roda está no interior da circunferência fixa, enquanto nas epiciclóides passa-se precisamente o contrário. Epiciclóides e hipociclóides foram usadas (provavelmente a partir do século XVII) para desenhar o então conhecido *gerador cicloidal*. Como seria de esperar, a forma destas curvas depende da relação entre os raios das duas circunferências, a que roda e a que está fixa. Se a circunferência que rola for a exterior, se o ponto fixo estiver exactamente sobre a circunferência e, ainda, se o raio de  $b$  for igual ao raio de  $c$ , geramos a *cardióide*. A *cardióide* é uma epiciclóide com forma de coração cuja equação é

$$(x^2 + y^2 - 2bx)^2 = 4b^2(x^2 + y^2),$$

onde  $b$  representa o raio da circunferência centrada num ponto no eixo das abcissas como mostra a figura seguinte.

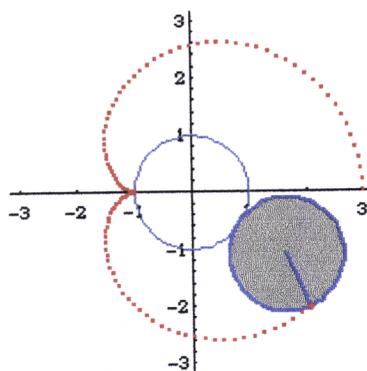


Fig. 3

A curva *nefróide* (forma de rim) é também uma epiciclóide em que  $c = 2b$ . Como hipociclóides famosas temos a *deltóide*, em que  $3b = c$ , e a *astróide*, em que  $4b = c$ . As suas equações no sistema de coordenadas rectangulares são dadas por:

$$\begin{aligned} (x^2 + y^2 - 4b^2)^3 &= 108b^4y^2 && \text{— Nefróide} \\ (x^2 + y^2)^2 - 8bx(x^2 - 3y^2) + 18b^2(x^2 + y^2) &= 27b^4 && \text{— Deltóide} \\ (x^2 + y^2 - b^2)^3 + 27b^2x^2y^2 &= 0. && \text{— Astróide.} \end{aligned}$$

## I. Introdução

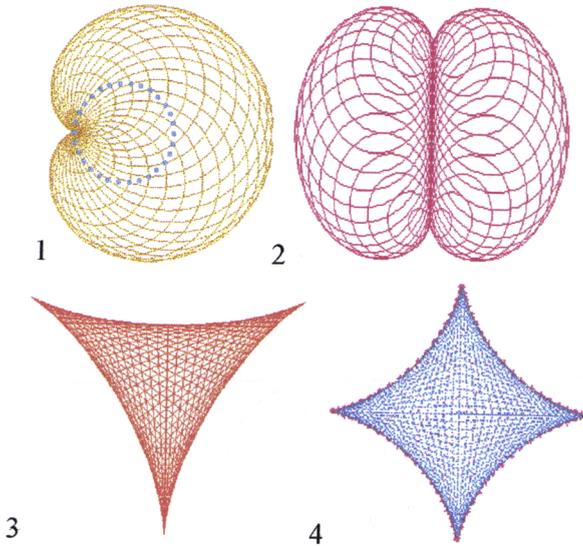


Fig. 4 — 1. *Cardioid*; 2. *Nefróide*; 3. *Deltóide*; 4. *Astróide*

A figura degenerada de uma epiciclóide, que ocorre quando a circunferência fixa é substituída por uma recta, é denominada de ciclóide (Fig. 5). Esta curva foi descoberta por Bernoulli por volta de 1700. É uma curva muito interessante que tem a particularidade de dados dois pontos no plano vertical, ser a curva que define o menor tempo que uma partícula demora a percorrer quando sujeita à gravidade. É o tão conhecido problema da braquistócrona. Também, uma partícula que percorra uma trajectória cicloidal, com o eixo da ciclóide na vertical atingirá o ponto mais baixo ao fim do mesmo tempo, seja qual for o ponto de partida. Por outras palavras, além de ser braquistócrona, a ciclóide é tautócrona.

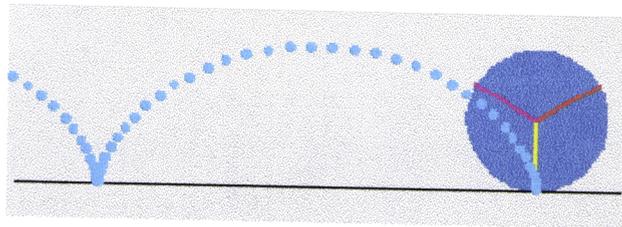


Fig. 5 — *Ciclóide*

Outra curva descoberta pelos Gregos é a *cissóide de Diocles*. Esta curva pode ser construída a partir de duas outras curvas  $c$  e  $l$  e de um ponto fixo  $O$ . Uma recta que passa por  $O$  é desenhada intersectando  $c$  e  $l$  em dois pontos  $P_1$  e  $P_2$ . Determina-se o ponto  $Q$  de forma a

## I. Introdução

que este satisfaça a igualdade  $|OQ| = |P_1P_2|$ , cujos comprimentos são medidos pela das letras indicada. O lugar geométrico dos pontos  $Q$  definem a cissóide.

Na cissóide de Diocles as curvas  $c$  e  $d$  são uma circunferência e uma recta tangente, respectivamente, o ponto  $O$  está situado sobre a circunferência diametralmente oposto ao ponto de tangência (Fig. 6). Se passarmos o ponto para a origem e a recta tangente para  $x = a$ , obtemos a cissóide cuja equação é definida do seguinte modo

$$y^2(x - a) = x^3.$$

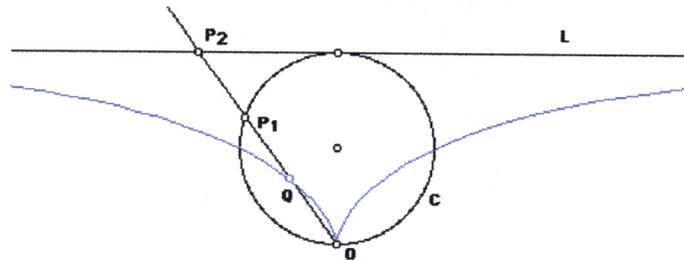


Fig. 6 — Cissóide

Ao ponto  $O$  denominamos *cúspide* que consiste num ponto de retorno. Este tipo de pontos, *pontos singulares*, vão ser estudados no capítulo IV, sendo a cissóide talvez o mais antigo exemplo (c. 180 b.C.) de curva com tal singularidade.

Diocles usou a *cissóide* para resolver o problema da *duplicação do cubo*.

Por volta de 150 b.C., um matemático Grego Perseus, teve a ideia de cortar um toro por um plano paralelo ao eixo de rotação, obtendo curvas muito interessantes. Devido aos Gregos chamarem o toro de *spira*, estas curvas ficaram conhecidas pelas *secções spiric de Perseus*. Delas destacamos as *curvas Cassini* que definimos do seguinte modo: são dados dois pontos  $A$  e  $B$  que distam  $2a$ ; a curva de Cassini associada vai ser o lugar geométrico de todos os pontos  $P$  tais que  $|PA| \times |PB| = c^2$ , sendo  $c$  uma constante positiva. Para  $A$  e  $B$  fixos e valores diferentes de  $c$ , estas curvas assemelham-se às da Fig. 7. Estas curvas foram descobertas pelo astrónomo Giovanni Domenico Cassini (c. 1650-1700). Ele acreditava que o sol movimentava-se à volta da terra segundo uma curva convexa deste tipo.

## I. Introdução

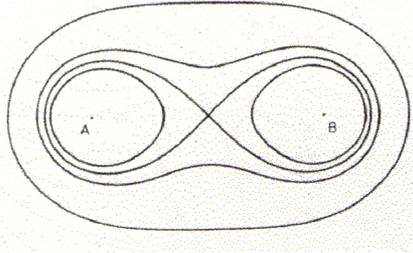


Fig. 7 — Curva Cassini

Quando  $a = c$  obtemos a *lemniscate* de Jacob Bernoulli (1694). Esta foi uma curva que grande importância teve no desenvolvimento da teoria das funções elípticas.

Nesta altura e na área da óptica, surgem as *cáusticas* como curvas algébricas reais de grande interesse, que foram investigadas por Tschirnhausen e Huygens, no final do século XVII. Para se obter uma cáustica é necessário uma curva e uma fonte de luz fixa. Os raios de luz provenientes da fonte e reflectidos (ou refractados) pela curva, envolvem uma nova curva chamada a cáustica da curva de partida. A cáustica de uma circunferência produzida por reflexão, pode ver-se grosseiramente quando uma lâmpada ilumina o interior de uma taça e os raios de luz são reflectidos sobre a superfície do líquido. A cáustica de uma circunferência é, de um modo geral, um *limaçon*. Há três posições excepcionais para a fonte de luz. Quando colocada no infinito, a cáustica obtida é uma nefróide, se a fonte de luz estiver sobre a circunferência, é uma cardióide, e se estiver no centro da circunferência é o próprio centro da circunferência.

## §1.2 Plano projectivo

Nesta segunda secção vamos construir o plano projectivo (real) a partir do espaço euclidiano (real), através da adição de pontos no infinito. Vamos definir pontos e rectas no plano projectivo, sendo para isso necessário introduzir o conceito de *coordenadas homogéneas*. Trabalhar no plano projectivo oferece-nos muitas vantagens. O estudo das curvas algébricas pode ser largamente simplificado se considerarmos o comportamento dessas curvas no infinito. Uma outra vantagem em trabalharmos neste plano deve-se ao facto de não necessitarmos de efectuar estudos particulares para casos de rectas paralelas, pois estas vão sempre intersectar-se, mesmo que somente no infinito. Duas rectas paralelas no plano euclidiano,  $z = 1$ , intersectam-se no infinito no plano projectivo. Esta afirmação vai ser apresentada e demonstrada no final desta secção sob a forma de um teorema. Vamos também

## I. Introdução

estender para o plano projectivo um outro resultado sobejamente conhecido do plano euclidiano, que nos diz que, dados dois pontos, existe sempre uma única recta que os contém.

Comecemos com o espaço euclidiano real, onde temos um sistema de três eixos coordenados perpendiculares entre si, cuja intersecção é a origem. Todos os pontos que se situam numa mesma recta do espaço euclidiano que passa pela origem vão representar o mesmo ponto no plano projectivo. Temos, no entanto, que excluir deste conjunto de pontos a origem, que não faz parte do plano projectivo. Assim, ao considerarmos o ponto  $(a, b, c)$ , onde que  $a, b$  e  $c$  não são simultaneamente iguais a zero, todos os pontos do tipo  $(ta, tb, tc)$ , para todo o  $t \in \mathbb{R} \setminus \{0\}$ , representam o mesmo ponto no plano projectivo, pois todos eles estão situados numa mesma recta do espaço euclidiano que passa pela origem. Chamamos *coordenadas homogéneas* a esses tripos ordenados de números reais.

Quando, nos tripos, a última coordenada é diferente de zero, as coordenadas homogéneas permitem-nos reduzir a dimensão dos tripos ordenados para pares ordenados. Assim, se considerarmos os pontos  $(a, b, c)$  com  $c \neq 0$  e consideramos  $t = \frac{1}{c}$ , obtemos o ponto  $(\frac{a}{c}, \frac{b}{c}, 1)$  do plano projectivo, que pode ser comparado ao ponto  $(\frac{a}{c}, \frac{b}{c})$  do plano euclidiano. Desta forma, todos os pontos  $(a, b, c)$  que pertencem a rectas que passam pela origem e que não estão contidas no plano  $z = 0$  têm um representante no plano  $z = 1$  que consiste no ponto  $(\frac{a}{c}, \frac{b}{c}, 1)$ . Por sua vez, identificamos as rectas que passam na origem e que estão contidas no plano  $z = 0$ , como sendo rectas que intersectam o plano  $z = 1$  no infinito e, portanto, a estas rectas vão corresponder pontos no infinito. Desta forma, podemos pensar no plano projectivo como sendo constituído pelo plano euclidiano  $z = 1$  a que juntámos pontos adicionais — os *pontos no infinito*.

Algebricamente, se  $c \neq 0$ , então  $\frac{1}{c}$  representa o valor de  $t$  tal que o triplo  $(ta, tb, tc)$  tem última coordenada igual a um. O conjunto destes pontos representam o plano  $z = 1$ . Reciprocamente, a todos os pontos  $(d, e, 1)$  do plano  $z = 1$  corresponde um único ponto no plano projectivo com coordenadas homogéneas  $(td, te, t)$ , para todo o  $t \neq 0$ . Neste panorama faz sentido estabelecer uma correspondência entre o plano projectivo cuja última coordenada é diferente de zero com os pontos do plano  $z = 1$ .

Até agora temos pensado apenas em pontos cuja última coordenada é diferente de zero. Vejamos agora os pontos cuja última coordenada é zero, ou seja, pontos situados no plano  $z = 0$ . Comecemos pelos pontos  $(a, b, 0)$  do plano projectivo em que  $a \neq 0$ . Se considerarmos  $t = \frac{1}{a}$ , temos a forma geral destes tripos  $(1, \frac{b}{a}, 0)$ . Se  $a = 0$  e  $b \neq 0$  [note-se que o ponto

## I. Introdução

$(0, 0, 0)$  não pertence ao plano projectivo] e tomarmos  $t = \frac{1}{b}$ , obtemos um único ponto de coordenadas homogéneas  $(0, 1, 0)$ .

Assim, de forma resumida, no plano projectivo existem dois tipos genéricos de pontos:

- os pontos de coordenadas homogéneas em que a última coordenada é diferente de zero, e que têm como representantes os pontos do tipo  $(\frac{a}{c}, \frac{b}{c}, 1)$ , correspondentes aos pontos do plano euclidiano  $z = 1$ ; e

- os pontos de coordenadas homogéneas do tipo  $(1, \frac{b}{a}, 0)$  e do tipo  $(0, 1, 0)$  que correspondem aos pontos no infinito e que representam as rectas que estão contidas no plano  $z = 0$ .

De forma esquemática e simplista podemos apresentar o plano projectivo como um quadrado e uma curva como mostra a Fig. 8. O quadrado representa o plano euclidiano  $z = 1$  e a curva  $m$  representa a recta no infinito que é constituída por todos os pontos no infinito.

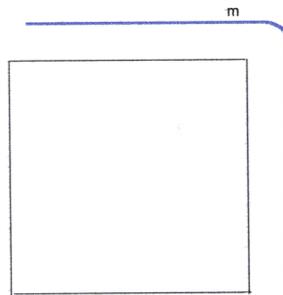


Fig. 8

Sem antes passarmos ao estudo das rectas do plano projectivo real, gostaríamos de estabelecer uma generalização deste plano para um outro que por vezes permite-nos grandes simplificações. Estamos obviamente a falar do *plano projectivo complexo*. O plano projectivo complexo consiste em todos os triplos  $(x, y, z)$  de números complexos excepto o  $(0, 0, 0)$ , onde os triplos  $(kx, ky, kz)$  para  $k \in \mathbb{C} \setminus \{0\}$  representam o mesmo ponto. Se pensarmos nos triplos dos números reais como triplos de números complexos, concluímos que o plano projectivo real está contido no plano projectivo complexo.

Também o plano euclidiano real pode ser generalizado para o *plano complexo afim*, que consiste em todos os pares ordenados  $(x, y)$  de números complexos. De forma análoga com o que ocorre no plano euclidiano real, também no plano complexo afim, identificamos cada ponto  $(x, y)$  com o ponto  $(x, y, 1)$  do plano projectivo complexo. Reciprocamente, podemos identificar cada ponto  $(x, y, z)$ , em que  $z \neq 0$ , do plano projectivo complexo de forma única

## I. Introdução

com o ponto  $(x', y', 1)$ , do plano complexo, cuja última coordenada é diferente de zero. Quando a última coordenada é zero, o ponto é identificado com um ponto no infinito tal como ocorre no plano projectivo real.

Ainda de uma forma mais abstracta poderíamos generalizar todos estes conceitos para um plano nem real nem complexo, mas segundo um outro corpo genérico que designaríamos por  $K$ .

O nosso estudo incide essencialmente sobre o corpo dos reais. Por esse motivo, quando nada é dito sobre corpo em estudo é porque estamos a trabalhar sobre o conjunto dos números reais. Assim, nos capítulos III e IV vamos trabalhar sobre os complexos para que possamos deduzirmos um resultado fundamental conhecido por *Teorema de Bézout*, que nos possibilitará a classificação das cúbicas irredutíveis. Daí a importância de, ao longo deste trabalho, definirmos alguns conceitos sobre o plano complexo afim e plano projectivo complexo.

Falemos agora das rectas do plano projectivo real.

Uma recta no plano projectivo é um conjunto de pontos com coordenadas homogéneas  $(x, y, z)$  que satisfazem uma igualdade da forma

$$px + qy + rz = 0, \quad (1)$$

com  $p, q, r$  reais não todos nulos. Obviamente que se  $p, q, r$  forem complexos não todos nulos temos uma recta no plano projectivo complexo.

Ao multiplicarmos a igualdade (1) membro a membro por  $t$  obtemos  $ptx + qty + rtz = 0$ , o que mostra que os triplos  $(tx, ty, tz)$  também satisfazem (1).

Consideremos, primeiramente, o caso  $q \neq 0$ . De (1) obtemos

$$y = \left(-\frac{p}{q}\right)x + \left(-\frac{r}{q}\right)z, \text{ ou } y = mx + nz,$$

com  $m, n \in \mathbb{R}$ . As correspondentes rectas do plano euclidiano, são constituídas pelos pontos  $(x, y)$ , que satisfazem  $y = mx + n$ , ou seja todas as rectas não verticais.

Consideremos agora o caso  $q = 0$  e  $p \neq 0$ . Da igualdade (1) obtemos

$$x = \left(-\frac{r}{p}\right)z, \text{ ou } x = mz,$$

com  $m \in \mathbb{R}$ . As correspondentes rectas no plano euclidiano consistem no conjunto de pontos  $(x, y)$  que satisfazem  $x = m$ , ou seja todas as rectas verticais.

Por fim, se considerarmos o caso  $p = 0 = q$  e  $r \neq 0$  obtemos de (1) a equação  $z = 0$ . Neste caso temos a recta no infinito do plano projectivo que não tem correspondente no espaço euclidiano.

## I. Introdução

Em resumo, temos dois tipos de rectas: as rectas cuja equação geral é  $y = mx + nz$  e  $x = mz$  correspondentes, respectivamente, às rectas não verticais e verticais do plano euclidiano; e a recta no infinito que contém todos os pontos no infinito e cuja equação geral é  $z = 0$ . Cada ponto no infinito pertence a uma família de rectas do plano euclidiano paralelas entre si. Assim, a recta no infinito vai conter as direcções de todas as famílias de rectas paralelas do plano euclidiano. Podemos verificar esta afirmação se pensarmos nos pontos no infinito de coordenadas  $(1, s, 0)$  e  $(0, 1, 0)$  para  $s \in \mathbb{R}$ . Um ponto de coordenadas  $(1, s, 0)$  pertence à recta  $y = mx + nz$  desde que  $m = s$  (note-se que no plano euclidiano esta recta corresponde à recta  $y = mx + n$ ), logo, consoante o declive  $m$ , temos um ponto no infinito. O ponto de coordenadas  $(0, 1, 0)$  pertence à recta  $x = mz$ , qualquer que seja  $m$ . Assim, existe um ponto no infinito que pertence às famílias de rectas verticais do plano euclidiano.

As rectas do tipo  $y = mx + n$  e  $x = m$  do plano euclidiano estendem-se às rectas  $y = mx + nz$  e  $x = mz$  do plano projectivo. Mais adiante, vamos confirmar que a recta no infinito  $z = 0$  não é extensão de nenhuma recta do plano euclidiano pois o polinómio  $z$  não é o homogeneizado de nenhum polinómio em  $x$  e  $y$ .

No plano projectivo complexo as rectas têm a mesma caracterização com a diferença que os coeficientes passam a ser números complexos.

Chegámos ao momento de enunciar dois teoremas fundamentais do plano projectivo. Um primeiro que se refere ao facto de dadas duas rectas existir sempre um e um só ponto resultante da intersecção dessas duas rectas, e um segundo referente à existência e unicidade de uma recta dados dois pontos.

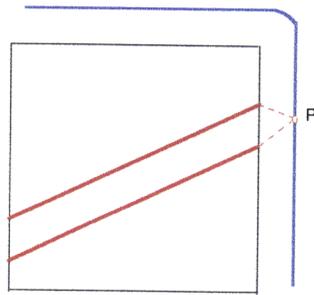
### **Teorema 1.1**

*Duas rectas do plano projectivo intersectam-se sempre num único ponto.*

### **Demonstração**

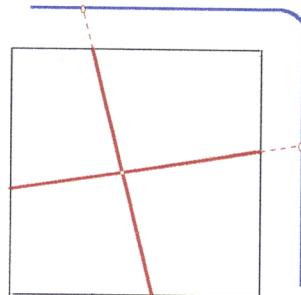
Vamos considerar os três casos possíveis. No primeiro temos duas rectas que não se intersectam no plano euclidiano (Fig. 9). Neste caso, as duas rectas são paralelas, logo pertencentes a uma família de rectas paralelas entre si que têm um mesmo ponto em comum, o ponto no infinito que pertence a essa direcção.

## I. Introdução



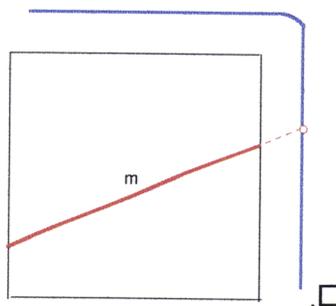
*Fig. 9*

No segundo caso vamos considerar duas rectas que se intersectam num ponto do plano euclidiano (Fig. 10). Neste caso, também no plano projectivo o ponto de intersecção é único, visto elas não terem nenhum ponto em comum da recta no infinito.



*Fig. 10*

Por fim, consideremos duas rectas em que uma é a recta  $m$  pertencente ao plano euclidiano e a outra é a recta no infinito (Fig. 11). Estas rectas intersectam-se num ponto no infinito, a saber, o ponto correspondente à direcção da família de rectas paralelas à recta euclidiana  $m$ .



*Fig. 11*

## I. Introdução

### Teorema 1.2

*Para quaisquer dois pontos do plano projectivo existe uma única recta que os contém.*

### Demonstração

Vamos considerar três casos que vão cobrir todas as possibilidades de pontos do plano projectivo.

Num primeiro temos dois pontos  $A$  e  $B$  pertencentes ao plano euclidiano (Fig. 12). Neste caso, pelo teorema equivalente referente ao plano euclidiano podemos garantir a existência de uma única recta que os contém. No plano projectivo continua a ser essa recta que os contém. Obviamente que a recta no infinito não contém esses dois pontos.

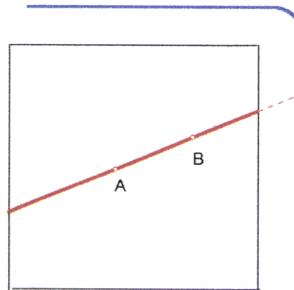


Fig. 12

Numa segunda situação temos dois pontos  $A$  e  $B$  pertencentes à recta no infinito (Fig. 13). Agora existe apenas uma recta que os contém, a recta no infinito. A unicidade advém do facto dessa recta ser única.

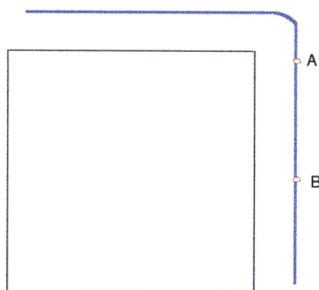
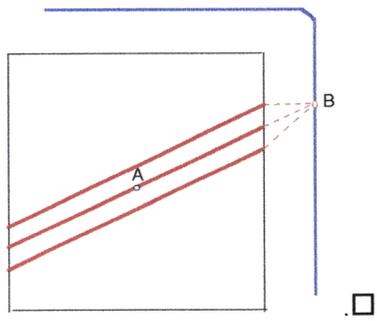


Fig. 13

Por último temos um ponto  $A$  no plano euclidiano e um ponto  $B$  na recta no infinito (Fig. 14). A recta que os contém vai ser a recta que passa por  $A$  e é paralela às rectas que contém também  $B$ .

I. Introdução



*Fig. 14*

# Capítulo II

## SINOPSE HISTÓRICA DA GEOMETRIA ALGÉBRICA

A geometria algébrica moderna tem sido considerada desde há muito tempo um ramo muito complexo da matemática, surgindo como uma ferramenta indispensável para construir conceitos e métodos em todas as demais áreas da matemática.

Em conjunto com a teoria dos números, a geometria algébrica tem uma das mais longas e complicadas histórias quando comparada com os outros ramos das ciências, tendo sido presenteada, ao longo das várias gerações, pelos contributos dos melhores matemáticos de todos os tempos. Estas duas áreas sempre tiveram mais problemas em aberto do que propriamente resolvidos, daí o interesse no seu progresso de forma que possibilite encontrar resoluções para problemas que arrastam consigo um conjunto de novos e interessantes métodos. Segundo Hilbert, estas duas áreas são as melhores candidatas da teoria matemática perfeita, consideradas segundo ele o “sangue” da matemática.

A mente humana tem grande dificuldade em chegar a matérias complexas como um todo. O que em geral faz é dissecar os problemas através da divisão em problemas menores para, posteriormente, voltar a agrupá-los e então compreender o todo. Talvez por isso seja útil descrever a história da geometria algébrica como uma espécie de modelo multidimensional, onde existem variadas ramificações pertencentes a variados assuntos. Estes assuntos interligam-se e portanto qualquer divisão no tempo em períodos é muito limitativa, havendo em geral sobreposição. Contudo, uma tentativa vai ser feita neste sentido ao longo deste capítulo. Iremos começar por introduzir um primeiro grupo de ideias inerentes a este assunto, para que possamos, posteriormente, iniciar a nossa caminhada ao longo da história da geometria algébrica.

Assim, as ideias mais importantes inerentes a esta área vão ser:

- *Classificação e transformação.* Estes dois assuntos surgem associados. A classificação é feita através da noção de invariância. As variedades algébricas, que podem ser deduzidas a partir de outras através de transformações, são classificadas num mesmo grupo. Note-se que falamos em transformações de uma forma geral, no entanto estas serão definidas no capítulo III.

## II. Sinopse Histórica da Geometria Algébrica

- *Pontos infinitamente próximos.* Desta ideia surge o conceito de singularidades, que iremos trabalhar, bem como a multiplicidade de intersecções;
  - *Extensão do corpo de escalares.* Para uma melhor simplicidade introduziremos os pontos complexos e mais tarde os pontos genéricos que são os percursos de um dos aspectos mais importantes da geometria algébrica — a ideia de mudança de bases;
  - *Extensão do espaço.* Aqui destacamos a geometria projectiva e a geometria  $n$ -dimensional, que nos permite avançar no sentido de alcançar os conceitos modernos das variedades abstractas;
  - *Análise e Topologia na geometria algébrica.* Este é o tema que melhor estabelece a relação existente entre os vários ramos da matemática. Dele salientamos um dos conceitos mais importantes — o de superfície de Riemann;
  - *Álgebra comutativa e geometria algébrica.* Com Riemann surge o corpo das funções racionais de uma curva, posteriormente, com Kronecker, Dedekind e Weber, surgem os conceitos de ideais e de divisores. Estes, juntamente com a álgebra comutativa, definem uma base fundamental, onde a geometria algébrica vai buscar as suas ferramentas (anéis locais, valuações, normalização, teoria de campo e mais recentemente a álgebra homológica).
- Após a introdução destas ideias iniciais vamos então iniciar a nossa divisão temporal da história da geometria algébrica.

### §2.1 «Pré-história» (circa 400 a.C.–1630 d.C.)

Os Gregos inventaram a geometria como ciência dedutiva usada essencialmente para resolver problemas algébricos. Este facto é bem visível nas primeiras curvas estudadas depois das rectas e das circunferências — *as cónicas*.

Tinham métodos geométricos muito sofisticados mas poucos conhecimentos algébricos. Para eles uma circunferência não era definida pela equação

$$(x - a)^2 + (y - b)^2 = r^2,$$

mas como o lugar geométrico de todos os pontos que têm igual distância  $r$  a um ponto fixo  $P = (a, b)$ . Analogamente, a parábola, para os Gregos, era definida como o lugar geométrico de todos os pontos que têm igual distância a um ponto  $P$  e a uma recta dada  $l$ , enquanto a elipse (hipérbole) era definida como o lugar geométrico de todos os pontos cuja soma (diferença) das distâncias as dois pontos dados  $P$  e  $Q$  é um valor fixo.

## II. Sinopse Histórica da Geometria Algébrica

Desenvolveram mecanismos complicados para construir parábolas, elipses e hipérbolas. Mas também conheciam construções geométricas mais simples que lhes permitiam determinar a raiz da equação  $x^2 = ab$ , onde  $a$  e  $b$  representam comprimentos de segmentos. O desconhecido  $x$  era visto como um lado de um quadrado e desta forma trabalhavam a equação escrevendo-a como uma proporção  $\frac{a}{x} = \frac{x}{b}$ . Um dos problemas desenvolvidos foi o conhecido *problema de Delic* (duplicação do cubo) onde se pretendia construir um segmento de comprimento  $x$  dada a equação  $x^3 = a^2b$  (para o problema da duplicação do cubo queremos que  $b = 2a$ ). Este era transformado, segundo Hipócrates de Quios (420 a.C.), na proporção dupla  $\frac{a}{x} = \frac{x}{y} = \frac{y}{b}$ , em que  $x$  e  $y$  eram dois comprimentos de segmentos desconhecidos. Problemas semelhantes a este foram também trabalhados muitos deles através do uso de régua e compasso. Como exemplos podemos referir a trisseccção de um ângulo arbitrário ou a construção de um polígono regular. Mas falharam. Mais tarde, Galois mostra que estas construções são impossíveis de se realizarem com régua e compasso.

Com os vários problemas trabalhados pelos Gregos, em particular na teoria das cónicas de Apolónio, tudo leva a crer que já faziam uso das coordenadas sem, contudo, chegarem à abordagem mais tarde alcançada por Decartes e Fermat. O método de resolver equações através de intersecções de curvas usado no século V a.C. levou ao aparecimento de várias curvas algébricas e transcendentess, não sendo ainda feita a distinção entre ambas.

Para além das rectas, circunferências, elipses, parábolas e hipérbolas, os Gregos conheciam construções para muitas outras curvas, tais como as curvas epiciclóides usadas para descrever os movimentos dos planetas, que mais tarde foram descritas pelas tão conhecidas leis de Kepler.

Os Gregos estudaram também superfícies de revolução, tais como o cone, o cilindro e até mesmo o toro. Deste assunto destacamos três nomes: Menecmo, o primeiro a reconhecer que era possível obter uma secção plana do cone de revolução; Arquitas (século V a.C.) que resolveu o *problema de Delic* através da intersecção de um cilindro com um toro; Eudócio que nos deixou um primeiro exemplo da representação paramétrica de uma curva.

### §2.2 Explorando (1630–1795)

Os matemáticos Gregos foram esquecidos na Europa Ocidental por muitos séculos após a queda do Império Romano, mas na Idade Média e principalmente no Renascimento foram gradualmente redescobertos através dos contactos com os matemáticos Árabes. Durante o

## II. Sinopse Histórica da Geometria Algébrica

Renascimento novas curvas algébricas foram descobertas por artistas, nomeadamente, Leonardo da Vinci.

O final do século XVII está bem definido pela *geometria analítica* que surge com Fermat e Decartes. Este facto marca, certamente, o verdadeiro nascimento da geometria algébrica. É nesta altura que se dá a distinção entre as curvas algébricas e transcendentais. A concepção de dimensão é já clara para Fermat, que explicita situações onde define uma curva a duas dimensões ou uma superfície a três dimensões.

O método do cálculo diferencial começa a ser gradualmente compreendido e aplicado às curvas.

A palavra chave deste período é a *exploração*. Fermat mostra que todas as curvas de grau dois são cónicas. Newton classifica as curvas cúbicas planas que se encontram no capítulo *Curves de Lexicon Technicum*, escrito por John Harris e publicado em Londres em 1710. Classifica todas as cúbicas em 72 tipos, mostrando que as suas equações podem ser simplificadas (no plano euclidiano) para uma das seguintes formas

$$\begin{aligned}xy^2 + ey &= ax^3 + bx^2 + cx + d, \\xy &= ax^3 + bx^2 + cx + d, \\y^2 &= ax^3 + bx^2 + cx + d, \\y &= ax^3 + bx^2 + cx + d,\end{aligned}$$

quando escolhido um sistema de eixos apropriado que, na época, não necessitava que os eixos fossem ortogonais.

Esta classificação foi bastante criticada por Euler por ser muito geral. Plücker apresentou, mais tarde, uma nova classificação com maior detalhe, compreendendo cerca de 219 tipos de curvas.

Surge a classificação de Euler das quádras e das primeiras curvas assimétricas obtidas por intersecção de duas superfícies. Nesta altura, o conceito de representação paramétrica de uma curva passa a ser fundamental.

O problema da intersecção de duas curvas vai ser tratado com Newton. Ele e Leibniz chegam a um *processo de eliminação* que permite determinar a multiplicidade de intersecções num ponto pertencente a duas curvas. Este processo consiste no seguinte: dadas duas curvas  $f(x, y) = 0$  e  $g(x, y) = 0$ , pretende-se eliminar a maior potência de  $y$  num dos polinómios  $f$  ou  $g$ , através da soma simultânea de múltiplos de  $f$  e  $g$  (todo este procedimento pode também ser feito em relação a maior potência de  $x$ ). Seguindo este raciocínio vai-se eliminando todas as potências de  $y$ , obtendo-se, no final, um polinómio  $r(x)$  com grau mínimo, denominado

resultante de  $f$  e  $g$ , tal que

$$r(x) = f(x, y)u(x, y) + g(x, y)v(x, y)$$

onde  $u$  e  $v$  são polinómios. Se  $f$  e  $g$  não se intersectarem no infinito ou em dois pontos do plano complexo afim com a mesma abcissa, as raízes de  $r(x)$  são as abscissas das intersecções de  $f$  e  $g$  e a multiplicidade dada de cada raiz é a multiplicidade correspondente à intersecção.

O processo de eliminação foi descoberto no século XII pelos matemáticos Chineses. Em 1665, Newton afirma que curvas de graus  $m$  e  $n$  intersectam-se  $m \times n$  vezes quando incluímos as intersecções imaginárias. Em 1720, Colin Maclaurin explora esta afirmação e deduz que uma curva irredutível de grau  $n$  tem no máximo  $\frac{(n-1)(n-2)}{2}$  pontos singulares. Em 1764, independentemente Etienne Bézout e Lenhard Euler desenvolvem explicitamente o algoritmo da eliminação e concluem que o produto dos graus de dois polinómios de determinada tipo é o grau dos seus resultantes. A demonstração completa deste teorema é dada por Bézout, quando vários resultados são combinados com as coordenadas homogéneas. Uma versão melhorada deste teorema diz-nos que: *dadas duas curvas  $f(x, y) = 0$  e  $g(x, y) = 0$  de graus  $m$  e  $n$ , respectivamente, e sem factores em comum, então  $f(x, y) = 0$  e  $g(x, y) = 0$  intersectam-se no plano projectivo complexo  $m \times n$  vezes contando as multiplicidades.*

## §2.3 A idade de ouro da geometria projectiva (1795–1850)

Com este período surge uma nova era. Este facto é devido a Monge e à sua escola e, especialmente, a Poncelet com a introdução de pontos imaginários e de pontos no infinito. Nesta altura e durante quase 100 anos, a geometria vai ser a geometria no plano projectivo complexo  $P_2(\mathbb{C})$  ou no espaço 3-dimensional projectivo complexo  $P_3(\mathbb{C})$ .

A ideia fundamental de geometria projectiva real surge com Desargues (século XVII) ao tentar dar fundamento à matemática com o método da perspectiva usado pelos pintores e arquitectos do Renascimento. Ele usa a concepção de pontos no infinito e usa a projecção central como meio de chegar a novos teoremas de resultados clássicos da geometria euclidiana. Estas ideias, também inspiradas por Pascal no seu trabalho com as cónicas, foram esquecidas, tendo-se mesmo pensado que estes trabalhos tivessem sido perdidos.

## II. Sinopse Histórica da Geometria Algébrica

Outros matemáticos do século XVIII, tais como Euler e Stirling, fizeram alusão à existência de pontos imaginários de forma a poderem enunciar alguns teoremas sem destacarem casos especiais.

Com Möbius e Plücker na Alemanha e Cayley em França, surgem as *coordenadas homogêneas*. Esta tendência da escola projectiva tinha como finalidade minimizar, tanto quanto possível, a computação algébrica para apoiar-se em princípios heurísticos, os quais não necessitavam de justificar algebricamente.

August Ferdinand Möbius foi o primeiro a introduzir as coordenadas homogêneas em 1827. Quando as massas  $m_1$ ,  $m_2$  e  $m_3$  eram colocadas nos vértices de um tetraedro fixo, Möbius dava ao centro de gravidade (baricentro) destas massas as coordenadas  $m_1 : m_2 : m_3$  e mostrava como estas são próprias para descrever as propriedades projectivas e afins do plano. As coordenadas homogêneas, a partir desta altura, tornaram-se um instrumento fundamental no tratamento algébrico da geometria projectiva.

Em 1830 Julius Plücker, no livro *Neue Geometrie des Raumes*, reconstrói a geometria analítica aplicando grande profusão de novas ideias. É neste livro que introduz as coordenadas homogêneas, conhecidas como coordenadas projectivas, baseadas num tetraedro fundamental.

Plücker vai sustentar o princípio fundamental, que a geometria não necessita de assentar no conceito de ponto como elemento básico. Rectas, planos, circunferências e esferas podem ser usados como elementos sobre os quais a geometria se pode basear. Esta concepção deu lugar a novas formas de *dualidade*. Plücker derivou fórmulas que relacionam seis quantidades: primeira e segunda, o grau e a classe<sup>1</sup> de uma curva  $C$ ; terceira e quarta, o número de pontos singulares de  $C$  dos dois tipos mais básicos; quinta, o número de rectas tangentes a  $C$  em dois pontos diferentes; e a última, o número de pontos de inflexão de  $C$ . A dual da primeira quantidade é segunda enquanto que as duais da terceira e quarta são a quinta e sexta, respectivamente. Assim, as seis quantidades dão lugar a três pares de duais.

Um dos sucessos mais notáveis deste período foi a ideia de *transformação geométrica*. Möbius e Plücker consideraram transformações no plano projectivo produzidas por transformações lineares invertíveis de coordenadas homogêneas. Estas vão ser as nossas transformações que irão ser discutidas no capítulo III. Assim, vai se preparando o caminho para Klein e o seu famoso *Programa Erlangen*.

---

<sup>1</sup> Seja  $f(x) = 0$  uma curva no plano projectivo, sem componentes múltiplas, e seja  $q$  um ponto que não pertence a  $f$ . Chamamos *classe* de  $f$  ao número máximo de rectas  $m$  que passam por  $q$  e são tangentes a  $f$  num ponto que não é um ponto singular nem um flexão.

## II. Sinopse Histórica da Geometria Algébrica

A maior parte da geometria algébrica do século XIX era dedicada à *teoria dos invariantes*, combinações algébricas de coordenadas em espaço de  $n$  dimensões que eram preservadas por transformações lineares invertíveis. Descoberta em 1841 por George Boole, a teoria dos invariantes foi desenvolvida na segunda metade do século XIX por Arthur Cayley, James Sylvester, George Salmon e Paul Gordan. Mais tarde, métodos de álgebra abstracta vieram dominar a teoria dos invariantes ao serem introduzidos, no final do século XIX, por David Hilbert e, no princípio do século XX, por Emmy Noether.

Representantes da escola projectiva tais como Chasles, em França, e Steiner e von Staudt, na Alemanha, pensavam que a geometria pura devia estar completamente separada da álgebra e até mesmo do conceito de número real. Obviamente que tal esforço foi infrutífero, dificultando apenas o progresso da álgebra linear na geometria clássica.

Na teoria geral das curvas ( $P_2(\mathbb{C})$ ) e superfícies ( $P_3(\mathbb{C})$ ) algébricas, os principais problemas estudados antes de Riemann são de carácter enumerativo. Chasles, e mais tarde com Schubert e Zeuthen, propuseram fórmulas semi empíricas para resolver estes problemas, baseadas no conceito intuitivo de *multiplicidade de intersecções* que só mais tarde serão justificados.

### §2.4 Geometria de Riemann (1850–1866)

No século XIX, com a adição de pontos no infinito às curvas algébricas complexas, o espaço topológico torna-se *compacto*. Neste espaço topológico faz sentido falar em muitos dos conceitos da teoria da análise complexa tais como de *funções holomorfas* e *meromorfas*, e consequentemente, da teoria das *superfícies de Riemann*, assuntos que irão ser tratados neste período.

Uma das duas maiores contribuições deixadas por Riemann na história da geometria é a introdução do corpo das funções racionais de uma curva<sup>2</sup>. A outra contribuição é o desenvolvimento que este matemático faz do estudo dos *integrals abelianos*<sup>3</sup>. A origem destes integrals deve-se ao estudo dos integrals do tipo

---

<sup>2</sup> A uma curva irreduzível  $f(x, y) = 0$ , está associado um importante conceito conhecido como *corpo das funções racionais da curva*. Este corpo é definido por  $K(\xi, \eta)$ , onde  $K$  é um corpo,  $\xi$  é um elemento transcendente sobre  $K$  e  $\eta$  é um elemento algébrico sobre  $K(\xi)$  satisfazendo a equação irreduzível  $f(\xi, \eta) = 0$ .

<sup>3</sup> Integral Abeliano é um integral da forma  $\int_0^x \frac{dt}{\sqrt{R(t)}}$ , onde  $R(t)$  é um polinómio de grau maior que 4. São também chamados integrals hiperelípticos.

## II. Sinopse Histórica da Geometria Algébrica

$$\int \frac{R(t)}{\sqrt{P(t)}} dt,$$

onde  $P(t)$  é um polinómio e  $R(t)$  é uma função racional. Quando  $P(t)$  tem grau 3 ou 4 este integral tem o nome de *integral elíptico*, quando  $P(t)$  tem grau superior ou igual a 5 estamos na presença de um *integral hiperelíptico*. O nome *elíptico* deveu-se ao facto deste integral expressar o comprimento de um arco de uma elipse. Com efeito, dada a equação da elipse  $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ , o comprimento do arco compreendido entre o ponto de abcissa  $c$  e o ponto de abcissa  $d$  é dado por

$$\frac{1}{a} \int_c^d \frac{a^4 + (b^2 - a^2)x^2}{\sqrt{(a^2 - x^2)(a^4 + (b^2 - a^2)x^2)}} dx.$$

Algumas cúbicas são actualmente chamadas de *curvas elípticas* devido à sua ligação com os integrais elípticos. Esta relação, foi inicialmente apresentada por Gauss, Niels, Abel e Carl Jacobi nos anos vinte do século XIX, sendo, posteriormente, desenvolvida e clarificada por Riemann.

Na primeira metade do século XVIII, Fagnano e Euler procurando uma alternativa para a fórmula clássica que define a soma de dois arcos de uma circunferência, quando a circunferência dá lugar a uma elipse, verificaram que a soma

$$\int_a^x \frac{1}{\sqrt{P(t)}} dt + \int_a^y \frac{1}{\sqrt{P(t)}} dt$$

podia ser escrita como

$$\int_a^z \frac{1}{\sqrt{P(t)}} dt + V(x, y),$$

onde  $z$  é uma função algébrica de  $x$  e  $y$ , e  $V$  uma função racional ou logarítmica de  $x$  e  $y$ .

Abel mostra que as relações de Fagnano-Euler são casos especiais de um teorema mais geral. Ele trabalha exclusivamente no domínio da Análise não estando familiarizado com a geometria projectiva. Esta lacuna fez com que não tivesse presente o conceito de integração no plano complexo. O conceito de integral de primeira espécie e a definição *genus*<sup>4</sup> de uma curva também falharam.

---

<sup>4</sup> *Genus* de uma curva, é uma propriedade topológica invariante de uma curva ou superfície. *Genus* de uma superfície é o número máximo de linhas fechadas simples disjuntas duas a duas sobre a superfície, sem a separar em duas ou mais componentes conexas.

## II. Sinopse Histórica da Geometria Algébrica

Em 1851 surge um trabalho que marcou, de certa forma, todo este panorama em que se vivia, estamos a falar da tese de doutoramento de Riemann sobre a teoria das funções complexas  $u + iv = f(x + iy)$ . Sob a influência de considerações de hidrodinâmica, aplicou o plano  $xy$  conformemente sobre o plano  $uv$  e estabeleceu a existência de uma função capaz de transformar qualquer região simplesmente conexa de um plano, numa outra região simplesmente conexa de outro plano. Esta ideia conduziu à concepção da *superfície de Riemann*<sup>5</sup> que introduziu considerações topológicas na análise. Riemann demonstra a importância central da topologia para a teoria das funções complexas. Esta tese também clarifica a definição de Riemann de uma função complexa — *holomorfa*<sup>6</sup>.

Em 1854 introduz o espaço como uma *variedade topológica* de um número arbitrário de dimensões, na qual é definida uma métrica através de uma forma diferencial quadrática. Estamos a referir-nos ao conceito de *superfície de Riemann*.

Riemann atacou o problema dos integrais abelianos classificando os integrais de todas as *funções meromorfas*<sup>7</sup> da superfície.

A escolha das funções meromorfas leva Riemann à concepção geral de *transformação birracional* entre duas curvas algébricas irredutíveis, correspondendo a uma transformação biholomorfa das suas superfícies de Riemann. Uma transformação birracional é uma transformação  $f : V \rightarrow W$ , onde  $V$  e  $W$  são variedades e onde  $f$  é uma função racional invertível. Com o aparecimento das transformações birracionais foi possível estabelecer uma ligação entre a geometria algébrica e a álgebra abstracta. Ao trabalharmos com as transformações birracionais podemos estudar corpos de funções algébricas. Desta forma, possibilita-nos uma maior liberdade e uma análise mais simples de muitas das propriedades que estas curvas possuem e que são preservadas pelas transformações, tais como o *genus* de uma curva.

---

<sup>5</sup> V. Frances Kirwan, *Complex Algebraic Curves*, London Mathematical Society Student Texts 23, Cambridge 1992 pp111–138.

<sup>6</sup> Seja  $W$  um subconjunto aberto do plano complexo  $\mathbb{C}$ . Uma função holomorfa em  $W$  é uma função diferenciável em todos os pontos de  $W$ , isto é, uma função  $f : W \rightarrow \mathbb{C}$  tal que, para todo  $a \in W$ , existe a derivada  $f'(a) = \lim_{z \rightarrow a} \frac{f(z) - f(a)}{z - a}$  (v. J. Sebastião e Silva, *Análise Superior*, Parte II.2 da obra *Textos Didácticos*, vol. II, Fundação Calouste Gulbenkian, 1999).

<sup>7</sup> Uma função meromorfa é uma função  $f : W \rightarrow \mathbb{C} \cup \{\infty\}$  onde  $W$  é subconjunto aberto no plano complexo e  $f : W \setminus f^{-1}\{\infty\} \rightarrow \mathbb{C}$  é uma função holomorfa que está definida na vizinhança de um ponto  $a$  do seguinte modo  $f(x) = \frac{g(x)}{(x-a)^m}$  para  $m > 0$ , onde  $g$  é holomorfa numa vizinhança de  $a$  e  $g(a) \neq 0$ . (v. Phillip A. Griffiths, *Introduction to Algebraic Curves*, Translation of mathematical Monographs, Volume 76, American Mathematical Society, 1980, pp.11-19)

O contributo de Riemann permitiu o nascimento da topologia algébrica, possibilitando aos seus sucessores a evolução da teoria das curvas e superfícies algébricas.

## §2.5 Desenvolvimento até aos dias de hoje (1866–...)

A extraordinária riqueza de novas ideias e métodos introduzidos por Riemann, deu origem a um desenvolvimento estável da geometria algébrica por cerca de mais de oitenta anos. Durante este período vão-se destacar duas ou três escolas de geometria algébrica, com concepções e métodos diferentes. A primeira tarefa de cada uma é a sistematização da teoria birracional das curvas planas algébricas, incorporando os resultados de Riemann em conformidade com os seus princípios.

Neste primeiro período iniciado por volta de 1882 efectuou-se uma abordagem algébrica, onde se destacam duas correntes, uma defendida por Kronecker e outra por Dedekind e Weber. Tal permitiu o nascimento dos conceitos modernos, em particular a relação entre as *variedades algébricas* e a teoria das *variedades analíticas complexas*. De uma forma resumida definimos variedade algébrica como o conjunto de soluções para um número finito de equações polinomiais com um número finito de variáveis sobre um corpo  $K$ , e uma variedade complexa, *manifold*, é um espaço topológico separado (à Hausdorff) com dimensão complexa  $n$ , que é localmente euclidiana, isto é, localmente isomorfa e biholomorfa a um espaço complexo  $\mathbb{C}^n$ .<sup>8</sup>

Dedekind e Weber observaram a grande proximidade entre a geometria algébrica e a embrionária teoria dos números algébricos. A concepção de geometria algébrica é actualmente simples e clara devido a nossa familiaridade com a álgebra abstracta, mas foi precisamente essa «abstracção» a característica que fez deste tema o menos popular possível e o menos perceptível do seu tempo.

O estudo profundo de Kronecker sobre a teoria das quantidades algébricas teve grande impacto sobre os algebristas e especialistas em teoria dos números. Os seus trabalhos foram seguidos por Lasker e Macaulay, nas primeiras duas décadas do século XX. Consistiam, essencialmente, no uso de um método de eliminação bem mais flexível e poderoso que os anteriores. Com este avanço foi, pela primeira vez, possível dar um significado preciso aos conceitos de *dimensão* e de *variedade irredutível* e mostrar que cada variedade (definida por

---

<sup>8</sup> V. *Encyclopedic Dictionary of Mathematics*, vol. 1, Second edition, MIT Press, 1993, pp. 269–278.

## II. Sinopse Histórica da Geometria Algébrica

um sistema arbitrário de equações algébricas) no espaço projectivo  $n$ -dimensional decompõe-se, de uma única forma, na união de variedades irredutíveis (em geral de diferentes dimensões).

O objectivo de Dedekind e Weber era diferente mas mais limitado que o de Kronecker. Eles tinham métodos puramente algébricos para obter os mesmos resultados algébricos anteriormente obtidos por Riemann que usou a análise complexa e a topologia. Estes dois matemáticos mostram que a maior parte da teoria das curvas algébricas mantém-se válida, quando o corpo dos complexos é substituído por um outro corpo  $K$  (preferencialmente algebricamente fechado). Desta forma, em vez de estudarmos uma curva  $C$  definida por um polinómio irredutível  $P(x, y)$ , estudamos o corpo de funções racionais em  $C$ .

Este tratamento puramente algébrico abriu um novo caminho para a geometria pós-riemanniana.

Em geral, é útil estudar curvas definidas sobre outros corpos, que não o corpo dos reais ou dos complexos. Por exemplo: para quem trabalha em teoria dos números interessa saber as soluções inteiras de uma equação diofantina  $P(x, y) = 0$ , onde  $P(x, y)$  representa um polinómio com coeficientes inteiros. Esta equação pode ser analisada como uma congruência modulo  $p$ , sendo  $p$  um número primo. Por sua vez, tal congruência pode ser pensada como definindo uma curva algébrica sobre o corpo finito  $F_p = \mathbb{Z}/p\mathbb{Z}$ , que consiste nos inteiros modulo  $p$ , ou sobre o seu fecho algébrico.

No final do século XIX os matemáticos começaram a fazer progressos no estudo de soluções de sistemas de mais de uma equação polinomial a mais de duas variáveis. Durante o século XX muitas mais ideias e técnicas foram desenvolvidas nesta área da matemática. Curvas e superfícies algébricas são actualmente bem conhecidas, mas a teoria das variedades de dimensão superior a dois é ainda uma área que permanece com muitas lacunas.

As primeiras décadas do século XX presenciaram uma grande divisão. Por um lado, a tradição geométrica do estudo de curvas e superfícies dirigida pela escola italiana originando um desenvolvimento da topologia e geometria diferencial. Por outro, a força da álgebra comutativa que criava fundamentos e providenciava técnicas de demonstração.

Com o aparecimento da álgebra abstracta, seguida por Hilbert e Emmy Noether, o rigor e os fundamentos da geometria algébrica aumentaram nos anos vinte e trinta, devido a van der Waerden, Zariski e Weil. Um dos interesses centrais era trabalhar a geometria algébrica sobre um corpo arbitrário.

## II. Sinopse Histórica da Geometria Algébrica

Os conceitos fundamentais de geometria abstracta, topologia e espaços vectoriais, foram estabelecidos entre 1920 e 1940, mas os vinte anos que se seguiram viram uma verdadeira evolução nos métodos de topologia algébrica. O resultado foi o aparecimento de uma nova disciplina chamada *álgebra homológica*. A álgebra homológica é um ramo da álgebra abstracta que trata de resultados válidos para muitas espécies diferentes de espaços.

Mais tarde, em 1945, num artigo de Eilenberg & MacLane intitulado “General Theory of natural Equivalences” surgem as noções de *categoria*<sup>9</sup> e *functor*<sup>10</sup>.

**A era Grothendieck.** Entre 1955 a 1970, a geometria algébrica foi dominada pelos matemáticos de Paris, primeiro Serre e depois Grothendieck e a sua escola. Grothendieck iniciou um programa gigante no qual defendia a generalização da geometria algébrica, absorvendo desenvolvimentos anteriores apoiados na teoria das categorias. É importante não subestimar a influência da abordagem de Grothendieck. Graças ao uso sistemático da noção de *scheme* (noção mais geral de variedade), este foi um período onde grandes avanços conceptuais e técnicos foram feitos. A geometria algébrica teve uma participação importante nos avanços observados na topologia, álgebra homológica, teoria de números, etc.

O «culto da personalidade» de Grothendieck teve, no entanto, alguns efeitos negativos. A maioria das pessoas que passaram as suas vidas a ensinar os fundamentos de Weil sofreram rejeição e humilhação. Foram poucos os que se adaptaram a esta nova linguagem.

Muitos dos matemáticos franceses desse tempo sofreram terrorismo intelectual. À parte de um pequeno número dos estudantes de Grothendieck, que foram capazes de passar por todo este ambiente e sobreviver, as pessoas que mais benefícios tiraram das ideias deste homem, foram as que as propagaram, mas à distância, na escola de Harvard, na escola de Moscovo e eventualmente na escola Japonesa de algebristas comutativos.

---

<sup>9</sup> Uma Categoria  $C$  pode ser descrita como uma colecção  $Ob$ , de *objectos* de  $C$ , que satisfazem as seguintes condições: • Para cada par  $a, b$  de objectos, existe uma colecção  $Mor(a, b)$ , chamada de morfismos de  $a$  para  $b$  em  $C$  (quando  $f$  é um morfismo de  $a$  para  $b$  escrevemos  $f: a \rightarrow b$ );

• Para todo triplo  $a, b$  e  $c$  de objectos, existe uma operação entre pares de morfismos em  $Mor(a, b) \times Mor(b, c)$  para morfismos em  $Mor(a, c)$ , chamada composição de morfismos em  $C$  (quando  $f: a \rightarrow b$  e  $g: b \rightarrow c$ , então  $(g \circ f): a \rightarrow c$ )

• Para cada objecto  $a$ , existe um morfismo  $id_a$  em  $Mor(a, a)$ , chamado identidade em  $a$ .

Os morfismos têm ainda que satisfazer dois axiomas:

Se  $f: a \rightarrow b, g: b \rightarrow c$  e  $h: c \rightarrow d$ , então  $h \circ (g \circ f) = (h \circ g) \circ f$  – Associatividade

Se  $f: a \rightarrow b$ , então  $id \circ f = f$  e  $f \circ id = f$  – Identidade. (v.Orlando Neto *Equações diferenciais em Superfícies de Riemann*, Universidade de Lisboa, Faculdade de Ciências, 1994, pp.5-9).

<sup>10</sup> Um functor é uma função definida entre categorias que transforma objectos em objectos e morfismos em morfismos.

## II. Sinopse Histórica da Geometria Algébrica

Durante os anos setenta algumas escolas tinham os seus interesses particulares. A escola de Mumford, com a compactificação de espaços modulares, Griffith com a teoria de Hodge e de curvas algébricas, Delic e a cohomologia de variedades, Shafarevich e as superfícies  $K3$ , Iitaka e a classificação de variedades de grande dimensão, etc. Parece que todas estavam a estudar o mesmo objecto, a geometria algébrica, sendo esta vista como um bloco monolítico.

Por volta dos anos oitenta todo este ambiente sofre alterações. A geometria algébrica parece então separar-se em cerca de doze ou mais escolas sem grandes interações, das quais destacamos: curvas e variedades abelianas, superfícies algébricas e teoria de Donaldson, K-teoria e ciclos algébricos, teoria da interação e geometria enumerativa, teoria de Hodge, geometria algébrica aritmética, aplicações à álgebra computacional etc.

Como se sabe, o estudo das curvas algébricas complexas está intimamente relacionado com muitas áreas da matemática. No entanto, gostaríamos de apresentar de uma forma resumida, no final deste percurso histórico, uma importante relação existente entre as curvas algébricas complexas e a teoria dos números. Trata-se de um tema que muita polémica levantou — o *último teorema de Fermat*.

Desde os tempos de Diofanto de Alexandria que os estudiosos da teoria dos números estiveram interessados nas soluções inteiras de equações polinomiais (Análise Diofantina) e, em particular, em equações do tipo  $x^n + y^n = z^n$ .

Uma pergunta que se colocava era saber se existiam soluções inteiras para além da nula quando  $n > 2$ . Esta questão leva-nos a uma outra análoga, que consiste em saber se existem soluções racionais diferentes de zero  $s = \frac{x}{z}$  e  $t = \frac{y}{z}$  para a equação

$$s^n + t^n = 1.$$

Esta última equação define uma curva algébrica fechada a que Fermat chamou curva de grau  $n$ . Este matemático francês disse ter provado que tal equação não tinha soluções não triviais quando  $n > 2$ . O que é certo é que nunca ninguém viu tal demonstração e só cerca de trezentos e cinquenta anos depois, em 1995, foi apresentada por Andrew Wiles.

Em 1983, Gerd Faltings, um matemático alemão provou que esta curva algébrica complexa de genus  $n > 2$  tem apenas um número finito de pontos com coeficientes racionais (*conjectura de Mordell*). A curva de Fermat de grau  $n$  tem genus  $\frac{1}{2}(n-1)(n-2)$ , e, quando  $n > 4$ , existe um teorema que nos permite concluir a existência de apenas um número finito de soluções racionais para tal equação. Se esse número finito era, alguma vez, diferente de zero foi uma questão que ficou em aberto. Posteriormente, dois matemáticos, Granville e

## II. Sinopse Histórica da Geometria Algébrica

Heath-Brown, usaram o resultado de Faltings para mostrarem que o número de soluções da equação de Fermat, se existissem, desceria à medida que o expoente  $n$  aumentasse.

Mais alguns avanços foram necessários para que finalmente fosse possível chegar à demonstração deste tão “misterioso” teorema. Talvez um dos maiores avanços tenha sido a *conjectura de Shimura-Taniyama*. Esta conjectura consistia no seguinte: todas as curvas elípticas<sup>11</sup> são modulares. Em 1995, Andrew Wiles prova esta conjectura, permitindo-lhe consequentemente chegar à demonstração do último teorema de Fermat.

Muitos contributos foram necessários para se chegar à solução final: De forma resumida podemos afirmar que sem o trabalho de Ernst Kummer não havia a teoria dos ideais e sem os ideais o trabalho de Barry Mazur não teria existido. Por sua vez sem Mazur não teria surgido a conjectura de Frey e sem a sua sintetização feita por Serre não haveria a demonstração de Ribert, segundo a qual a conjectura de Shimura-Taniyama<sup>12</sup> iria estabelecer o último teorema de Fermat. Parece portanto que nenhuma demonstração do último teorema de Fermat seria possível sem a conjectura apresentada por Yutaka Taniyama em Tóquio-Nikko em 1955 e depois aperfeiçoada e precisada por Goro Shimura.

Obviamente que Fermat não poderia ter feito tal demonstração, até porque a maior parte dos resultados necessários para a mesma só foram apresentados depois da sua morte. No entanto, talvez Fermat tivesse pensado numa outra demonstração para este teorema. Este será um mistério que permanecerá para sempre.

---

<sup>11</sup>Uma curva elíptica é uma cúbica não singular da forma  $y^2 = x^3 + ax^2 + bx + c$ , onde  $a, b$  e  $c$  representam números racionais.

<sup>12</sup> V. Amir D. Aczel, *O Último Teorema de Fermat*, Gradiva, 1996.

## Capítulo III | INTERSECÇÕES

Uma curva algébrica pode ser definida, como já referimos, por uma equação polinomial a duas variáveis  $f(x, y) = 0$  no plano euclidiano. O termo “curva algébrica” vai ser abreviado para “curva”, visto que, no presente trabalho, apenas consideramos curvas que são algébricas. Referimo-nos indistintamente à curva  $f(x, y) = 0$ , ou à curva  $f(x, y)$ , ou ainda à curva  $f$ .

Uma forma de estudar uma curva é através da análise da sua intersecção com outras curvas em pontos particulares. Daí a grande importância do estudo da intersecção das curvas.

Inicialmente, vamos apresentar de forma intuitiva, o conceito de intersecção de duas curvas na origem. Segue-se um conjunto de propriedades a que chamamos *propriedades de intersecção* e, por fim, alguns teoremas que delas se deduzem. Posteriormente, alargamos o conceito de intersecção de duas curvas a outros pontos que não a origem. Na secção 3.3, depois de definirmos formalmente a intersecção entre duas curvas num ponto através da independência de polinómios, vamos poder demonstrar todas as propriedades apresentadas nas secções 3.1 e 3.2. Necessitamos, porém, de apresentar um outro conceito, o de geradores de intersecções.

### §3.1 Intersecção entre duas curvas na origem

Começemos com a ideia de que uma curva pode intersectar-se mais do que uma vez num determinado ponto. Esta ideia está presente quando pensamos na curva representada na Fig.15. Neste caso, parece-nos intuitivo que a curva passa pela origem duas vezes.

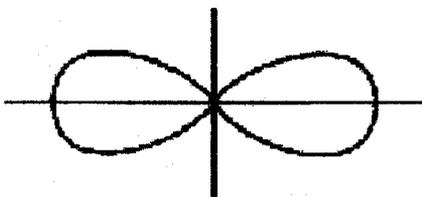


Fig. 15

### III. Intersecções

Também se tivermos duas circunferências secantes em dois pontos  $P$  e  $Q$  e se as afastarmos de forma a que apenas fiquem tangentes, então os dois pontos parecem colapsar num único ponto, como se pode ver na Fig. 16. De acordo com este raciocínio, parece natural pensarmos que as duas circunferências se intersectam duas vezes nesse ponto de tangência.

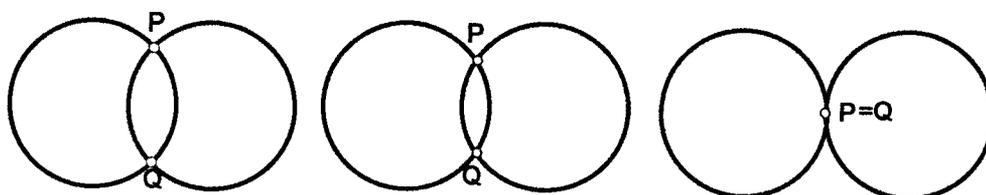


Fig. 16

Consideremos ainda outro exemplo em que temos a curva definida pela equação  $y = x^3$  e uma recta de declive positivo que passa pela origem. Esta recta vai intersectar a curva em três pontos, como se observa na Fig. 17. Com a rotação desta recta em torno da origem, podemos verificar que dois destes três pontos vão se aproximando-se cada vez mais da origem, coincidindo com esta quando a recta se sobrepõe ao eixo das abcissas. Concluimos assim que a curva  $y = x^3$  intersecta a origem três vezes.

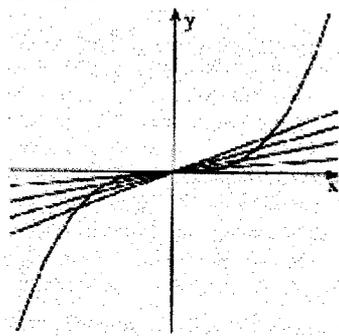


Fig. 17

Depois de dados estes exemplos, e seguindo este tipo de raciocínio, chegámos ao momento de introduzir o conceito de intersecção entre duas curvas na origem.

A intersecção entre duas curvas  $f$  e  $g$  na origem, que designaremos por  $I_0(f, g)$ , representa a multiplicidade de intersecção das curvas  $f$  e  $g$  na origem, que designaremos por  $O$ . Quando nos referimos a este valor pensamos no número de vezes que as curvas  $f(x, y) = 0$  e  $g(x, y) = 0$  se intersectam na origem. Vejamos algumas propriedades deste valor.

#### **Propriedade 3.1**

$I_0(f, g)$  é um número inteiro não negativo ou  $\infty$ .

### III. Intersecções

**Observação:**

Mais adiante (teorema 3.6) iremos verificar que a intersecção entre duas curvas é  $\infty$  quando uma das curvas é múltipla da outra e ambas contêm a origem.

#### **Propriedade 3.2**

$$I_O(f, g) = I_O(g, f).$$

O valor de  $I_O(f, g)$  não depende da ordem de  $f$  e  $g$ .

#### **Propriedade 3.3**

$I_O(f, g)$  é maior ou igual a 1 se ambas as curvas  $f$  e  $g$  contiverem a origem.

#### **Observação**

Consideremos  $x$  e  $y$ , os eixos das abcissas e ordenadas, respectivamente. Como estes eixos se intersectam na origem apenas uma vez, então  $I_O(x, y) = 1$ . Apesar desta afirmação ser intuitiva, necessita de uma demonstração, que irá ser apresentada na secção 3.3.

#### **Propriedade 3.4**

Sejam  $f$ ,  $g$  e  $h$  três polinómios com duas variáveis. Então  $I_O(f, g) = I_O(f, g + fh)$ .

Esta propriedade é verificada porque as equações  $f(a, b) = 0$  e  $g(a, b) = 0$  são equivalentes às equações  $f(a, b) = 0$  e  $g(a, b) + f(a, b)h(a, b) = 0$ , logo  $f$  e  $g$  intersectam-se em  $(a, b)$  se e só se  $f$  e  $g + fh$  também se intersectarem nesse ponto. Se generalizarmos este resultado para intersecções múltiplas na origem então temos que as equações  $f(a, b) = 0$  e  $g(a, b) = 0$ , ou  $f(a, b) = 0$  e  $h(a, b) = 0$  são equivalentes às equações  $f(a, b) = 0$  e  $g(a, b)h(a, b) = 0$ . As intersecções na origem de  $f$  e  $gh$  são as de  $f$  e  $g$ , e as de  $f$  e  $h$ .

#### **Propriedade 3.5**

$$I_O(f, gh) = I_O(f, g) + I_O(f, h).$$

Mediante estas cinco propriedades podemos determinar, de uma forma simples, intersecções entre duas curvas na origem, que à priori seriam um pouco difíceis de determinar. Vejamos um exemplo. Queremos determinar  $I_O(f, g)$ , em que as curvas  $f$  e  $g$  são definidas do seguinte

### III. Intersecções

modo:  $f(x, y) = x^2$  e  $g(x, y) = y^3$ . Assim,

$$\begin{aligned}
 I_O(f, g) &= I_O(x^2, y^3) \\
 &= I_O(x^2, y) + I_O(x^2, y) + I_O(x^2, y) && \text{(prop. 3.5)} \\
 &= 3I_O(x^2, y) \\
 &= 3I_O(y, x^2) && \text{(prop. 3.2)} \\
 &= 3(I_O(y, x) + I_O(y, x)) && \text{(prop. 3.5)} \\
 &= 3 \cdot 2I_O(y, x) \\
 &= 3 \cdot 2 && \text{(prop. 3.2 e obs. precedente à prop. 3.4)} \\
 &= 6.
 \end{aligned}$$

Vamos agora deduzir alguns teoremas fundamentais para o estudo presente.

#### Teorema 3.6

Se  $f$  e  $g$  são polinómios tais que  $f$  é factor de  $g$  e a curva  $f(x, y) = 0$  contém a origem, então  $I_O(f, g) = \infty$ .

#### Demonstração

Vamos considerar dois casos:

1º Caso —  $g(x, y) = 0$ .

Pela propriedade 3.3 sabemos que  $I_O(f, g) \geq 1$ .

Para  $n$  inteiro positivo temos  $n \cdot I_O(f, g) \geq n$ . Pela propriedade 3.5 temos

$$n \cdot I_O(f, g) = I_O(f, g^n) = I_O(f, g) \quad (\text{pois } g^n = 0^n = 0).$$

Logo  $\forall n \in \mathbb{N}^+ I_O(f, g) \geq n$ , portanto  $I_O(f, g) = \infty$ .

2º Caso —  $g(x, y) \neq 0$ .

Como  $f$  é factor de  $g$ , tem-se  $g = f \cdot h$  para algum polinómio  $h$ . Assim, temos

$$\begin{aligned}
 I_O(f, g) &= I_O(f, fh) \\
 &= I_O(f, fh - fh) && \text{(prop. 3.4)} \\
 &= I_O(f, 0) \\
 &= \infty && \text{(1.º caso) } \square
 \end{aligned}$$

#### Teorema 3.7

Se  $f$ ,  $g$  e  $h$  são curvas tais que  $g$  não contém a origem, então  $I_O(f, gh) = I_O(f, h)$ .

### III. Intersecções

#### Demonstração

Pela propriedade 3.5 temos que  $I_O(f, gh) = I_O(f, g) + I_O(f, h)$ . Como  $g$  não contém a origem, temos  $I_O(f, g) = 0$ , donde se obtém a igualdade pretendida.  $\square$

Para mostrarmos a aplicabilidade deste teorema, vamos considerar o seguinte exemplo: Queremos determinar o número de vezes que as curvas  $f(x, y) = y - x^2$  e  $g(x, y) = y^3 + x^2y + 2x^2 + x$  se intersectam na origem, ou seja o valor de  $I_O(f, g)$ .

Efectuando o algoritmo da divisão<sup>13</sup> obtemos:

$$y^3 + x^2y + 2x^2 + x = (y - x^2)(y^2 + x^2y + x^4 + x^2) + (x^6 + x^4 + 2x^2 + x),$$

donde concluímos, pela propriedade 3.4,

$$\begin{aligned} I_O(y - x^2, y^3 + x^2y + 2x^2 + x) &= I_O(y - x^2, x^6 + x^4 + 2x^2 + x) \\ &= I_O(y - x^2, (x^5 + x^3 + 2x + 1)x). \end{aligned}$$

Como  $x^5 + x^3 + 2x + 1 = 0$  não contém a origem, então pelo teorema 3.7 e recorrendo novamente à propriedade 3.4 obtemos:

$$I_O(y - x^2, y^3 + x^2y + 2x^2 + x) = I_O(y - x^2, x) = I_O(y, x)$$

Pela propriedade 3.2 e observação que precede a propriedade 3.3 concluímos finalmente

$$I_O(y - x^2, y^3 + x^2y + 2x^2 + x) = 1.$$

O teorema que se segue dá-nos um resultado relativo à divisibilidade entre polinómios.

<sup>13</sup>

$$\begin{array}{r} y^3 \qquad \qquad \qquad + x^2y \qquad \qquad \qquad 2x^2 + x \\ - y^3 \quad + x^2y^2 \\ \hline \qquad \qquad \qquad + x^2y^2 \\ \qquad \qquad \qquad - x^2y^2 \qquad \qquad \qquad + x^4y \\ \hline \qquad \qquad \qquad \qquad \qquad \qquad (x^2 + x^4)y \\ \qquad \qquad \qquad - (x^2 + x^4)y \quad x^6 + x^4 \\ \hline \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad x^6 + x^4 + 2x^2 + x \end{array} \qquad \left| \begin{array}{l} y - x^2 \\ \hline y^2 + x^2y + x^4 + x^2 \end{array} \right.$$

### III. Intersecções

#### **Teorema 3.8**

Sejam  $p(x)$  e  $g(x, y)$  polinómios.

(i) Se dividirmos  $g(x, y)$  por  $y - p(x)$ , obtemos como resto o polinómio  $g(x, p(x))$ , quer dizer, existe um polinómio  $h(x, y)$  tal que

$$g(x, y) = (y - p(x))h(x, y) + g(x, p(x)); \quad (1)$$

(ii) Em particular,  $y - p(x)$  é factor de  $g(x, y)$  se e só se  $g(x, p(x))$  é o polinómio zero.

#### **Demonstração**

(i) Seja  $h(x, y)$  o quociente e  $r(x, y)$  o resto resultante da divisão de  $g(x, y)$  por  $y - p(x)$ , ou seja:

$$g(x, y) = (y - p(x)) h(x, y) + r(x, y). \quad (2)$$

Ao substituírmos  $p(x)$  por  $y$  em  $g(x, y)$  obtemos  $y - p(x) = p(x) - p(x) = 0$ , e de (2) resulta  $g(x, p(x)) = r(x, p(x))$ , onde não ocorre  $y$ . Desta última igualdade e de (2) temos (1).

(ii) Se  $y - p(x)$  é um factor de  $g(x, y)$ , então existe um polinómio  $k(x, y)$  tal que  $g(x, y) = (y - p(x))k(x, y)$  e, portanto,  $g(x, p(x))$  é o polinómio zero.

Reciprocamente, se  $g(x, p(x))$  é o polinómio zero, por (1) concluímos que  $y - p(x)$  é um factor de  $g(x, y)$  e podemos escrever  $g(x, y) = (y - p(x))k(x, y)$  para um determinado polinómio  $k(x, y)$ .  $\square$

Como caso particular do teorema 3.8, temos o teorema seguinte, em que  $g$  é função apenas de  $y$  e em que  $p(x) = b$ , sendo  $b$  um número real.

#### **Teorema 3.9**

Seja  $g(y)$  um polinómio em  $y$ , e seja  $b$  um número real.

(i) Com a divisão de  $g(y)$  por  $y - b$  obtemos o resto  $g(b)$ , logo existe um polinómio  $h(y)$  tal que  $g(y) = (y - b)h(y) + g(b)$ .

(ii) Em particular,  $y - b$  é um factor de  $g(y)$  se e só se  $g(b) = 0$ .

Chegámos ao momento de determinar a multiplicidade de intersecção na origem entre duas curvas, em que uma é do tipo  $y = p(x)$ . Esta multiplicidade vai ser dada pelo resultado que se segue.

### III. Intersecções

#### **Teorema 3.10**

Sejam  $g(x, y) = 0$  e  $y = p(x)$  duas curvas tais que  $y = p(x)$  contém a origem e não é factor de  $g(x, y) = 0$ . O número de vezes que  $y = p(x)$  e  $g(x, y) = 0$  se intersectam na origem é o menor grau de todos os termos diferentes de zero de  $g(x, p(x))$ .

#### **Demonstração**

Por hipótese  $y - p(x)$  não é factor de  $g(x, y) = 0$  logo, pelo teorema 3.8 (ii),  $g(x, p(x))$  é diferente de zero. Seja  $s$  o menor grau de todos os termos diferentes de zero de  $g(x, p(x))$ . Queremos mostrar que  $I_O(y - p(x), g(x, y)) = s$ .

Como  $x^s$  é comum a todos os termos, podemos escrever

$$g(x, p(x)) = x^s q(x).$$

Note-se que o termo independente do polinómio  $q(x)$  é diferente de zero e, portanto,  $q(x) = 0$  não contém a origem. Assim, de (1) obtemos

$$g(x, y) = (y - p(x))h(x, y) + x^s q(x).$$

Logo,

$$\begin{aligned} I_O(y - p(x), g(x, y)) &= I_O(y - p(x), (y - p(x))h(x, y) + x^s q(x)) \\ &= I_O(y - p(x), x^s q(x)) \quad (\text{prop. 3.4}) \end{aligned}$$

Como  $q(x) = 0$  não contém a origem e aplicando o teorema 3.7 obtemos

$$\begin{aligned} I_O(y - p(x), g(x, y)) &= I_O(y - p(x), x^s) \\ &= s I_O(y - p(x), x) \quad (\text{prop. 3.5}) \end{aligned}$$

Como, por hipótese,  $y = p(x)$  contém a origem, então  $p(0) = 0$  e, portanto, o termo independente de  $p(x)$  é zero. Desta forma, podemos escrever  $p(x) = xt(x)$  para algum polinómio  $t$ , e assim

$$\begin{aligned} I_O(y - p(x), g(x, y)) &= s I_O(y - xt(x), x) \\ &= s I_O(x, y) \quad (\text{prop. 3.2 e 3.4}) \\ &= s \quad (\text{obs. que precede a prop. 3.4}). \end{aligned}$$

Concluimos então que  $I_O(y - p(x), g(x, y)) = s$ .  $\square$

Neste momento e recorrendo ao teorema 3.10, podemos, de forma simples, determinar o número de vezes que duas curvas se intersectam na origem quando, na equação de uma delas, é possível expressar  $y$  como um polinómio em  $x$ . Podemos, assim, voltar a estudar o exemplo

### III. Intersecções

anteriormente trabalhado em que tínhamos as curvas  $f(x, y) = y - x^2$  e  $g(x, y) = y^3 + x^2y + 2x^2 + x$ , e determinar  $I_O(f, g)$ , agora recorrendo a este teorema.

Considerando  $y = p(x) = x^2$ , temos  $g(x, p(x)) = (x^2)^3 + x^2x^2 + 2x^2 + x$ .

Como  $g(x, p(x))$  é diferente de zero, pelo teorema 3.8 (ii),  $y - x^2$  não é factor de  $y^3 + x^2y + 2x^2 + x$ . Também sabemos que  $y = x^2$  contém a origem, logo podemos aplicar o teorema 3.10 e concluir que o número de vezes que  $y = x^2$  e  $g(x, y) = y^3 + x^2y + 2x^2 + x$  se intersectam na origem é definido pelo menor grau de todos os termos diferentes de zero do polinómio  $g(x, p(x))$ , ou seja 1.

Tomemos agora para  $p(x)$  um polinómio diferente de zero sem termo constante. Porque  $p(x)$  é diferente de zero,  $y - p(x)$  não é factor de  $y$ . Aplicando o teorema 3.10 e considerando  $g(x, y)$  o polinómio  $y - p(x)$ , concluímos que o número de intersecções na origem que  $y = p(x)$  faz com o eixo das abcissas  $y = 0$  corresponde ao menor grau da potência de  $x$  de  $p(x)$ . Com este resultado podemos, de forma muito rápida, determinar o número de intersecções na origem que algumas curvas fazem com o eixo das abcissas. Consideremos a título de exemplo a curva  $y = 2x^7 - 2x^6 + 4x^2$ . Como o menor grau da potência de  $x$  é dois, este é também o número de intersecções pretendido.

Com o teorema 3.10 podemos determinar o número de vezes que duas curvas se intersectam na origem quando uma das curvas é susceptível de ser escrita na forma  $y = f(x)$ . No entanto, com um pouco mais de trabalho, podemos generalizar este resultado para duas curvas quaisquer. O processo de determinação deste número consiste na eliminação da maior potência de  $y$  que aparece nas duas equações. Para tal, recorreremos às propriedades 3.1–3.5 e aos teoremas 3.6–3.7. Esta eliminação é feita várias vezes de modo a fazer desaparecer por completo com o “ $y$ ” de uma das duas equações. Obviamente que todo este processo pode ser realizado de modo a eliminar as potências de  $x$  e não as de  $y$ . Depois de estabelecida esta técnica, estamos aptos a determinar a multiplicidade de intersecções existentes nessas duas curvas na origem.

Para melhor compreendermos este procedimento vejamos o seguinte exemplo.

Sejam  $f(x, y) = y^3 - 2x^4$  e  $g(x, y) = xy^2 + 2y - x^2$  duas curvas. Queremos determinar  $I_O(y^3 - 2x^4, xy^2 + 2y - x^2)$ .

Pela propriedade 3.5 temos

$$I_O(x, xy^2 + 2y - x^2) + I_O(y^3 - 2x^4, xy^2 + 2y - x^2) = I_O(x(y^3 - 2x^4), xy^2 + 2y - x^2),$$

### III. Intersecções

ou seja,

$$I_O(y^3 - 2x^4, xy^2 + 2y - x^2) = I_O(xy^3 - 2x^5, xy^2 + 2y - x^2) - I_O(x, xy^2 + 2y - x^2).$$

Ora,

$$\begin{aligned} I_O(f, g) &= I_O(xy^3 - 2x^5, xy^2 + 2y - x^2) - I_O(x, x(y^2 - x) + 2y) \\ &= I_O(xy^3 - 2x^5, xy^2 + 2y - x^2) - I_O(x, 2y) && \text{(prop. 3.4)} \\ &= I_O(xy^3 - 2x^5, xy^2 + 2y - x^2) - I_O(x, y) && \text{(teorema 3.7)} \\ &= I_O(xy^3 - 2x^5, xy^2 + 2y - x^2) - 1 \quad \text{(obs. que precede a prop. 3.4).} \end{aligned}$$

Vejamos agora a quantidade  $I_O(xy^3 - 2x^5, xy^2 + 2y - x^2)$ .

A potência mais alta de  $y$  existente nas duas curvas é  $y^3$ . Desta forma, e com a finalidade de eliminar o termo  $xy^3$ , vamos recorrer à propriedade 3.4 e multiplicar a segunda equação por  $-y$  para posteriormente somar à primeira:

$$\begin{aligned} I_O(f, g) &= I_O(xy^3 - 2x^5 - y(xy^2 + 2y - x^2), xy^2 + 2y - x^2) - 1 \\ &= I_O(-2y^2 - x^2y - 2x^5, xy^2 + 2y - x^2) - 1. \end{aligned}$$

Procedendo à técnica de eliminação anterior, vamos agora eliminar o termo de  $y^2$  da segunda equação. A forma mais simples de o fazer é através da propriedade 3.4, onde multiplicamos a primeira equação por  $-\frac{1}{2}x$  e somamos à segunda:

$$\begin{aligned} I_O(f, g) &= I_O(-2y^2 - x^2y - 2x^5, xy^2 + 2y - x^2 - \frac{1}{2}x(-2y^2 - x^2y - 2x^5)) - 1 \\ &= I_O(-2y^2 - x^2y - 2x^5, (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1. \end{aligned}$$

Vamos aplicar o teorema 3.7 e multiplicar a primeira equação por  $1 + \frac{1}{4}x^3$ . Note-se que a curva  $1 + \frac{1}{4}x^3 = 0$  não contém a origem:

$$\begin{aligned} I_O(f, g) &= I_O((1 + \frac{1}{4}x^3)(-2y^2 - x^2y - 2x^5), (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1 \\ &= I_O(-(2 + \frac{1}{2}x^3)y^2 + (-x^2 - \frac{1}{4}x^5)y - 2x^5 - \frac{1}{2}x^8, (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1. \end{aligned}$$

Voltando a recorrer à técnica de eliminação anterior e somando à primeira equação o produto de  $y$  pela segunda equação obtemos, depois de feitas as devidas simplificações, a seguinte expressão:

$$\begin{aligned} I_O(f, g) &= I_O((-2x^2 - \frac{1}{4}x^5 + x^6)y - 2x^5 - \frac{1}{2}x^8, (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1 \\ &= I_O(x^2((-2 - \frac{1}{4}x^3 + x^4)y - 2x^3 - \frac{1}{2}x^6), (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1 \end{aligned}$$

### III. Intersecções

$$\begin{aligned}
 I_0(f, g) &= I_0(x^2, (2 + \frac{1}{2}x^3)y + x^6 - x^2) + \\
 &\quad I_0((-2 - \frac{1}{4}x^3 + x^4)y - 2x^3 - \frac{1}{2}x^6, (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1 \quad (\text{prop. 3.5}) \\
 &= I_0(x^2, (2 + \frac{1}{2}x^3)y + (x^4 - 1)x^2) + \\
 &\quad I_0((-2 - \frac{1}{4}x^3 + x^4)y - 2x^3 - \frac{1}{2}x^6, (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1 \\
 &= I_0(x^2, (2 + \frac{1}{2}x^3)y) + \\
 &\quad I_0((-2 - \frac{1}{4}x^3 + x^4)y - 2x^3 - \frac{1}{2}x^6, (2 + \frac{1}{2}x^3)y + x^6 - x^2) - 1 \quad (\text{prop. 3.4}).(3)
 \end{aligned}$$

Efectuando os cálculos em separado de cada uma das duas intersecções que estão envolvidas no cálculo da intersecção  $I_0(f, g)$  obtemos:

$$\begin{aligned}
 I_0(x^2, (2 + \frac{1}{2}x^3)y) &= I_0(x^2, 2 + \frac{1}{2}x^3) + I_0(x^2, y) \\
 &= 0 + 2I_0(x, y) \quad (\text{a curva } 2 + \frac{1}{2}x^3 = 0 \text{ não contém a origem e prop. 3.5}) \\
 &= 2. \quad (\text{obs. que precede a prop. 3.4}).
 \end{aligned}$$

Na segunda intersecção  $I_0((-2 - \frac{1}{4}x^3 + x^4)y - 2x^3 - \frac{1}{2}x^6, (2 + \frac{1}{2}x^3)y + x^6 - x^2)$  vamos aplicar a propriedade 3.4 somando a segunda equação à primeira de forma a obtermos

$$I_0((-2 - \frac{1}{4}x^3 + x^4)y - 2x^3 - \frac{1}{2}x^6 + (2 + \frac{1}{2}x^3)y + x^6 - x^2, (2 + \frac{1}{2}x^3)y + x^6 - x^2).$$

Depois de simplificada a expressão anterior, obtemos

$$I_0((\frac{1}{4}x^3 + x^4)y - 3x^3 + \frac{1}{2}x^6, (2 + \frac{1}{2}x^3)y + x^6 - x^2).$$

Ora,

$$\begin{aligned}
 I_0((\frac{1}{4}x^3 + x^4)y - 3x^3 + \frac{1}{2}x^6, (2 + \frac{1}{2}x^3)y + x^6 - x^2) &= \\
 &= I_0(x^3((\frac{1}{4} + x)y - 3 + \frac{1}{2}x^3), (2 + \frac{1}{2}x^3)y + x^6 - x^2) \\
 &= I_0(x^3, (2 + \frac{1}{2}x^3)y + x^6 - x^2) \quad [\text{teorema 3.7, a curva} \\
 &\quad (\frac{1}{4} + x)y - 3 + \frac{1}{2}x^3 = 0 \text{ não contém a origem}] \\
 &= 3I_0(x, (2 + \frac{1}{2}x^3)y + x^6 - x^2) \quad (\text{prop. 3.5})
 \end{aligned}$$

### III. Intersecções

$$\begin{aligned}
 &= 3I_O(x, (2 + \frac{1}{2}x^3)y + (x^5 - x)x) \\
 &= 3I_O(x, (2 + \frac{1}{2}x^3)y) \quad (\text{prop. 3.4}) \\
 &= 3I_O(x, y) \quad (\text{teorema 3.7, a curva } 2 + \frac{1}{2}x^3 = 0 \text{ não contém a origem}) \\
 &= 3
 \end{aligned}$$

Retomando a igualdade em (3) e já efectuadas as operações aí definidas obtemos  $I_O(f, g) = 2 + 3 - 1$ , logo  $I_O(y^3 - 2x^4, xy^2 + 2y - x^2) = 4$ .

## §3.2 Intersecção em coordenadas homogéneas

Em coordenadas homogéneas uma curva algébrica, ou simplesmente uma curva, é uma equação do tipo  $F(x, y, z) = 0$ , em que  $F(x, y, z)$  representa um polinómio homogéneo. Começamos por estender as curvas algébricas do plano euclidiano ao plano projectivo. Todavia, é necessário termos cuidado pois uma equação polinomial  $F(x, y, z) = 0$  a três variáveis não define necessariamente uma curva no plano projectivo. De facto  $F$  tem que verificar a seguinte propriedade:

$$F(a, b, c) = 0 \text{ se e só se } F(ta, tb, tc) = 0, \text{ para } t \neq 0 \text{ e } (a, b, c) \neq (0, 0, 0).$$

Um polinómio homogéneo  $F(x, y, z)$ , que iremos representar por uma letra maiúscula, de grau  $d$  e variáveis  $x, y, z$  é uma expressão do tipo:

$$F(x, y, z) = \sum e_{ij} x^i y^j z^{d-i-j}, \quad (3)$$

onde os  $e_{ij} \in \mathbb{R}$  não são todos iguais a zero e  $i, j \in \mathbb{Z}_0^+$  com  $i + j + (d - i - j) = d$ . Da igualdade anterior, ao substituírmos  $(x, y, z)$  por  $(tx, ty, tz)$ , obtemos

$$\begin{aligned}
 F(tx, ty, tz) &= \sum e_{ij} (tx)^i (ty)^j (tz)^{d-i-j} \\
 &= t^d \sum e_{ij} x^i y^j z^{d-i-j} \\
 &= t^d F(x, y, z),
 \end{aligned}$$

donde se conclui que  $F(ta, tb, tc) = 0 \iff F(a, b, c) = 0$  para todo o  $t \neq 0$  e todo o ponto  $(a, b, c)$ .

Por analogia à definição anterior, um polinómio homogéneo de grau  $d$  sobre o corpo dos complexos é um polinómio  $F(x, y, z)$ , que tem uma equação do tipo (3), onde os coeficientes são números complexos não todos iguais a zero.

### III. Intersecções

Um ponto  $(x, y)$  do plano euclidiano pertence ao gráfico  $f(x, y) = 0$  se e só se o ponto correspondente  $(x, y, 1)$  do plano projectivo pertencer ao gráfico  $F(x, y, z) = 0$ . Assim, ambos os gráficos representam curvas que contêm o mesmo ponto do plano euclidiano. Chamamos  $f$  à *restrição de  $F$  ao plano euclidiano*. Reciprocamente, se  $f(x, y)$  é um polinómio diferente de zero de grau  $d$  de duas variáveis, podemos estender a curva  $f(x, y) = 0$  do plano euclidiano para o plano projectivo através da homogeneização  $F(x, y, z)$  de  $f$ . Esta homogeneização é obtida multiplicando cada termo de  $f$  pela potência de  $z$  necessária para que o termo fique com grau  $d$ . Desta forma, se  $f(x, y) = \sum e_{ij} x^i y^j$ , temos

$$F(x, y, z) = \sum e_{ij} x^i y^j z^{d-i-j},$$

de modo que  $F$  é o polinómio homogéneo do mesmo grau ( $d$ ) que  $f$ . Quando  $z = 1$  temos  $f(x, y) = F(x, y, 1)$ . Neste caso dizemos que  $F$  é *uma extensão de  $f$  ao plano projectivo*. Obtemos o gráfico de  $F$  a partir do gráfico de  $f$  adicionando pontos no infinito.

Para exemplificar esta ideia consideremos a hipérbole  $xy = 1$  do plano euclidiano. O polinómio  $xy - 1$  tem, como sabemos, grau 2. Para se obter a homogeneização deste polinómio, multiplicamos cada termo pela potência de  $z$  necessária de forma a manter o grau 2 em todos os termos. Assim, obtemos a curva  $xy = z^2$ . Esta não é mais do que a extensão da curva  $xy = 1$  ao plano projectivo. Os pontos  $(x, y, 1)$  de  $xy = z^2$  são exactamente os pontos  $(x, y)$  de  $xy = 1$ , no entanto a primeira curva contém mais alguns pontos, os pontos no infinito. Analisemos primeiramente os pontos no infinito do tipo  $(1, s, 0)$  e posteriormente o ponto  $(0, 1, 0)$ . Os primeiros pontos vão ser caracterizados por terem  $s = 0$ , logo o ponto que pertence a esta curva é o ponto de coordenadas homogéneas  $(1, 0, 0)$ . Por sua vez, o ponto no infinito  $(0, 1, 0)$  também pertence à curva. Desta forma, concluímos que os pontos no infinito que a curva contém são o ponto  $(1, 0, 0)$ , que pertence a uma recta horizontal, e o ponto  $(0, 1, 0)$ , que pertence a uma recta vertical. Podemos associar às duas “extremidades” da hipérbole que se aproximam do eixo das ordenadas o ponto  $(0, 1, 0)$ , e às duas “extremidades” da hipérbole do plano euclidiano que se aproximam do eixo das abcissas o ponto  $(1, 0, 0)$ . Desta forma, a hipérbole no plano projectivo pode ser vista como uma curva fechada.

O número de vezes que duas curvas se intersectam na origem não é alterado quando passamos do plano euclidiano para o plano projectivo e passamos das coordenadas usuais  $(x, y)$  para as coordenadas homogéneas. Formalizamos esta ideia através da seguinte propriedade que irá ser demonstrada na secção seguinte.

### III. Intersecções

#### **Propriedade 3.11**

Sejam  $F(x, y, z)$ ,  $G(x, y, z)$  polinómios homogéneos e  $O$  a origem e consideremos, ainda, as seguintes igualdades:  $f(x, y) = F(x, y, 1)$  e  $g(x, y) = G(x, y, 1)$ . Então temos

$$I_O(F(x, y, z), G(x, y, z)) = I_O(f(x, y), g(x, y)).$$

Chegámos ao momento de introduzir uma generalização da ideia inicial de intersecção entre duas curvas na origem. Estamos a falar na multiplicidade de intersecção entre duas curvas do plano projectivo num ponto  $P$  que não a origem, ou seja, o inteiro associado a todo o par de polinómios homogéneos  $F(x, y, z)$  e  $G(x, y, z)$  e a todo o ponto  $P$  do plano projectivo. Este inteiro definido por  $I_P(F, G)$  representa o número de vezes que ambas as curvas se intersectam no ponto  $P$ . Segue-se a definição de transformação linear associada a mudanças de variáveis em coordenadas homogéneas.

#### **Definição 3.12**

Sejam  $f(x, y)$  e  $g(x, y)$  polinómios diferentes de zero,  $F(x, y, z)$  e  $G(x, y, z)$  as suas homogeneizações e  $(a, b)$  um ponto no plano euclidiano. Definimos *multiplicidade de intersecção das curvas*  $f(x, y) = 0$  e  $g(x, y) = 0$  no ponto  $(a, b)$  do plano euclidiano,  $I_{(a,b)}(f, g)$ , como sendo a multiplicidade de intersecção  $I_{(a,b,1)}(F, G)$  das curvas  $F(x, y, z) = 0$  e  $G(x, y, z) = 0$  no ponto  $(a, b, 1)$  do plano projectivo.

As transformações lineares em coordenadas homogéneas vão-nos possibilitar tirar partido da simetria do espaço euclidiano. Usamos estas transformações lineares de duas formas. Uma, com vista a determinar a multiplicidade de intersecção entre duas curvas num qualquer ponto do plano projectivo. Neste caso transportamos esse ponto para a origem e usando as técnicas anteriores para determinar a multiplicidade de intersecção. Outra, com a finalidade de simplificar as equações das curvas.

#### **Definição 3.13**

Uma transformação é uma aplicação do plano projectivo real nele próprio, que transforma qualquer ponto  $(x, y, z)$  no ponto  $(x', y', z')$  determinado pelas seguintes equações:

$$\begin{cases} x' = ax + by + cz \\ y' = dx + ey + fz \\ z' = gx + hy + iz \end{cases} \quad (4)$$

### III. Intersecções

onde  $a, \dots, i$  são números reais, em que nem todos  $x, y, z$  são iguais a zero, de tal modo que as equações em (4) são equivalentes às equações da forma:

$$\begin{cases} x = Ax' + By' + Cz' \\ y = Dx' + Ey' + Fz' \\ z = Gx' + Hy' + Iz' \end{cases}$$

em que expressa  $x, y,$  e  $z$  em termos de  $x', y', z'$  onde  $A, \dots, I$  são números reais.

As transformações do plano projectivo real consistem em transformações lineares invertíveis em coordenadas homogéneas.

#### Observações

(i) Se substituirmos  $x, y, z$  na definição por  $tx, ty, tz$  (com  $t \neq 0$ ), respectivamente, os correspondentes valores  $x', y', z'$  aparecem também multiplicados por  $t$ .

(ii) Estas transformações preservam as rectas: pontos colineares são transformados em pontos colineares.

(iii) Como nem todos  $x, y, z$  são iguais a zero, logo nem todos  $x', y', z'$  são iguais a zero.

(iv) Quando trabalhamos sobre o corpo dos complexos as transformações são do mesmo tipo (4), sendo  $a, \dots, i$  números complexos, gozando também da invertibilidade.

Como exemplos destes tipos de transformações temos:

1. A translação do plano euclidiano de  $h$  «unidades» horizontais e de  $k$  «unidades» verticais, isto é, uma aplicação que transforma o ponto  $(x, y)$  no ponto  $(x + h, y + k)$ . A correspondente transformação do plano projectivo envia o ponto  $(x, y, z)$  para o ponto  $(x', y', z')$  onde  $x' = x + hz, y' = y + kz$  e  $z' = z$ ;

2. Uma transformação que consiste na troca de duas ou mais coordenadas. Como um exemplo deste tipo de transformação temos a aplicação que alterna a primeira com a terceira coordenada definida por  $x' = z, y' = y$  e  $z' = x$ . Neste exemplo, a recta no infinito  $z = 0$  é transformada na recta  $x = 0$ . Usamos frequentemente estas transformações para enviar pontos no infinito para pontos do plano euclidiano.

3. A transformação em que se multiplicam as coordenadas por constantes diferentes de zero. Esta transformação é definida da seguinte forma  $x' = rx, y' = sy$  e  $z' = tz$  onde  $r, s$  e  $t$  são números reais diferentes de zero. Neste caso os pontos  $(x, y, z)$  são enviados para os pontos  $(rx, sy, tz)$ .

### III. Intersecções

Obviamente que destes três tipos de transformações que foram apresentados, podem sempre obter-se novas transformações que resultam da composição destas iniciais.

O teorema que se segue permite-nos garantir a existência, em determinadas condições, de uma transformação que transforma quatro pontos noutros quatro do plano projectivo.

#### **Teorema 3.14**

*Consideremos no plano projectivo quatro pontos diferentes  $A, B, C$  e  $D$ , dos quais nenhuns três são colineares, e sejam  $A', B', C'$  e  $D'$  quatro pontos com as mesmas características. Então existe uma transformação que aplica  $A, B, C$  e  $D$  em  $A', B', C'$  e  $D'$ , respectivamente.*

#### **Demonstração**

Vamos demonstrar que existe uma aplicação  $T$  que transforma os pontos  $A, B, C$  e  $D$  nos pontos  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(0, 0, 1)$  e  $(1, 1, 1)$ , respectivamente. Logo, existe uma outra transformação  $G$  que envia os pontos  $A', B', C'$  e  $D'$  para  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(0, 0, 1)$  e  $(1, 1, 1)$ , respectivamente. Como as transformações aqui definidas admitem inversa, fazendo a composta  $G^{-1} \circ T$  obtemos a transformação pretendida.

Começemos por arranjar uma transformação que envia o ponto  $A$  para o ponto de coordenadas  $(1, 0, 0)$ . Como  $A$  tem pelo menos uma coordenada diferente de zero então podemos assumir que esta é a última. Caso esta coordenada fosse a primeira, ou a segunda podíamos sempre aplicar uma transformação que alternasse a última coordenada com uma outra, de forma a garantir que esta última fosse diferente de zero.  $A$  tem coordenadas homogêneas, logo consideramos  $A = (r, s, 1)$ . Aplicando a transformação  $x' = x - rz$ ,  $y' = y - sz$  e  $z' = z$ , o ponto  $A$  é enviado para  $(0, 0, 1)$ . Aplicando novamente a transformação que alterna a primeira coordenada com a terceira, obtemos o ponto pretendido  $(1, 0, 0)$ .

Consideremos  $B'$  a imagem de  $B$  resultante das transformações até aqui aplicadas. Como as nossas transformações são invertíveis e portanto injectivas e  $A \neq B$ , logo o ponto  $B' \neq (1, 0, 0)$ . Desta forma, este ponto vai ter a terceira ou a segunda coordenada diferente de zero. Fixando o ponto  $(1, 0, 0)$  e eventualmente alternando a segunda com a terceira coordenada podemos assumir que a última coordenada de  $B'$  é diferente de zero. Seguindo o raciocínio anterior temos  $B' = (t, u, 1)$ . Aplicando a transformação  $x' = x - tz$ ,  $y' = y - uz$  e  $z' = z$ , o ponto  $B'$  é transformado em  $(0, 0, 1)$  e  $(1, 0, 0)$  mantém-se fixo. Aplicando

### III. Intersecções

novamente a transformação que altera as duas últimas coordenadas concluímos que o ponto  $B$  é transformado em  $(0, 1, 0)$ .

Consideremos  $C'$  a imagem de  $C$  resultante de todas estas transformações. Seguindo um raciocínio semelhante ao anterior podemos afirmar que  $C'$  tem coordenadas homogéneas  $(u, w, 1)$ . A transformação  $x' = x - vz$ ,  $y' = y - wz$  e  $z' = z$  vai fixar os pontos de coordenadas  $(1, 0, 0)$  e  $(0, 1, 0)$  e enviar o  $C'$  para  $(0, 0, 1)$ .

Nesta altura os pontos  $A$ ,  $B$  e  $C$  foram transformados, respectivamente, nos pontos  $A'' = (1, 0, 0)$ ,  $B'' = (0, 1, 0)$  e  $C'' = (0, 0, 1)$ .

Seja  $D'$  a imagem de  $D$  mediante todas estas transformações até aqui apresentadas.  $D'$  não pertence às rectas  $A''B''$  ( $z = 0$ ),  $B''C''$  ( $x = 0$ ) e  $A''C''$  ( $y = 0$ ), pois as transformações preservam a colineariedade. Assim,  $D'$  tem as três coordenadas diferentes de zero  $(h, k, l)$ . Aplicando a transformação  $x' = \frac{x}{h}$ ,  $y' = \frac{y}{k}$  e  $z' = \frac{z}{l}$ , o ponto  $D'$  é enviado para  $(1, 1, 1)$  e os outros três pontos mantêm-se fixos.

Fazendo a composta de todas estas transformações pela ordem indicada, concluímos que existe uma transformação que transforma os pontos  $A$ ,  $B$ ,  $C$  e  $D$  nos pontos  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(0, 0, 1)$  e  $(1, 1, 1)$  como pretendíamos.  $\square$

As transformações no plano projectivo correspondem a transformações lineares invertíveis em  $\mathbb{R}^3$ . Como sabemos, estas transformações lineares em  $\mathbb{R}^3$  são determinadas pela imagem de três vectores linearmente independentes. Parece-nos que este último teorema entra em desacordo com esta última afirmação. Este último teorema leva-nos a pensar que existem quatro graus de liberdade e não três. De facto, o quarto grau de liberdade está relacionado com a homogeneidade das coordenadas do plano projectivo.

O resultado que se segue permite-nos concluir que as transformações preservam o grau de uma curva, bem como a multiplicidade de intersecções entre curvas. A demonstração desta propriedade será apresentada na secção seguinte.

#### **Propriedade 3.15**

Consideremos a transformação do plano projectivo que transforma o ponto  $(x, y, z)$  no ponto  $(x', y', z')$ . Sejam  $P$  um ponto do plano projectivo e  $P'$  a sua imagem quando transformado. Sejam  $F(x, y, z) = 0$  e  $G(x, y, z) = 0$  curvas e  $F'(x', y', z') = 0$  e  $G'(x', y', z') = 0$  as suas imagens pela transformação. Então temos:

$$I_P(F(x, y, z), G(x, y, z)) = I_{P'}(F'(x', y', z'), G'(x', y', z')).$$

### III. Intersecções

Podemos, neste momento, estabelecer as propriedades de intersecção entre duas curvas para um ponto  $P$ , que não seja necessariamente a origem. Vamos portanto, generalizar as propriedades anteriores referentes à intersecção, mas agora, em qualquer ponto.

#### **Teorema 3.16**

Sejam dadas as curvas de equações  $F(x, y, z) = 0$ ,  $G(x, y, z) = 0$  e  $H(x, y, z) = 0$  no plano projectivo e um ponto  $P$ . Então:

- (i)  $I_P(F, G)$  representa um número inteiro não negativo ou infinito;
- (ii)  $I_P(F, G) = I_P(G, F)$ ;
- (iii)  $I_P(F, G) \geq 1$  se e só se  $F$  e  $G$  contêm  $P$ ;
- (iv)  $I_P(F, G) = I_P(F, G + FH)$  se  $G + FH$  é homogéneo;
- (v)  $I_P(F, GH) = I_P(F, G) + I_P(F, H)$ ;
- (vi)  $I_P(F, G) = \infty$  se  $F$  é factor de  $G$  e contém  $P$ .

#### **Demonstração**

Pelo teorema 3.14, sabemos que existe uma transformação que envia o ponto  $P$  para a origem. Como as transformações preservam a multiplicidade de intersecções entre duas curvas, logo pelas propriedades 3.1 a 3.5 e teorema 3.6, fica demonstrado o presente teorema.  $\square$

#### **Observação**

Seja  $K$  uma constante diferente de zero e  $F$  e  $H$  polinómios homogéneos, então

$$I_P(F, KH) = I_P(F, K) + I_P(F, H) = I_P(F, H).$$

Os polinómios  $KH$  e  $H$  representam a mesma curva, pois um é múltiplo escalar do outro. Ambas as curvas têm as mesmas soluções no plano projectivo. Identificamos numa mesma recta, todas as rectas que diferem entre si por produtos de escalares diferentes de zero.

Tal como referimos anteriormente, segue-se um resultado que nos permite afirmar que as translações preservam a multiplicidade de intersecções.

**Teorema 3.17**

Sejam  $a$  e  $b$  números reais.

(i) Sejam  $F(x, y, z)$  e  $G(x, y, z)$  polinómios homogéneos, e sejam  $f(x, y)$  e  $g(x, y)$  as suas restrições ao plano euclidiano, respectivamente, logo  $F(x, y, 1) = f(x, y)$  e  $G(x, y, 1) = g(x, y)$ . Então

$$I_{(a,b,1)}(F(x, y, z), G(x, y, z)) = I_{(0,0)}(f(x + a, y + b), g(x + a, y + b));$$

(ii) Sejam  $f(x, y)$  e  $g(x, y)$  polinómios diferentes de zero. Então

$$I_{(a,b)}(f(x, y), g(x, y)) = I_{(0,0)}(f(x + a, y + b), g(x + a, y + b));$$

(iii) Sejam  $F$  e  $G$  polinómios homogéneos, e consideremos  $F(x, y, 1) = f(x, y)$  e  $G(x, y, 1) = g(x, y)$ . Então

$$I_{(a,b,1)}(F(x, y, z), G(x, y, z)) = I_{(a,b)}(f(x, y), g(x, y)).$$

**Demonstração**

Consideremos a transformação definida por  $x' = x - az$ ,  $y' = y - bz$  e  $z' = z$  ou seja  $x = x' + az'$ ,  $y = y' + bz'$  e  $z = z'$ . Esta transformação vai transformar o ponto  $(a, b, 1)$  no ponto  $(0, 0, 1)$ . De acordo com a propriedade 3.15 temos

$$I_{(0,0,1)}(F(x' + az', y' + bz', z'), G(x' + az', y' + bz', z')) = I_{(a,b,1)}(F(x, y, z), G(x, y, z)).$$

Tomando  $z' = 1$  da igualdade anterior obtemos:

$$I_{(0,0,1)}(F(x' + a, y' + b, 1), G(x' + a, y' + b, 1)) = I_{(a,b,1)}(F(x, y, z), G(x, y, z)). \quad (6)$$

Pela propriedade 3.11 temos

$$I_{(0,0,1)}(F(x' + a, y' + b, 1), G(x' + a, y' + b, 1)) = I_{(0,0)}(f(x' + a, y' + b), g(x' + a, y' + b)). \quad (7)$$

De (6) e (7) obtemos a igualdade pretendida.

(ii) Sejam  $F(x, y, z)$  e  $G(x, y, z)$  as homogeneizadas de  $f(x, y)$  e  $g(x, y)$ . Pela definição 3.12 temos:

$$I_{(a,b)}(f(x, y), g(x, y)) = I_{(a,b,1)}(F(x, y, z), G(x, y, z)).$$

Por (i) concluímos

$$I_{(a,b)}(f(x, y), g(x, y)) = I_{(0,0)}(f(x + a, y + b), g(x + a, y + b)).$$

### III. Intersecções

(iii) De (i) e (ii) obtemos a igualdade pretendida.  $\square$

Com o teorema 3.17 (ii) facilmente determinamos a multiplicidade de intersecção entre duas curvas num ponto específico. Vejamos um exemplo.

Consideremos as curvas  $y = -2x$  e  $y = x^2 + 2x$  e consideremos o ponto  $(-4, 8)$ , queremos determinar  $I_{(-4,8)}(y + 2x, y - x^2 - 2x)$ .

Pelo teorema 3.17 (ii) temos

$$\begin{aligned} I_{(-4,8)}(y + 2x, y - x^2 - 2x) &= I_{(0,0)}(y + 8 + 2(x - 4), y + 8 - (x - 4)^2 - 2(x - 4)) \\ &= I_{(0,0)}(y + 2x, y - x^2 + 6x). \end{aligned}$$

Pelo teorema 3.8 (ii) sabemos que  $y + 2x$  não é factor de  $g(x, y) = y - x^2 + 2x$ . Como  $y = -2x$  contém a origem podemos aplicar o teorema 3.10, em que a multiplicidade de intersecção vai ser dada pelo menor grau de qualquer termo diferente de zero quando substituímos  $-2x$  por  $y$  na expressão  $y - x^2 + 6x$ . Assim, a expressão é  $(-2x) - x^2 + 6x = -x^2 + 4x$  e o valor pretendido é 1.

Até agora trabalhámos com intersecções entre duas curvas em pontos do plano euclidiano. Sabemos no entanto que existem pontos no infinito. Será que podemos determinar as intersecções em pontos no infinito? A resposta é afirmativa. Para isso basta aplicarmos uma transformação que alterna as coordenadas de forma a transportar esses pontos no infinito para o plano euclidiano e posteriormente aplicar o teorema 3.17.

Antes de terminarmos esta secção gostaríamos de dizer que todas estas propriedades da multiplicidade de intersecção do plano euclidiano real são ainda válidas no plano complexo afim. Para isso assumimos que  $O = (0, 0)$  é a origem do plano complexo afim. Denominamos  $I_O(f, g)$  como a *multiplicidade de intersecção de  $f$  e  $g$  em  $O$* , em que  $f(x, y)$  e  $g(x, y)$  são polinómios sobre os complexos de forma a estendermos as propriedades 3.1-3.5 para o plano complexo afim. Assumimos que a *multiplicidade de intersecção  $I_P(F, G)$  de  $F$  e  $G$  em  $P$*  é determinada para todos os polinómios homogéneos  $F(x, y, z)$  e  $G(x, y, z)$  com coeficientes complexos e todos os pontos  $P$  do plano projectivo complexo de forma que as propriedades 3.11 e 3.15 sejam ainda verificadas. Os restantes teoremas 3.6-3.10, 3.14, 3.16 e 3.17 seguem-se directamente das propriedades de intersecção juntamente com a definição 3.12 referente à multiplicidade de intersecção  $I_{(a,b)}(f, g)$ , que podem ser estendidos, sem qualquer alteração, ao plano complexo.

### §3.3 Independência e geradores

Na secção 3.1 e 3.2 trabalhámos com intersecções entre curvas sem nunca definirmos formalmente estas quantidades. Só agora o vamos fazer, tal como demonstrar as várias propriedades referentes a este tema que foram introduzidas anteriormente. Estamos a referir-nos às propriedades 3.1–3.5, 3.11 e 3.15. A base desta definição é a *independência de polinómios em relação a duas curvas  $f$  e  $g$  na origem*. Este vai ser o fundamento para a determinação do valor de  $I_0(f, g)$ .

Vamos começar por demonstrar as 5 primeiras propriedades relativas à intersecção entre duas curvas na origem. As primeiras 4 propriedades são de demonstração quase imediata. A propriedade 3.5, que consiste na igualdade  $I_0(f, gh) = I_0(f, g) + I_0(f, h)$ , irá ser demonstrada através de duas desigualdades. Para a demonstração de uma das desigualdades é necessário recorrer à forma fraca do teorema de Bézout. Para a demonstração da outra, vamos necessitar de introduzir uma nova definição referente ao conceito de *geradores de intersecções*. Iremos ver que para determinarmos a intersecção entre duas curvas num ponto  $P$ , que não a origem, em coordenadas homogéneas, necessitamos de uma recta (que não contém  $P$ ) que nos permite a homogeneização dos polinómios. No entanto, verificaremos que o valor da intersecção não é influenciado por essa recta. Por fim, demonstramos as propriedades 3.11 e 3.15.

Nesta secção vamos trabalhar sobre os números complexos, sendo por isso necessário rever, de uma forma breve, algumas propriedades que estes números possuem. Começemos com algumas considerações relativamente às diferenças existentes entre as curvas reais e as complexas. Se tivermos uma curva real de grau positivo (por exemplo:  $x^2 + 1 = 0$ ), esta poderá não ter pontos ou ter apenas um número finito de pontos no plano projectivo real. Este facto nunca é observado quando trabalhamos com curvas complexas de grau positivo, pois estas têm sempre infinitos pontos. Numa primeira abordagem esta afirmação parece ser pouco evidente necessitando, por isso, de ser justificada. Para isso, vamos recorrer ao *Teorema Fundamental da Álgebra* (TFA) que nos diz que *todo o polinómio de grau  $n \geq 1$  sobre os números complexos se decompõe em  $n$  factores não necessariamente diferentes*.

Consideremos a curva complexa de grau positivo  $H(x, y, z) = 0$ . Aplicando uma transformação que altere as variáveis de forma a garantirmos que  $H$  tem um termo diferente de zero de grau positivo  $t$  em  $y$ , e posteriormente substituímos  $z$  por 1, obtemos a curva

### III. Intersecções

$h(x, y) = 0$  em que

$$h(x, y) = \sum_{i=0}^t p_i(x)y^i,$$

de grau  $t$  em  $y$ , onde  $p_i(x)$  é diferente de zero. Assumindo que o polinómio  $p_i(x)$  tem grau  $k$ , pode, pelo TFA, decompor-se do seguinte modo:

$$p_i(x) = r(x - w_1) \cdots (x - w_k),$$

onde  $r, w_1, \dots, w_k$  são números complexos não necessariamente diferentes e  $r \neq 0$ . Se considerarmos um número complexo  $a$  diferente de todos os  $w_1, \dots, w_k$ , então  $p(a) \neq 0$  e, conseqüentemente,  $h(a, y)$  é um polinómio de grau positivo em  $y$ , logo, pelo TFA,  $h(a, y)$  tem pelo menos uma raiz  $b \in \mathbb{C}$ . À medida que  $a$  vai variando, vamos tendo infinitos pontos  $(a, b)$  que pertencem a  $h$  e estão no plano complexo afim. Estes correspondem a infinitos pontos  $(a, b, 1)$  pertencentes ao plano projectivo complexo.

Depois de justificada a afirmação anterior, seguem-se dois resultados relativos a polinómios sobre os complexos que facilmente se verificam. A saber:

Sejam  $F, G$  e  $H$  polinómios homogéneos. Então:

- (i) O grau do polinómio  $FG$  é a soma dos graus de  $F$  e  $G$ ;
- (ii) Se  $FG = FH$ , então  $G = H$  (Lei do Corte).

Este resultado é válido quando trabalhamos com polinómios  $F, G$  e  $H$  com coeficientes pertencentes a um domínio de integridade. No entanto, na lei do corte, temos que garantir que o polinómio  $F$  é diferente de zero.

Depois de introduzidas estas noções essenciais para a compreensão de algumas das demonstrações dos teoremas aqui apresentados, vamos então definir em que circunstâncias um conjunto de polinómios é *dependente* ou *independente* em relação a duas curvas  $f$  e  $g$  na origem.

#### **Definição 3.18**

Sejam  $n$  um inteiro positivo e  $q_1(x, y), \dots, q_n(x, y)$  polinómios com coeficientes complexos. Dizemos que  $q_1, \dots, q_n$  *dependem* de  $f$  e  $g$  na origem se e só se existem polinómios  $r(x, y), s(x, y), t(x, y)$ , e números complexos  $b_1, \dots, b_n$  tais que

$$r(b_1q_1 + \cdots + b_nq_n) = sf + tg, \tag{8}$$

onde  $r$  é diferente de zero na origem, e  $b_1, \dots, b_n$  não são todos iguais a zero.

### III. Intersecções

Dizemos que  $q_1, \dots, q_n$  são *independentes* em relação a  $f$  e  $g$  na origem se não forem dependentes.

Por convenção, o conjunto vazio de polinómios é independente em relação a  $f$  e  $g$  na origem.

A independência de polinómios relativamente a duas curvas num ponto permite-nos introduzir a seguinte definição, referente à multiplicidade de intersecção.

#### **Definição 3.19**

Definimos  $I_O(f, g)$ , *multiplicidade de intersecção* de  $f$  e  $g$  na origem do seguinte modo:

$$I_O(f, g) = \begin{cases} \infty & \text{se, para todo número inteiro positivo } c, \text{ existem pelo menos } c \\ & \text{polinómios independentes em relação a } f \text{ e a } g \text{ na origem;} \\ e & \text{onde } e \text{ é o maior número inteiro de polinómios independentes} \\ & \text{em relação a } f \text{ e a } g \text{ na origem.} \end{cases}$$

Pela definição 3.19, verificamos que  $I_O(f, g)$  é um inteiro não negativo, que representa o maior número de polinómios independentes em relação a  $f$  e  $g$  na origem. Se um conjunto de polinómios  $q_1, \dots, q_n$  é dependente em relação a  $f$  e  $g$  na origem, então facilmente se verifica que um outro conjunto finito de polinómios que o contenha também é dependente. Suponhamos que existe um inteiro positivo  $v$  tal que todo o conjunto de  $v$  polinómios é dependente em relação a  $f$  e  $g$  na origem. O mesmo se verifica para todo o conjunto com mais de  $v$  polinómios, pois este conjunto contém um subconjunto de  $v$  polinómios. Neste caso,  $I_O(f, g) < v$ .

Vejamos novamente as propriedades de intersecção 3.1-3.5 a fim de as demonstrar, tendo presente esta definição.

Existem sempre  $n$  polinómios independentes em relação a  $f$  e  $g$  na origem para  $n = 0$ , isto porque, tal como referimos acima, o conjunto vazio de polinómios é independente. De acordo com a definição 3.19,  $I_O(f, g)$  é um número inteiro não negativo ou  $\infty$  (propriedade 3.1).

Obviamente que o número de polinómios independentes em relação a  $f$  e  $g$  na origem é o mesmo que o número de polinómios independentes em relação a  $g$  e  $f$  na origem, ou seja é válida a propriedade 3.2.

### III. Intersecções

Na propriedade 3.3 pretendemos mostrar que  $I_O(f, g)$  é zero se um dos polinómios,  $f$  ou  $g$ , não contém a origem. Suponhamos, sem perda de generalidade, que  $f(0, 0) \neq 0$ . Assim, existe um polinómio  $q$  tal que  $fq = qf + 0g$ , onde  $0$  é o polinómio zero. A igualdade (8) da definição 3.18 é satisfeita: basta que  $r = f$ ,  $n = 1$ ,  $b_1 = 1$  e  $t = 0$ . Como  $f(0, 0) \neq 0$ , todo o polinómio  $q$  é dependente em relação a  $f$  e  $g$  na origem. Então também todo o conjunto com mais de um polinómio é dependente e, portanto,  $I_O(f, g) = 0$ . Consideremos agora que  $f$  e  $g$  são iguais a zero na origem. Podemos escrever  $r(b \times 1) = sf + tg$ , onde  $1$  representa o polinómio constante igual a um,  $r, s, t$  são polinómios e  $b$  um número complexo. Como o segundo membro da equação é zero na origem, então  $r(b.1) = 0$ , ou seja,  $r = 0$  na origem ou  $b = 0$ . De acordo com a definição 3.19, a constante  $1$  é independente de  $f$  e  $g$  na origem e, portanto,  $I_O(f, g)$  é, pelo menos, igual a  $1$ . O polinómio  $r(x, y)$  está associado à igualdade (8) para garantir que  $I_O(f, g) = 0$ , se  $f$  ou  $g$  não conterem a origem. O facto de se ter  $I_O(f, g) \geq 1$ , garante-nos que  $f$  e  $g$  contêm a origem.

Antes de passarmos à demonstração da propriedade 3.4, vamos estudar o exemplo referido na secção 3.1, que consiste na determinação de  $I_O(x, y)$ . Para isso, tomemos dois polinómios  $q_1$  e  $q_2$  em  $x$  e  $y$  em que os termos independentes são  $c_1$  e  $c_2$ , respectivamente. Consideremos a diferença

$$c_2q_1(x, y) - c_1q_2(x, y).$$

Esta diferença consiste num polinómio sem termo independente que é igual a  $s(x, y)x + t(x, y)y$ , onde  $s(x, y)$  e  $t(x, y)$  são polinómios. Tomando  $r(x, y) = 1$ , pela definição 3.18, temos que  $q_1$  e  $q_2$  são dependentes em relação a  $x$  e  $y$  na origem. Este raciocínio ainda é válido mesmo quando um dos polinómios  $q_1$  ou  $q_2$  não tem termo independente: neste caso consideramos  $c_1 = 0$  ou  $c_2 = 0$ . Assim, concluímos que dois quaisquer polinómios são dependentes em relação a  $x$  e  $y$  na origem e, portanto,  $I_O(x, y) \leq 1$ . Por outro lado, sabemos que  $x$  e  $y$  contêm a origem, logo  $I_O(x, y) \geq 1$ , donde se conclui que  $I_O(x, y) = 1$ .

Recordemos a propriedade 3.4 que nos diz que dados três polinómios  $f, g$  e  $h$ , temos a igualdade

$$I_O(f, g) = I_O(f, g + fh).$$

Para demonstrarmos esta igualdade vamos primeiramente mostrar a desigualdade  $I_O(f, g) \geq I_O(f, g + fh)$  e posteriormente a desigualdade  $I_O(f, g) \leq I_O(f, g + fh)$ .

Se  $I_O(f, g) = \infty$  a primeira desigualdade é imediata. Vamos assumir que  $I_O(f, g)$  é um número finito  $m$ . Seja  $m < n$  e consideremos  $q_1, \dots, q_n$  polinómios em  $x$  e  $y$ . Pela definição

### III. Intersecções

3.19 estes  $n$  polinómios são dependentes em relação a  $f$  e  $g$ , logo existem polinómios  $s(x, y)$ ,  $t(x, y)$  e  $r(x, y)$ , e complexos  $b_1, \dots, b_n$  não todos iguais a zero tais que

$$r(b_1q_1 + \dots + b_nq_n) = sf + tg = (s - th)f + t(g + fh),$$

onde  $r(0, 0) \neq 0$ . Donde se conclui que todos os polinómios que são dependentes em relação a  $f$  e  $g$ , são dependentes em relação a  $f$  e  $g + fh$  na origem e, portanto,  $I_0(f, g) \geq I_0(f, g + fh)$ . Tendo presente esta desigualdade e substituindo  $g$  por  $g + fh$  e  $h$  por  $-h$ , obtemos

$$I_0(f, g + fh) \geq I_0(f, (g + fh) + f(-h)) = I_0(f, g).$$

Obtidas as duas desigualdades fica demonstrada a propriedade 3.4.

Chegámos ao momento de mostrarmos a propriedade 3.5 que consiste na igualdade

$$I_0(f, gh) = I_0(f, g) + I_0(f, h),$$

onde  $f, g$  e  $h$  são polinómios. Tal como na propriedade 3.4, a demonstração desta igualdade é feita através de duas desigualdades, sendo no entanto mais trabalhosa que as demonstrações das propriedades anteriores. Com vista ao nosso objectivo, comecemos por demonstrar a desigualdade

$$I_0(f, gh) \geq I_0(f, g) + I_0(f, h).$$

Para isso, vamos introduzir alguns teoremas dos quais destacamos dois: um relativo à intersecção de duas curvas complexas sem factores comuns de grau positivo (forma fraca do teorema de Bézout); e um segundo em que as duas curvas complexas têm factores comuns que contêm a origem (teorema 3.23).

Antes porém, vamos enunciar um teorema que consiste num caso particular da forma fraca do teorema de Bézout em que uma das curvas é uma recta.

#### **Teorema 3.20**

*Sejam  $L = 0$  uma recta e  $G = 0$  uma curva no plano projectivo complexo. Se  $L = 0$  não é factor de  $G = 0$ , então  $L = 0$  intersecta  $G = 0$  apenas num número finito de pontos diferentes do plano projectivo complexo.*

#### **Demonstração**

Pelo teorema 3.14, existe uma transformação  $T$  que envia a recta  $L$  para o eixo das abcissas e  $G$  para  $G'$ . Como as transformações preservam a factorização, podemos assumir

### III. Intersecções

que  $L$  é a recta  $y = 0$  e que  $G'$  não tem  $y$  como factor. Juntando os termos de  $G'$  onde  $y$  não aparece, de forma a obter um novo polinómio homogéneo que denominaremos por  $H(x, z)$ , e factorizando  $y$  nos outros termos, obtemos um novo polinómio  $Q(x, y, z)$ . Assim, temos a igualdade

$$G'(x, y, z) = yQ(x, y, z) + H(x, z). \quad (9)$$

Quando  $z = 1$  em  $H(x, z)$  temos, pelo Teorema Fundamental da Álgebra, uma factorização do polinómio

$$H(x, 1) = r(x - a_1)^{s_1} \dots (x - a_k)^{s_k}, \quad (10)$$

para certos números complexos  $r \neq 0$  e  $a_1, \dots, a_k$  e inteiros positivos  $s_1, \dots, s_k$ . Da equação (10) concluímos, que os pontos do plano complexo afim que pertencem a  $y = 0$  e a  $G' = 0$ , são os pontos do tipo  $(b, 0, 1)$ , tais que  $b$  é um dos  $a_1, \dots, a_k$ . Assim,  $y = 0$  e  $G' = 0$  intersectam-se apenas num número finito de pontos diferentes do plano complexo afim.

No infinito, quando  $z = 0$ , o único ponto pertencente a  $G' = 0$  e a  $y = 0$  é  $(1, 0, 0)$ , mantendo-se ainda finito, o número de pontos diferentes resultantes da intersecção. Concluímos assim que  $L = 0$  e  $G = 0$  intersectam-se apenas num número finito de pontos diferentes do plano projectivo complexo.  $\square$

Para que possamos generalizar o teorema anterior para o caso em que  $L$  e  $G$  são duas curvas não necessariamente rectas, necessitamos de recorrer a uma técnica que nos permite reduzir o grau de uma dessas curvas. Para isso, temos que garantir que a diminuição do grau não altera o número de intersecções. Essa garantia é-nos dada pelo teorema que se segue.

Antes de enunciarmos o teorema seguinte, necessitamos de ter presente o conceito de grau de uma variável de um polinómio homogéneo. Definimos *grau em  $y$  de um polinómio homogéneo  $F$* , como sendo o maior expoente de  $y$  que aparece em todos os termos diferentes de zero do polinómio.

#### **Teorema 3.21**

*Sejam  $F = 0$  e  $G = 0$  duas curvas complexas de graus  $s$  e  $t$  em  $y$ , respectivamente. Consideremos  $s \geq t > 0$  e  $F$  e  $G$  sem factores comuns de grau positivo. Então existem curvas complexas  $F_1 = 0$  e  $G_1 = 0$  tais que:*

- (i)  $F_1$  e  $G_1$  não têm factores comuns de graus positivos;
- (ii) o grau de  $F_1$  em  $y$  é menor que  $s$  e o grau de  $G_1$  em  $y$  é  $t$ ;

### III. Intersecções

(iii)  $F$  e  $G$  intersectam-se apenas num número finito de pontos diferentes se e só se o mesmo suceder com  $F_1$  e  $G_1$ .

#### Demonstração

Seja  $G$  um polinómio homogéneo de grau  $t$  em  $y$ . Definimos um novo polinómio que designamos por  $G_1$  e que é constituído apenas pelos factores de  $G$  que contêm  $y$ ; é claro que  $G_1$  tem grau  $t$  em  $y$ . Com os restantes factores de  $G$ , construímos um novo polinómio  $H$ , que não contém  $y$ , verificando-se a igualdade  $G = G_1H$ .

Como, por hipótese,  $F$  não tem factores de grau positivo em comum com  $G$ , então não os tem com  $H$  nem com  $G_1$ .

Consideremos, ainda,  $P(x, z)$  o coeficiente de  $y^s$  em  $F$ , e  $Q(x, z)$  o coeficiente de  $y^s$  de  $G_1$ , onde  $P$  e  $Q$  são polinómios homogéneos em  $x$  e  $z$  e não contêm  $y$ .

Sejam os polinómios homogéneos  $QF$  e  $P y^{s-t} G_1$ , ambos do mesmo grau  $s$  em  $y$ , e com o mesmo coeficiente de  $y^s$  ( $PQ$ ). Chamamos  $F_1$  à diferença

$$F_1 = QF - P y^{s-t} G_1,$$

e é claro que  $F_1$  tem grau em  $y$  menor que  $s$  e não tem factores de grau positivo em comum com  $G_1$ .

Da equação  $QF - P y^{s-t} G_1 = F_1$  concluímos que os pontos que resultam da intersecção entre  $QF$  e  $G_1$  são os mesmos que resultam da intersecção entre  $F_1$  e  $G_1$ .

Sabemos que  $H$  não contém nenhum factor de grau positivo em comum com  $F$  e que não contém  $y$ , logo, ou é o polinómio constante diferente de zero, ou então pode ser factorizado como produto de factores lineares. Se  $H$  for um polinómio constante diferente de zero então os polinómios  $G_1H$  e  $G_1$  representam a mesma curva. Se  $H$  for susceptível de factorizar como produto de factores lineares e aplicando o teorema 3.20,  $H$  intersecta  $F$  num número finito de pontos diferentes no plano projectivo complexo.

Assim,  $F$  e  $G$  intersectam-se num número finito de pontos diferentes do plano projectivo complexo se e só se  $F$  e  $G_1$  também se intersectarem. Ora, isso só ocorre se e só se  $QF$  e  $G_1$  também se intersectarem num número finito de vezes. O teorema segue-se porque  $QF$  e  $G_1$  intersectam os mesmos pontos que  $F_1$  e  $G_1$ .  $\square$

#### **Teorema 3.22 (Forma fraca do teorema de Bézout)**

*Duas curvas que não têm factores em comum de grau positivo, intersectam-se num número finito de pontos no plano projectivo complexo.*

### III. Intersecções

#### Demonstração

Sejam  $F = 0$  e  $G = 0$  duas curvas complexas. Se ambas tiverem graus positivos em  $y$ , pelo teorema 3.21 podemos reduzir o grau de uma delas repetidas vezes, de forma a que este seja zero. Pelos teoremas 3.20 e 3.21, concluímos que as curvas intersectam-se num número finito de pontos no plano projectivo complexo.  $\square$

Dizemos que um polinómio é *irreduzível*, sobre um corpo, quando não é possível factoriza-lo como produto de dois polinómios de menores graus sobre o mesmo corpo.

#### Teorema 3.23

Se  $f$  e  $g$  são curvas complexas que têm um factor em comum que contém a origem. Então  $I_O(f, g) = \infty$ .

#### Demonstração

Seja  $w(x, y)$  um factor comum a  $f$  e  $g$  que contém a origem. Se  $w$  é zero então podemos dizer que  $w$  contém um termo irreduzível como, por exemplo,  $x$  ( $x \times 0 = 0$ ). Se  $w$  é diferente de zero, então, por conter a origem, não é um polinómio constante, sendo, por isso, um polinómio de grau maior ou igual a 1. Neste último caso, pelo TFA podemos garantir que existe um termo linear irreduzível que contém a origem. Em suma,  $w(x, y)$  é um factor comum a  $f$  e  $g$  que contém um termo irreduzível  $p(x, y)$  de grau 1 que contém a origem.

Se necessário, podemos aplicar uma transformação que altere  $y$  com o  $x$  de forma a garantirmos que  $x$  esteja no polinómio  $p(x, y)$ .

Vamos verificar que os  $n$  polinómios  $y, y^2, \dots, y^n$  são independentes em relação a  $f$  e  $g$  na origem para todo o inteiro positivo  $n$ . Para isso, consideremos os polinómios  $r, s, t$  em  $x$  e  $y$  e os números complexos  $b_1, \dots, b_n$  de forma a satisfazer a equação

$$r(b_1y + b_2y^2 + \dots + b_ny^n) = sf + tg.$$

Se os números  $b_1, \dots, b_n$  não forem todos iguais a zero, obrigatoriamente  $r$  terá que ser zero na origem, donde concluímos que, para todo o  $n$ , existem  $y, y^2, \dots, y^n$ , polinómios independentes em relação a  $f$  e  $g$  na origem e consequentemente  $I_O(f, g) = \infty$ . Assim, temos um factor  $p$  irreduzível, comum a  $f$  e a  $g$ , logo um factor de  $sf + tg$ . Pela igualdade anterior, este é também um factor de  $r(b_1y + b_2y^2 + \dots + b_ny^n)$ . Se nem todos os  $b_1, \dots, b_n$  forem iguais a zero,  $b_1y + b_2y^2 + \dots + b_ny^n$  não tem factores em comum com  $p$ , e portanto  $p$  é factor de  $r$ . Como  $p$  contém a origem também  $r$  a vai conter, e portanto  $r$  é zero na origem.

### III. Intersecções

Assim, concluímos que para todo o  $n$  existem  $y, y^2, \dots, y^n$  polinómios independentes em relação a  $f$  e a  $g$  na origem e, conseqüentemente,  $I_O(f, g) = \infty$ .  $\square$

Neste momento podemos provar a primeira desigualdade da propriedade 3.5.

#### Teorema 3.24

Sejam  $f, g, h$  polinómios em  $x$  e  $y$ , e seja  $O$  a origem. Então temos

$$I_O(f, gh) \geq I_O(f, g) + I_O(f, h).$$

#### Demonstração

Se  $f$  e  $g$  contêm um factor comum que contenha a origem então também  $gh$  contém esse mesmo factor. Nestas circunstâncias, pelo teorema 3.23, sabemos que

$$I_O(f, gh) = I_O(f, g) = \infty,$$

sendo verdadeira a desigualdade. Assim, se  $f$  não contiver a origem, então pelas propriedades 3.1 e 3.3 concluímos que  $I_O(f, gh) = I_O(f, g) = I_O(f, h) = 0$ , e neste caso também é válida a desigualdade.

Vamos supor que  $f$  e  $g$  não contêm nenhum factor em comum que contenha a origem mas que, no entanto,  $f$  contém a origem. Tendo em consideração estes pressupostos, temos a garantia que  $g \neq 0$ .

Sejam  $p_1, \dots, p_m$  polinómios em  $x$  e em  $y$  independentes em relação a  $f$  e  $g$  na origem e  $q_1, \dots, q_n$  polinómios em  $x$  e em  $y$  independentes em relação a  $f$  e  $h$  na origem. Vamos mostrar que  $p_1, \dots, p_m, q_1g, \dots, q_n g$  são independentes em relação a  $f$  e  $gh$  na origem. Para isso, consideremos os polinómios  $r(x, y), s(x, y), t(x, y)$  e os números complexos  $a_1, \dots, a_m, b_1, \dots, b_n$  tais que

$$r(a_1 p_1 + \dots + a_m p_m + b_1 q_1 g + \dots + b_n q_n g) = s f + t g h, \quad (11)$$

onde  $r(0, 0) \neq 0$ .

Ora,

$$r(a_1 p_1 + \dots + a_m p_m) = s f + (t h - b_1 q_1 - \dots - b_n q_n) g. \quad (12)$$

De (12) e sabendo que  $p_1, \dots, p_m$  são independentes em relação a  $f$  e  $g$  na origem [como  $r(0, 0) \neq 0$ ], então  $a_1, \dots, a_m$  são todos iguais a zero, ou seja de (11) obtemos

$$r(b_1 q_1 + \dots + b_n q_n) g = s f + t g h. \quad (13)$$

### III. Intersecções

Com o objectivo de eliminar  $g$  da igualdade anterior, vamos considerar o polinómio  $d$  definido como sendo o produto de todos os factores comuns existentes em  $f$  e  $g$  (no caso de  $f$  e  $g$  não terem factores comuns temos  $d = 1$ ). Assim, existem polinómios  $f'(x, y)$  e  $g'(x, y)$  tais que  $f = f'd$  e  $g = g'd$ . Substituindo estes valores na igualdade (13), temos

$$r(b_1q_1 + \dots + b_nq_n)g'd = sf'd + tg'dh.$$

Pela lei do corte e porque  $d \neq 0$ , obtemos

$$r(b_1q_1 + \dots + b_nq_n)g' = sf' + tg'h. \quad (14)$$

Como  $g'$  é factor do primeiro membro e de  $tg'h$ , então é necessariamente factor de  $sf'$ . Mas como não existem factores em comum a  $g'$  e  $f'$ , logo  $g'$  é factor de  $s$ . Assim, existe um polinómio  $w(x, y)$  tal que  $g'w = s$ . Considerando esta igualdade, aplicando novamente a lei do corte ( $g' \neq 0$ ) e multiplicando (14) por  $d$  obtemos

$$r(b_1q_1 + \dots + b_nq_n)d = wf'd + thd.$$

Como  $f'd = f$  então

$$rd(b_1q_1 + \dots + b_nq_n) = wf + thd.$$

Como  $q_1, \dots, q_n$  são polinómios em  $x$  e em  $y$  independentes em relação a  $f$  e  $h$  na origem, e  $rd$  é diferente de zero na origem, então  $b_1, \dots, b_n$  são todos iguais a zero. Assim  $a_1, \dots, a_m$ , e  $b_1, \dots, b_n$  são todos iguais a zero e, pela igualdade (11), concluimos que os  $m + n$  polinómios  $p_1, \dots, p_m, q_1g, \dots, q_n g$  são independentes em relação a  $f$  e a  $gh$  na origem.

Resumindo: se tivermos  $n$  polinómios independentes em relação a  $f$  e  $g$  na origem e  $m$  polinómios independentes em relação a  $f$  e  $h$  na origem, então temos  $n + m$  polinómios independentes em relação a  $f$  e  $gh$  na origem. Segue-se a desigualdade pretendida.  $\square$

Depois de demonstrada a desigualdade  $I_0(f, gh) \geq I_0(f, g) + I_0(f, h)$ , vamos continuar o nosso estudo de forma a demonstrar a desigualdade  $I_0(f, g) + I_0(f, h) \geq I_0(f, gh)$  para que possamos obter a igualdade. Para atingirmos esse objectivo necessitamos de introduzir o conceito de geradores que nos é dado pela definição 3.26. Antes, porém, vamos apresentar um resultado relativo a um algoritmo entre polinómios necessário para a demonstração da desigualdade pretendida.

### III. Intersecções

#### **Teorema 3.25:**

Sejam  $I_0(f, g)$  um número finito e  $r(x, y)$  um polinómio diferente de zero na origem. Então existem polinómios  $c, d, s$  e  $t$  em  $x$  e  $y$  tais que

$$c(rd - 1) = sf + tg,$$

onde  $c$  e  $d$  são diferentes de zero na origem.

#### **Demonstração**

Seja  $I_0(f, g) = e$ , onde  $e$  é um número inteiro não negativo. Sejam  $1, x, \dots, x^e, e + 1$  polinómios dependentes em relação a  $f$  e  $g$  na origem. Assim, existem polinómios  $u, v, w$  em  $x$  e  $y$  e números complexos  $b_0, \dots, b_e$  não todos iguais a zero tais que:

$$u(b_0 + b_1x + \dots + b_ex^e) = vf + wg,$$

onde  $u(0, 0) \neq 0$ .

Seja  $m$  o menor inteiro tal que  $b_m \neq 0$ . Podemos factorizar  $x^m$  de forma a obtermos

$$x^m p = vf + wg, \quad (15)$$

onde  $p(0, 0) \neq 0$ . Analogamente, mostramos que existem polinómios  $p', v', w'$  em  $x$  e  $y$  e um inteiro não negativo  $n$  tais que

$$y^n p' = v'f + w'g, \quad (16)$$

onde  $p'(0, 0) \neq 0$ .

Visto que  $r(0, 0) \neq 0$ , vamos designar por  $a$  o seu termo constante diferente de zero. Podemos escrever  $a^{-1}r = 1 + q$ , onde  $q(x, y)$  é um polinómio sem termo constante.

Seja o polinómio  $d(x, y)$  definido por:

$$d = a^{-1}(1 - q + q^2 - \dots + (-1)^{m+n}q^{m+n}).$$

Como  $q(x, y)$  não tem termo constante então  $d(0, 0) = a^{-1} \neq 0$ .

Ora,

$$\begin{aligned} rd - 1 &= ra^{-1}(1 - q + q^2 - \dots + (-1)^{m+n}q^{m+n}) - 1 \\ &= (1 + q)(1 - q + q^2 - \dots + (-1)^{m+n}q^{m+n}) - 1 \\ &= (-1)^{m+n}q^{m+n+1}. \end{aligned}$$

Observe-se que  $q$  não tem termo constante. Todos os seus termos têm  $x$  ou  $y$  como factor. Assim, todos os termos de  $q^{m+n+1}$  vão ter  $x^m$  ou  $y^n$  como factor. De (15) e (16) segue-se que

### III. Intersecções

$pp'q^{m+n+1}$  é a soma de múltiplos de  $f$  e  $g$ . Desta forma, e tomando  $c = pp'$  (diferente de zero na origem), obtemos a igualdade pretendida.  $\square$

Tal como referimos, estamos, neste momento, preparados para introduzir o conceito de geradores, mais precisamente de polinómios gerarem intersecções, para isso, vamos assumir que  $f, g, e h$  são polinómios em  $x$  e  $y$  e  $O$  a origem.

#### **Definição 3.26**

Seja  $n$  um inteiro não negativo e sejam  $q_1, \dots, q_n$  polinómios em  $x$  e  $y$ . Dizemos que  $q_1, \dots, q_n$  geram a intersecção de  $f$  e  $g$  na origem, se para todo o polinómio  $e(x, y)$  existem polinómios  $r(x, y), s(x, y), t(x, y)$ , e números complexos  $b_1, \dots, b_n$  tais que

$$r(e + b_1q_1 + \dots + b_nq_n) = sf + tg \quad (17)$$

para  $r(0, 0) \neq 0$ .

Os geradores permitem-nos reconhecer conjuntos maximais de polinómios independentes em relação a duas curvas na origem. Se tivermos um conjunto de polinómios independentes que não gera a intersecção de duas curvas na origem, então este conjunto é um subconjunto de um outro que a gera. Ou seja, um conjunto maximal de polinómios independentes gera a intersecção. Este resultado é apresentado pelo teorema seguinte.

#### **Teorema 3.27**

*Seja  $m$  um inteiro não negativo. Se a intersecção de  $f$  e  $g$  na origem é gerada por  $m$  polinómios, então qualquer conjunto de polinómios independentes em relação a  $f$  e  $g$  na origem contém, no máximo,  $m$  polinómios.*

#### **Demonstração**

Queremos mostrar que qualquer conjunto com mais de  $m$  polinómios é dependente. Seja  $n$  um número inteiro maior que  $m$ . Consideremos  $n$  polinómios em  $x$  e  $y$ , que designaremos por  $q_1, \dots, q_n$ . Por hipótese, existem  $m$  polinómios em  $x$  e  $y$ ,  $p_1, \dots, p_m$  que geram a intersecção de  $f$  e  $g$  na origem. Porque estes polinómios geram esta intersecção, então para cada polinómio  $q_j$ , existem polinómios  $r_j, s_j, t_j$  em  $x$  e  $y$  e números complexos  $b_{1j}, \dots, b_{mj}$ , que satisfazem a equação

### III. Intersecções

$$r_j(q_j + b_{1j}p_1 + \dots + b_{mj}p_m) = s_j f + t_j g,$$

onde  $r_j(0, 0) \neq 0$ .

Multiplicamos a equação anterior membro a membro por  $r_1 \dots r_j r_{j-1} \dots r_n$ , de forma a obtermos  $r$  no primeiro membro:

$$r(q_j + b_{1j}p_1 + \dots + b_{mj}p_m) = u_j f + v_j g, \quad (18)$$

para os polinómios  $u_j, v_j$  em  $x$  e  $y$ , onde  $r = r_1 \dots r_n$  não depende de  $j$ ,  $r(0, 0) \neq 0$ ,  $u_j = r_1 \dots r_j r_{j-1} \dots r_n s_j$  e  $v_j = r_1 \dots r_j r_{j-1} \dots r_n t_j$ . Multiplicando novamente (18) membro a membro por um complexo  $c_j$  que irá ser determinado mais tarde, obtemos

$$r(c_j q_j + b_{1j} c_j p_1 + \dots + b_{mj} c_j p_m) = c_j u_j f + c_j v_j g. \quad (19)$$

Consoante o valor de  $j = 1, \dots, n$ , temos  $n$  equações do tipo (19). Somando todas elas membro a membro, obtemos:

$$r[(c_1 q_1 + \dots + c_n q_n) + (b_{11} c_1 + \dots + b_{1n} c_n) p_1 + \dots + (b_{m1} c_1 + \dots + b_{mn} c_n) p_m] = u f + v g \quad (20)$$

para  $u = c_1 u_1 + \dots + c_n u_n$  e  $v = c_1 v_1 + \dots + c_n v_n$ .

Determinemos, agora, os valores de  $c_1, \dots, c_n$  de forma a garantirmos que os coeficientes de  $p_1, \dots, p_m$ , na equação (20), sejam todos iguais a zero. Para isso, consideremos o sistema homogéneo de equações lineares nos  $c_i$ 's:

$$\begin{cases} b_{11} c_1 + \dots + b_{1n} c_n = 0, \\ \dots \\ b_{m1} c_1 + \dots + b_{mn} c_n = 0. \end{cases}$$

Neste sistema temos  $m$  equações e  $n$  variáveis, ou seja, maior número de variáveis do que de equações. Um resultado sobejamente conhecido da álgebra linear diz-nos que, um sistema de equações lineares homogéneas com mais variáveis que equações tem sempre solução, para além da solução trivial. Consideremos  $c_1, \dots, c_n$  uma solução não trivial deste sistema.

Substituindo os valores  $b_{11} c_1 + \dots + b_{1n} c_n = 0, \dots, b_{m1} c_1 + \dots + b_{mn} c_n = 0$ , na equação (20), obtemos

$$r(c_1 q_1 + \dots + c_n q_n) = u f + v g,$$

onde  $r(0, 0) \neq 0$  e  $c_1, \dots, c_n$  são números complexos não todos iguais a zero, logo  $q_1, \dots, q_n$  são dependentes. Concluimos, assim, que qualquer conjunto de mais de  $m$  polinómios em  $x$  e  $y$  é linearmente independente em relação a  $f$  e  $g$  na origem.  $\square$

### III. Intersecções

Chegámos ao momento de completar a demonstração da propriedade 3.5.

#### **Teorema 3.28**

*Sejam  $f, g, h$  polinómios em  $x$  e  $y$ , e seja  $O$  a origem. Então temos*

$$I_O(f, gh) \leq I_O(f, g) + I_O(f, h).$$

#### **Demonstração**

Se  $I_O(f, g)$  ou  $I_O(f, h)$  forem iguais a  $\infty$  então a demonstração é imediata. Vamos, por isso, assumir que ambas as quantidades são diferentes de  $\infty$ . Desta forma, existem inteiros não negativos  $m$  e  $n$ , tais que  $I_O(f, g) = m$  e  $I_O(f, h) = n$ . Pela definição 3.19 e teorema 3.27, existem no máximo  $m$  polinómios independentes  $p_1, \dots, p_m$  em relação a  $f$  e  $g$  na origem, e existem no máximo  $n$  polinómios independentes  $q_1, \dots, q_n$  em relação a  $f$  e  $h$  na origem.

O nosso objectivo é mostrar que os  $m + n$  polinómios  $p_1, \dots, p_m, q_1g, \dots, q_n g$  geram a intersecção de  $f$  e  $gh$  na origem. Se o fizermos, pelo teorema 3.27, todo o conjunto de polinómios independentes em relação a  $f$  e  $gh$  na origem tem, no máximo,  $m + n$  polinómios, e, portanto,  $I_O(f, gh) \leq m + n = I_O(f, g) + I_O(f, h)$ .

Vamos então provar que os  $m + n$  polinómios apresentados geram  $I_O(f, gh)$ .

Seja  $e(x, y)$  um polinómio. Como  $p_1, \dots, p_m$  geram  $I_O(f, g)$ , então existem polinómios  $r(x, y)$ ,  $s(x, y)$  e  $t(x, y)$  e números complexos  $a_1, \dots, a_m$  tais que

$$r(e + a_1 p_1 + \dots + a_m p_m) = sf + tg, \quad (21)$$

onde  $r(0, 0) \neq 0$ .

Passando o termo  $tg$  para o primeiro membro e sabendo que  $I_O(f, h)$  é finito e  $r(0, 0) \neq 0$ , concluímos, pelo teorema 3.25, que existem polinómios  $c, d, k$  e  $l$  em  $x$  e  $y$  tais que  $c(rd - 1) = kf + lh$ , onde  $c$  e  $d$  são diferentes de zero na origem. Aplicando a propriedade distributiva temos  $crd - c = kf + lh$ . Multiplicando ambos os membros da equação por  $-tg$ , esta vem:

$$-crdtg + ctg = -tkgf - tlgh. \quad (22)$$

Multiplicando ambos os membros de (21) por  $c$  e adicionando (22) membro a membro, obtemos

$$cr(e + a_1 p_1 + \dots + a_m p_m - dtg) = (cs - tkg)f - tlgh. \quad (23)$$

### III. Intersecções

Como  $q_1, \dots, q_n$  geram  $I_0(f, h)$ , então existem polinómios  $u, v, w$  e números complexos  $b_1, \dots, b_n$  tais que para  $u(0, 0) \neq 0$ , temos

$$u(dt + b_1q_1 + \dots + b_nq_n) = vf + wh. \quad (24)$$

Multiplicando ambos os membros de (23) por  $u$  e os de (24) por  $crg$  e adicionando membro a membro as duas equações resultantes, obtemos

$$cru(e + a_1p_1 + \dots + a_m p_m + b_1q_1g + \dots + b_nq_n g) = (csu - tkgu + vcrg)f + (wcr - tlu)gh.$$

O produto  $cru$  é diferente de zero na origem, pois é o produto de factores diferentes de zero nesse ponto. Assim, para todo a polinómio  $e(x, y)$  existem  $m + n$  polinómios que geram a intersecção de  $f$  e  $gh$  na origem, donde segue o resultado pretendido.  $\square$

Demonstradas as propriedades 3.1–3.5, vamos passar à demonstração das restantes propriedades (3.11 e 3.15) referentes à multiplicidade da intersecção num ponto qualquer do plano projectivo complexo, que não a origem.

Começemos por definir, para coordenadas homogéneas, dependência de polinómios em relação a duas curvas num ponto.

#### Definição 3.29

Sejam  $F, G, Q_1, \dots, Q_n$  polinómios homogéneos em  $x, y$  e  $z$  e  $n$  é um inteiro positivo. Seja  $P$  um ponto do plano projectivo complexo e  $L = 0$  uma recta que não contém  $P$ . Sejam  $k_1, \dots, k_n$  inteiros que representam os graus de  $Q_1, \dots, Q_n$ , respectivamente, onde  $k$  é o maior de todos os graus. Dizemos que  $Q_1, \dots, Q_n$  são dependentes em relação a  $F$  e  $G$  em  $P$  através de  $L$ , se existirem polinómios homogéneos ou polinómios iguais a zero  $R, S$  e  $T$  em  $x, y$  e  $z$  e números complexos  $b_1, \dots, b_n$  que satisfazem a equação

$$R(b_1L^{k-k_1}Q_1 + \dots + b_nL^{k-k_n}Q_n) = SF + TG,$$

onde  $R$  toma valor diferente de zero no ponto  $P$  e  $b_1, \dots, b_n$  não são todos iguais a zero.

Quando  $Q_1, \dots, Q_n$  não são dependentes em relação a  $F$  e  $G$  em  $P$  através de  $L$ , dizemos que são independentes. Tal como na definição 3.18, por convenção o conjunto vazio de polinómios é independente.

Com o factor  $L$  da equação da definição 3.29, temos a garantia de que todos os termos diferentes de zero, que estão dentro do parênteses, têm o mesmo grau  $k$ . Assim, o membro esquerdo desta equação é representado por um polinómio homogéneo ou pelo polinómio zero.

Podemos também generalizar a definição 3.19 para coordenadas homogéneas.

### III. Intersecções

#### **Definição 3.30**

Sejam  $F$  e  $G$  polinómios homogéneos em  $x, y$  e  $z$ . Seja  $P$  um ponto pertencente ao plano projectivo complexo e  $L = 0$  uma recta que não contém  $P$ . Definimos multiplicidade de intersecção de  $F$  e  $G$  em  $P$  através de  $L$ , que representamos por  $I_P^L(F, G)$ , do seguinte modo:

- $I_P^L(F, G) = \infty$  se, para todo número inteiro positivo  $c$ , existem pelo menos  $c$  polinómios independentes em relação a  $F$  e  $G$  em  $P$  através de  $L$ .

- $I_P^L(F, G) = e$ , onde  $e$  é o maior número inteiro de polinómios independentes em relação a  $F$  e  $G$  em  $P$  através de  $L$ .

O resultado seguinte estabelece a equivalência entre as definições 3.19 e 3.30, onde  $P$  é a origem e  $L = 0$  a recta no infinito.

#### **Teorema 3.31**

Sejam  $F$  e  $G$  polinómios homogéneos em  $x, y$  e  $z$ ,  $f(x, y) = F(x, y, 1)$  e  $g(x, y) = G(x, y, 1)$ . Seja  $O$  a origem e  $z = 0$  a recta no infinito. Então temos

$$I_P^z(F, G) = I_O(f, g).$$

#### **Demonstração**

Para chegarmos à igualdade vamos demonstrar as duas desigualdades:

(i)  $I_P^z(F, G) \leq I_O(f, g)$ ;

(ii)  $I_P^z(F, G) \geq I_O(f, g)$ .

(i) Como a desigualdade é trivialmente verdadeira quando  $I_O(f, g) = \infty$ , vamos assumir que existe um  $m$  inteiro não negativo tal que  $I_O(f, g) = m$ . Seja  $n$  um inteiro maior que  $m$ . Consideremos  $n$  polinómios homogéneos em  $x, y$  e  $z$ ,  $Q_1, \dots, Q_n$ , em que os graus são respectivamente  $k_1, \dots, k_n$ . Representamos por  $k$  o maior de todos os graus. Quando  $z = 1$  os polinómios  $Q_1, \dots, Q_n$  dão origem aos polinómios  $q_1, \dots, q_n$ , respectivamente. Porque  $I_O(f, g) = m$  e  $n > m$ , então  $q_1, \dots, q_n$  são dependentes em relação a  $f$  e  $g$  na origem (definição 3.19). Assim, existem polinómios  $r, s, t$  em  $x$  e  $y$  e números complexos  $b_1, \dots, b_n$  tais que

$$r(b_1q_1 + \dots + b_nq_n) = sf + tg, \quad (25)$$

para  $r(0, 0) \neq 0$  e  $b_1, \dots, b_n$  não todos iguais a zero. Multiplicamos a equação (25) por potências de  $z$  apropriadas, de modo a obtermos  $R, S, T$  como polinómios homogéneos em  $x, y$  e  $z$  ou como polinómios zero tais que

### III. Intersecções

$$R(b_1 z^{k-k_1} Q_1 + \dots + b_n z^{k-k_n} Q_n) = SF + TG, \quad (26)$$

para  $R(0, 0, 1) \neq 0$ . Pela definição 3.29,  $Q_1, \dots, Q_n$  são dependentes em relação a  $F$  e  $G$  na origem através da recta  $z = 0$ . Seguindo-se a desigualdade pretendida.

(ii) Como a desigualdade é trivialmente verdadeira quando  $I_P^z(F, G) = \infty$ , vamos assumir que existe um  $m$  inteiro não negativo tal que  $I_P^z(F, G) = m$ . Seja  $n$  um inteiro maior que  $m$ . Consideremos  $n$  polinómios em  $x, y$   $q_1, \dots, q_n$ . Vamos inicialmente assumir que  $q_1, \dots, q_n$  são todos diferentes de zero. Sejam  $Q_1, \dots, Q_n$  os seus homogeneizados, e  $k_1, \dots, k_n$  os respectivos graus, sendo  $k$  o maior de todos eles. Porque  $I_P^z(F, G) = m$  e  $n > m$ , então  $Q_1, \dots, Q_n$  são dependentes em relação a  $F$  e  $G$  na origem através de  $z = 0$  (definição 3.30). Assim, existem polinómios homogéneos ou polinómios zero  $R, S, T$  em  $x, y$  e  $z$  e números complexos  $b_1, \dots, b_n$  tais que

$$R(b_1 z^{k-k_1} Q_1 + \dots + b_n z^{k-k_n} Q_n) = SF + TG, \quad (27)$$

para  $R(0, 0, 1) \neq 0$  e  $b_1, \dots, b_n$  não todos iguais a zero. Considerando  $z = 1$  em  $R, S, T$  obtemos polinómios  $r, s, t$  em  $x$  e  $y$ . Tomando  $z = 1$  em (27), obtemos (25) e de  $R(0, 0, 1) \neq 0$  passamos para  $r(0, 0) \neq 0$ . Desta forma,  $b_1, \dots, b_n$  não são todos iguais a zero e  $q_1, \dots, q_n$  são dependentes em relação  $I_O(f, g)$  (definição 3.18). Suponhamos agora que existe um  $q_w$  tal que  $q_w = 0$ , neste caso considerarmos  $b_w = 1, b_j = 0$  para  $j \neq w, r = 1, s = 0$  e  $t = 0$ . Em resumo, dados  $n$  polinómios  $q_1, \dots, q_n$  em  $x$  e  $y$ , estes são dependentes em relação a  $f$  e  $g$  na origem para todo o inteiro  $n$  maior que  $I_P^z(F, G)$ , verificando-se a desigualdade pretendida.  $\square$

Como as transformações preservam as relações entre os polinómios, é de prever-se que as transformações preservem também as quantidades  $I_P^L(F, G)$ . Este resultado é nos dado pelo teorema seguinte.

#### **Teorema 3.32**

*Sejam  $F$  e  $G$  dois polinómios homogéneos em  $x, y$  e  $z$ . Sejam  $P$  um ponto pertencente ao plano projectivo complexo e  $L = 0$  uma recta que não contém  $P$ . Dada uma transformação  $T$ , em que  $F', G', P', L'$  são as imagens de  $F, G, P, L$ , respectivamente, temos a seguinte igualdade*

$$I_P^L(F, G) = I_{P'}^{L'}(F', G').$$

### III. Intersecções

#### Demonstração

Inicialmente vamos demonstrar a desigualdade  $I_P^L(F, G) \leq I_{P'}^{L'}(F', G')$ . Como para  $I_{P'}^{L'}(F', G') = \infty$  a desigualdade é imediata, vamos assumir que esta quantidade é igual a um número inteiro não negativo. Seja  $n$  um número inteiro maior que  $I_{P'}^{L'}(F', G')$  e consideremos  $n$  polinómios homogéneos em  $x, y$  e  $z$  que representamos por  $Q_1, \dots, Q_n$  cujos graus são  $k_1, \dots, k_n$  respectivamente. Seja  $k$  o maior de todos os graus. Consideremos, ainda, a transformação  $T$  que envia o ponto  $(x, y, z)$  para o ponto  $(x', y', z')$  como na definição 3.13, e sejam  $P'$  a imagem de  $P$ ,  $L'$  a imagem de  $L$ , e  $Q'_1, \dots, Q'_n$  as imagens dos polinómios  $Q_1, \dots, Q_n$ , respectivamente. Por hipótese sabemos que a recta  $L$  não contém  $P$ , logo a relação entre as respectivas imagens quando transformadas mantém-se, e portanto a recta  $L'$  não vai conter  $P'$ . Como  $n$  é maior que  $I_{P'}^{L'}(F', G')$ , então  $Q'_1, \dots, Q'_n$  são, pela definição 3.29, dependentes em relação a  $F'$  e  $G'$  em  $P'$  através de  $L'$ . Assim, existem polinómios homogéneos ou polinómios zero  $R', S', T'$  em  $x', y'$  e  $z'$  e números complexos  $b_1, \dots, b_n$  que satisfazem a equação

$$R'(b_1 L'^{k-k_1} Q'_1 + \dots + b_n L'^{k-k_n} Q'_n) = S' F' + T' G', \quad (28)$$

onde  $R'$  não contém  $P'$  e  $b_1, \dots, b_n$  não são todos iguais a zero.

Tal como referimos, a transformação  $T$  é dada pelas expressões de  $x', y'$  e  $z'$  como funções de  $x, y$  e  $z$ , como em (4) da definição 3.13. Fazendo essa substituição em (28), os polinómios  $R', S', T'$  em  $x', y', z'$  dão lugar aos polinómios  $R, S, T$  em  $x, y, z$  e a equação vem

$$R(b_1 L^{k-k_1} Q_1 + \dots + b_n L^{k-k_n} Q_n) = S F + T G,$$

onde  $R$  não contém  $P$ . Desta forma os polinómios  $Q_1, \dots, Q_n$  são dependentes em relação a  $F$  e  $G$  em  $P$  através de  $L$ . Como a igualdade é satisfeita para quaisquer  $n$  polinómios, então  $n$  é maior que  $I_P^L(F, G)$ .

Para demonstrarmos a outra desigualdade, vamos trabalhar com a inversa da transformação  $T$ . Aplicamos a inversa da transformação  $T$ , que envia o ponto  $(x', y', z')$  para o ponto  $(x, y, z)$ , e seguindo um raciocínio semelhante, concluímos que  $I_P^L(F, G) \leq I_{P'}^{L'}(F', G')$ .

Obtidas as duas desigualdades, temos a igualdade pretendida.  $\square$

### III. Intersecções

#### **Teorema 3.33**

Sejam  $F$  e  $G$  polinómios homogéneos em  $x$ ,  $y$  e  $z$  e seja  $P$  um ponto do plano projectivo complexo. Sejam  $L = 0$ ,  $M = 0$  duas rectas que não contêm  $P$ . Então temos a igualdade

$$I_P^L(F, G) = I_P^M(F, G).$$

#### **Demonstração**

Inicialmente vamos demonstrar a desigualdade  $I_P^L(F, G) \leq I_P^M(F, G)$ . Sejam  $D$  e  $E$  dois pontos da recta  $M$  e sejam  $D'$  e  $E'$  dois pontos da recta no infinito  $z = 0$ .  $P$  não é colinear a  $D$  e  $E$  (pois  $P$  não pertence a  $M$ ) e a origem não é colinear a  $D'$  e  $E'$  (pois a origem não pertence à recta no infinito). Existe uma transformação que envia  $P$  para a origem,  $D$  para  $D'$  e  $E$  para  $E'$  e portanto envia a recta  $M$  para a recta no infinito. Queremos mostrar  $I_O^L(F, G) \leq I_O^z(F, G)$ , ou seja, pelo teorema 3.31,

$$I_O^L(F, G) \leq I_O(f, g),$$

onde  $f(x, y) = F(x, y, 1)$  e  $g(x, y) = G(x, y, 1)$ . Como esta desigualdade é imediata quando  $I_O(f, g) = \infty$ , vamos assumir que esta quantidade é igual a um número inteiro não negativo. Seja  $n$  um número inteiro maior que  $I_O(f, g)$  e consideremos  $n$  polinómios homogéneos em  $x$ ,  $y$  e  $z$  que representamos por  $Q_1, \dots, Q_n$ , cujos graus são  $k_1, \dots, k_n$ , respectivamente. Seja  $k$  o maior de todos estes graus. Queremos provar que estes  $n$  polinómios são dependentes em relação a  $F$  e  $G$  na origem através de  $L$ .

Sejam  $l, q_1, \dots, q_n$  polinómios em  $x$  e  $y$  obtidos de  $L, Q_1, \dots, Q_n$  quando  $z = 1$ , respectivamente. Porque  $n$  é maior que  $I_O(f, g)$ , então os polinómios  $l^{k-k_1}q_1, \dots, l^{k-k_n}q_n$  são dependentes em relação a  $f$  e  $g$  na origem. Assim, existem polinómios  $r, s$  e  $t$  em  $x$  e  $y$  e números complexos  $b_1, \dots, b_n$ , que satisfazem a equação

$$r(b_1l^{k-k_1}q_1 + \dots + b_nl^{k-k_n}q_n) = sf + tg, \quad (29)$$

onde  $r(0, 0) \neq 0$  e  $b_1, \dots, b_n$  não são todos iguais a zero.

Multipliquando (29) por potências de  $z$  de forma a  $R, S$  e  $T$  serem polinómios homogéneos em  $x, y$  e  $z$  ou polinómios zero, obtemos

$$R(b_1L^{k-k_1}Q_1 + \dots + b_1L^{k-k_n}Q_n) = SF + TG,$$

para  $R$  é diferente de zero na origem. Como  $b_1, \dots, b_n$  não são todos iguais a zero, então  $Q_1, \dots, Q_n$  são dependentes em relação a  $F$  e  $G$  na origem através de  $L$ . Seguindo-se a desigualdade  $I_O^L(F, G) \leq I_O(f, g)$ .

### III. Intersecções

Seguindo um raciocínio análogo ao anterior, mas agora tomando dois pontos na recta  $L$ , chegamos à outra desigualdade.  $\square$

O último teorema permitem-nos provar que o valor de  $I_P^L(F, G)$  não depende da recta  $L$ . Assim, vamos definir novamente, de uma forma mais genérica, multiplicidade de intersecção entre duas curvas  $F$  e  $G$  num ponto  $P$ .

#### **Definição 3.34**

Sejam  $F$  e  $G$  polinómios homogéneos em  $x, y$  e  $z$  e seja  $P$  um ponto no plano projectivo complexo. A multiplicidade de intersecção entre  $F$  e  $G$  em  $P$ , representada por  $I_P(F, G)$ , é o valor comum da quantidade  $I_P^L(F, G)$  para toda a recta  $L = 0$  que não contém  $P$ .

Neste momento, recorrendo a esta definição, podemos demonstrar de forma quase imediata as propriedades 3.11 e 3.15. A propriedade 3.11 refere-se à igualdade  $I_O(F, G) = I_O(f, g)$ , onde  $F(x, y, z)$  e  $G(x, y, z)$  são polinómios homogéneos em  $x, y$  e  $z$ ,  $f(x, y) = F(x, y, 1)$  e  $g(x, y) = G(x, y, 1)$ . Pela definição 3.34 temos a igualdade  $I_O(F, G) = I_O^z(F, G)$ , e ainda, pelo teorema 3.31,  $I_O^z(F, G) = I_O(f, g)$ , ou seja, a definição 3.34 e a definição 3.19 dão-nos o mesmo valor da multiplicidade da intersecção para a origem, ficando assim verificada a propriedade 3.11.

A propriedade 3.15 refere-se à igualdade  $I_P(F, G) = I_{P'}(F', G')$ , na qual é definida uma transformação do plano projectivo que envia o ponto  $(x, y, z)$  para o ponto  $(x', y', z')$ , sendo  $P$  um ponto do plano projectivo e  $P'$  a sua imagem, e as curvas  $F'(x', y', z') = 0$  e  $G'(x', y', z') = 0$  as imagens das curvas  $F(x, y, z) = 0$  e  $G(x, y, z) = 0$ , respectivamente, quando sujeitas a essa mesma transformação. Para demonstrar esta propriedade consideremos a recta  $L$  que não contém  $P$  e  $L'$  a transformada de  $L$ . Pelo teorema 3.32, sabemos que  $I_P^L(F, G) = I_{P'}^{L'}(F', G')$  e, pela definição 3.34, temos  $I_P(F, G) = I_{P'}(F', G')$ .



## Capítulo IV | CÚBICAS

As cúbicas são curvas muito complicadas de serem analisadas directamente. Assim, para as classificar, vamos usar mudanças de variáveis de forma a transformar as suas equações noutras mais simples.

Neste capítulo vamos classificar todas as *cúbicas irredutíveis*. De início apenas trabalhamos com cúbicas que têm pontos notáveis, *flexões* ou *pontos singulares*. O facto das curvas terem estes pontos, permite-nos obter informação acerca da sua equação de forma a podermos simplificá-la algebricamente. As cúbicas são curvas dadas por polinómios de grau 3 que, por serem irredutíveis, não são susceptíveis de se decomporem em factores lineares ou de grau 2.

O nosso objectivo é provar que toda a cúbica irredutível pode ser escrita na forma

$$y^2 = x^3 + ax^2 + bx + c,$$

onde  $a$ ,  $b$  e  $c$  são números reais.

Na primeira secção vamos introduzir alguns conceitos intimamente ligados a estas curvas e necessários para atingirmos o nosso objectivo, a saber: pontos singulares, tangentes e flexões.

Na secção 4.2 mostraremos que toda a cúbica  $C$  irredutível que tem uma flexão ou um ponto singular pode ser escrita na forma anterior. Só na secção 4.4 com o estudo das hessianas, matrizes que envolvem as derivadas de segunda ordem do polinómio associado à cúbica, iremos perceber que toda a cúbica irredutível e não singular tem uma flexão. Desta forma, concluímos que toda a cúbica irredutível ou tem uma flexão ou um ponto singular. Assim, juntamente com os resultados obtidos no final da secção 4.2, compreendemos que temos classificadas todas as cúbicas irredutíveis. Necessitamos, no entanto, de alguns teoremas importantes dos quais destacamos o Teorema de Bézout que irá ser tratado na secção 4.3. Nas duas primeiras secções vamos trabalhar com curvas sobre o plano projectivo real. Na terceira secção estendemos o nosso estudo para curvas sobre o plano projectivo complexo, para na quarta secção, voltarmos a trabalhar com curvas sobre os reais. Consoante as nossas necessidades, vamos apresentando ao longo deste capítulo, alguns resultados relativos aos números complexos.

## §4.1 Tangentes, Pontos Singulares e Flexões

Uma recta  $l$  intersecta uma curva  $C$  de grau  $n$  que não a contenha, no máximo,  $n$  vezes, contando as multiplicidades. Quando o valor de  $I_P(l, C)$  é superior a um, dizemos que  $l$  é tangente em relação a  $C$  no ponto  $P$ .

O nosso objectivo é determinar o número de vezes, contando as multiplicidades, que uma recta intersecta uma curva algébrica no plano projectivo. Só assim saberemos se estamos na presença de uma recta que é tangente ou não. Vamos definir os conceitos de tangente e singularidade de uma curva em termos de multiplicidade de intersecções, sendo, para isso, necessário estudarmos uma série de teoremas que nos vão permitir chegar a tais definições. Por fim, definimos *flexão* de uma curva, como sendo uma generalização de um *ponto de inflexão*.

Vamos iniciar esta secção começando por voltar a enunciar o teorema 1.1 mas, agora, tendo presente o conceito de multiplicidade de intersecção.

### Teorema 4.1

*Quaisquer duas rectas do plano projectivo intersectam-se, com multiplicidade 1, no seu ponto de intersecção.*

### Demonstração

Consideremos  $l$  e  $m$  duas rectas e  $P$  o ponto de intersecção (teorema 1.1). Consideremos ainda  $Q$  e  $R$ , dois pontos distintos de  $P$ , pertencentes à recta  $l$  e  $m$ , respectivamente.

Pelo teorema 3.14, existe uma transformação que envia o ponto  $P$  para a origem, o ponto  $Q$  para o eixo das abcissas ( $y = 0$ ) e  $R$  para o eixo das ordenadas ( $x = 0$ ). Assim, a recta  $l$  é transformada na recta  $y = 0$ , e a recta  $m$  na recta  $x = 0$ . Pela propriedade 3.11 e o teorema 3.15, temos  $I_P(l, m) = I_O(x, y) = 1$ .  $\square$

Com o teorema 3.10 determinamos o número de vezes que uma curva  $y = f(x)$  intersecta uma outra curva  $g(x, y) = 0$  na origem, quando a segunda não contém a primeira. Agora, o que pretendemos é determinar, no plano euclidiano, o número de vezes que estas duas curvas se intersectam num ponto  $(a, f(a))$ , onde  $y = f(x)$ . Para isso, vamos transladar o ponto  $(a, f(a))$  para a origem e aplicar o teorema 3.10.

#### IV. Cúbicas

##### **Teorema 4.2**

Sejam  $y = f(x)$  e  $g(x, y) = 0$  duas curvas e  $a \in \mathbb{R}$ . Se

$$g(x, f(x)) = (x - a)^s h(x), \quad (1)$$

para algum inteiro  $s \geq 0$  e algum polinómio  $h(x)$  tal que  $h(a) \neq 0$ , então  $s$  representa o número de vezes que  $y = f(x)$  e  $g(x, y) = 0$  se intersectam no ponto  $(a, f(a))$ .

##### **Observação**

Chamamos ao factor  $(x - a)^s$  um factor repetido quando  $s$  é um inteiro maior que 1.

##### **Demonstração**

Pelo teorema 3.17 (ii) sabemos que

$$I_{(a, f(a))}(y - f(x), g(x, y)) = I_{(0,0)}(y + f(a) - f(x + a), g(x + a, y + f(a))).$$

Como  $y + f(a) - f(x + a) = y - [f(x + a) - f(a)]$ , vamos substituir  $y$  por  $f(x + a) - f(a)$  na segunda curva de forma a obtemos  $g(x + a, f(x + a))$ . Este é um polinómio diferente do polinómio zero, pois resulta do polinómio  $g(x, f(x))$  quando substituímos  $x - a$  por  $x$ , e como  $h(a) \neq 0$  por (1), temos  $g(x, f(x)) \neq 0$ . Assim, pelo teorema 3.8 (ii),  $y + f(a) - f(x + a)$  não é factor de  $g(x + a, y + f(a))$ . Sabemos também que a curva  $y + f(a) - f(x + a) = 0$  contém a origem. Estão, assim, reunidas as condições necessárias de aplicabilidade do teorema 3.10, donde concluímos que

$$I_{(0,0)}(y + f(a) - f(x + a), g(x + a, y + f(a)))$$

é igual ao menor grau de todos os termos diferente de zero de  $g(x + a, f(x + a))$ . Como  $g(x + a, f(x + a)) = x^s k(x)$ , onde  $k(x) = h(x + a)$  é um polinómio tal que  $k(0) = h(a) \neq 0$ , então  $y = f(x)$  e  $g(x, y) = 0$  intersectam-se  $s$  vezes no ponto  $(a, f(a))$ .  $\square$

O teorema seguinte dá-nos uma generalização do teorema anterior para os vários pontos  $(a_i, f(a_i))$  sendo  $a_i$  um número real.

##### **Teorema 4.3**

Sejam  $y = f(x)$  e  $g(x, y) = 0$  curvas do plano euclidiano. Se  $y - f(x)$  não é factor de  $g(x, y)$ , podemos escrever

$$g(x, f(x)) = (x - a_1)^{s_1} \dots (x - a_n)^{s_n} r(x),$$

#### IV. Cúbicas

onde  $a_i \in \mathbb{R}$  em que  $a_i \neq a_j$  para  $i \neq j$ ,  $s_i$  é um número inteiro, e  $r(x)$  representa um polinómio sem raízes reais. Então  $y = f(x)$  e  $g(x, y) = 0$  intersectam-se  $s_i$  vezes no ponto  $(a_i, f(a_i))$  para  $i = 1, \dots, v$ , sendo estes os únicos pontos de intersecção do plano euclidiano.

##### Demonstração

Como  $y - f(x)$  não é factor de  $g(x, y)$ , pelo teorema 3.8 (ii),  $g(x, f(x))$  não é o polinómio zero. Factorizado este polinómio, sabemos que o número de factores, contando as multiplicidades, é igual ao grau do polinómio  $g(x, f(x))$  menos o grau do polinómio  $r(x)$  [note-se que  $r(x)$  não tem factores lineares, pois não tem raízes reais]. Consideremos então  $g(x, f(x)) = (x - a_1)^{s_1} \dots (x - a_v)^{s_v} r(x)$ .

Ora, pressupondo que  $a_i \neq a_j$  para  $i \neq j$ , então  $g(x, f(x)) = (x - a_i)^{s_i} h(x)$ , onde  $h(a_i) \neq 0$ . Pelo teorema anterior concluímos que  $s_i$  é o número de vezes que  $y = f(x)$  e  $g(x, y) = 0$  se intersectam no ponto  $(a_i, f(a_i))$ .

Se tivermos um outro número real  $a$  diferente de todos os  $a_i$ , então  $g(a, f(a)) \neq 0$ , logo a curva  $g(x, y) = 0$  não contém o ponto  $(a, f(a))$ , ou seja, não intersecta  $y = f(x)$  nesse ponto. Assim, a intersecção nesse ponto é vazia.  $\square$

Quando temos uma curva do tipo  $y = f(x)$  e uma outra  $g(x, y) = 0$  que não contenha a primeira, o teorema 4.3 permite-nos obter todas as multiplicidades de intersecções de todos os pontos do plano euclidiano.

No plano euclidiano ou no plano projectivo, se  $d$  é a soma das múltiplas intersecções de duas curvas em todos os pontos, dizemos que *as duas curvas intersectam-se  $d$  vezes, contando as multiplicidades*.

Consideremos agora uma curva  $g(x, y) = 0$  de grau  $n$  e uma recta não vertical  $y = mx + b$  que não esteja contida na curva. Então o grau de  $g(x, mx + b) = 0$  é, no máximo,  $n$ . Pelo teorema 4.3 sabemos que esta recta intersecta a curva no máximo  $n$  vezes, contando a multiplicidade, no plano euclidiano. Com o teorema 4.5 estendemos este resultado para o plano projectivo. Vamos estudar inicialmente o caso particular em que a recta é o eixo das abcissas. Este resultado é-nos dado pelo teorema 4.4.

#### IV. Cúbicas

##### Teorema 4.4

Seja  $G(x, y, z)$  um polinómio homogéneo de grau  $n$  que não tem  $y$  como factor. Se tomarmos  $g(x, y) = G(x, y, 1)$ , podemos escrever

$$g(x, 0) = (x - a_1)^{s_1} \dots (x - a_v)^{s_v} r(x), \quad (2)$$

para números reais  $a_i$  distintos, inteiros positivos  $s_i$ , e um polinómio  $r(x)$  que não tem raízes reais. Então o número de vezes, contando as multiplicidades, que a curva  $G = 0$  intersecta o eixo das abcissas,  $y = 0$ , no plano projectivo é igual à diferença entre o grau  $n$  de  $G$  e o grau de  $r(x)$ .

##### Demonstração

Seja  $G$  é um polinómio homogéneo de grau  $n$ , então escrevemos

$$G(x, y, z) = \sum e_{ij} x^i y^j z^{n-i-j}.$$

Os termos que não têm  $y$ , ou seja, com  $j = 0$  são da forma  $e_{i0} x^i z^{n-i}$  e, pelo menos, um dos coeficientes  $e_{i0}$  é diferente de zero pois  $y$  não é factor de  $G$ . O termo correspondente  $e_{i0}$  em

$$g(x, y) = G(x, y, 1) = \sum e_{ij} x^i y^j \quad (3)$$

é diferente de zero, e portanto  $y$  não é factor de  $g(x, y)$ . Pelo teorema 4.3 podemos decompor  $g(x, 0)$  como em (2), e o número de vezes, contando a multiplicidade das intersecções de  $g(x, y)$  com o eixo das abcissas no plano euclidiano é  $s_1 + \dots + s_v$ . Sendo este também o número de vezes, contando as multiplicidades, que  $G(x, y, z) = 0$  intersecta  $y = 0$  no plano euclidiano, pelo teorema 3.17 (iii). A equação (2) mostra que  $s_1 + \dots + s_v$  é igual à diferença entre o grau de  $g(x, 0)$  e o grau de  $r(x)$ . Tomando  $y = 0$  em (3), temos

$$g(x, 0) = \sum e_{i0} x^i,$$

que consiste na soma dos termos em (3) que não contêm  $y$ . Assim, o grau de  $g(x, 0)$  é o maior inteiro  $d$  tal que  $e_{d0} \neq 0$ . Tal inteiro existe, porque nem todos os  $e_{d0}$  são iguais a zero. Desta forma, o número de vezes, contando as multiplicidades, que  $G = 0$  e  $y = 0$  se intersectam no plano euclidiano, é igual à diferença entre o grau de  $g(x, 0)$  e o grau de  $r(x)$ .

Surge então a questão: quantas vezes  $G = 0$  e  $y = 0$  se intersectam no infinito? Pelo teorema 3.16 (iii) e pelo facto de o único ponto no infinito da recta  $y = 0$  ser o ponto  $(1, 0, 0)$ , este vai ser o único candidato natural a ponto de intersecção. Alternando as coordenadas  $x$  e  $z$

#### IV. Cúbicas

concluimos que o número de vezes que  $G(x, y, z) = 0$  e  $y = 0$  se intersectam no ponto  $(1, 0, 0)$  é igual ao número de vezes que  $G(z, y, x) = 0$  e  $y = 0$  se intersectam no ponto  $(0, 0, 1)$ , pelo teorema 3.15. Tomando  $z = 1$  determinamos, através da propriedade 3.11, o número de vezes que as curvas  $G(1, y, x) = 0$  e  $y = 0$  se intersectam na origem, no plano euclidiano. Ora, substituindo  $x$  por 1 e  $z$  por  $x$ , obtemos

$$G(1, y, x) = \sum e_{ij} x^{n-i-j} y^j.$$

Como pelo menos um dos termos  $e_{i0} x^{n-i}$  tem coeficiente diferente de zero,  $y$  não é factor de  $G(1, y, x)$ . Assim, pelo teorema 3.10, o número de vezes que  $G(1, y, x) = 0$  e  $y = 0$  se intersectam na origem é o menor grau dos termos diferentes de zero de  $G(1, 0, x) = \sum e_{i0} x^{n-i}$ .

Este é  $n - d$ , porque  $n - i$  decresce à medida que  $i$  cresce e  $d$  é o maior inteiro tal que  $e_{d0} \neq 0$ .

Resumindo,  $G(x, y, z) = 0$  e  $y = 0$  intersectam-se  $n - d$  vezes, contando as multiplicidades, no infinito.

Somando o número de intersecções no plano euclidiano e no infinito, temos o número total de intersecções, contando as multiplicidades, no plano projectivo de  $G = 0$  e  $y = 0$ . Assim, o número de intersecções no plano euclidiano, é igual à diferença entre  $d$  e o grau de  $r(x)$ . No infinito, este número, é  $n - d$ . Deste modo, a soma de ambas as quantidades, é igual à diferença entre  $n$  e o grau de  $r(x)$ .  $\square$

Obs: Os teoremas 4.3 e 4.4, quando estendidos aos números complexos apresentam, pelo TFA (Teorema Fundamental da Álgebra),  $r(x)$  igual a uma constante. Como  $r(x)$  tem grau zero, o teorema 4.4 estendido aos números complexos enuncia-se da seguinte forma "*Um polinómio homogéneo  $G(x, y, z)$  de grau  $n$  que não tem  $y$  como factor, intersecta o eixo das abcissas,  $y = 0$ , exactamente  $n$  vezes contando as multiplicidades, no plano projectivo complexo.*"

Vamos agora supor que temos uma transformação que aplica o ponto  $(x, y, z)$  no ponto  $(x', y', z')$  e os polinómios homogéneos  $F(x, y, z)$  e  $G(x, y, z)$  nos polinómios  $F'(x', y', z')$  e  $G'(x', y', z')$ , respectivamente. Então  $F(x, y, z)$  é factor de  $G(x, y, z)$  se e só se  $F'(x', y', z')$  é factor de  $G'(x', y', z')$ . Esta afirmação é verdadeira porque toda a transformação admite inversa. Se partirmos da hipótese de que  $F'$  é factor de  $G'$ , ou seja,

$$G'(x', y', z') = F'(x', y', z')H'(x', y', z'),$$

#### IV. Cúbicas

e aplicarmos a transformação inversa, obtemos a seguinte igualdade

$$G(x, y, z) = F(x, y, z)H(x, y, z),$$

ou seja, também  $F$  é factor de  $G$ . As transformações preservam assim a irredutibilidade.

#### Teorema 4.5

*Sejam  $L = 0$  uma recta e  $G = 0$  uma curva de grau  $n$ . Se  $L$  não é factor de  $G$ , então  $L$  e  $G$  intersectam-se no máximo  $n$  vezes, contando as multiplicidades, no plano projectivo.*

#### Demonstração

Pelo teorema 3.14, existe uma transformação que envia a recta  $L$  para o eixo das abcissas. Esta transforma a recta  $G$  na recta  $G'$ . Pela explicação que antecede este teorema,  $y$  não é factor de  $G'$ . Pelo teorema 4.4  $y = 0$  intersecta  $G' = 0$  no máximo  $n$  vezes no plano projectivo, contando as multiplicidades. Como as transformações preservam a multiplicidade de intersecção, temos o resultado pretendido.  $\square$

Assim, uma recta intersecta uma curva de grau  $n$  no máximo  $n$  vezes, contando as multiplicidades, no plano projectivo. É necessário, para isso, que a recta não seja um factor da curva, pois, caso fosse, elas intersectar-se-iam infinitas vezes.

É chegado o momento de analisarmos com mais pormenor o número de vezes que uma recta e uma curva se intersectam num ponto. Começemos pela origem.

#### Teorema 4.6

*Consideremos no plano euclidiano uma recta  $l$  que contém a origem e uma curva  $g(x, y) = 0$  que passa na origem mas não contém  $l$ . Como  $g(x, y) = 0$  passa na origem, então  $g(x, y)$  pode ser definido*

$$g(x, y) = sx + ty + h(x, y),$$

onde  $h(x, y)$  é um polinómio em que todos os termos têm grau maior ou igual a dois. Então  $l$  e  $g$  intersectam-se na origem pelo menos duas vezes se e só se ocorrer uma das duas situações seguintes:

(i)  $s = t = 0$ : neste caso toda a recta que passa na origem intersecta  $g$  pelo menos duas vezes na origem;

#### IV. Cúbicas

(ii)  $s$  e  $t$  não são ambos iguais a zero: neste caso  $sx + ty = 0$  é a única recta que intersecta  $g$  mais do que uma vez na origem. Todas as outras rectas que passam na origem intersectam  $g$  nesse ponto exactamente uma vez.

#### Demonstração

Comecemos por demonstrar este resultado para rectas do tipo  $y = mx$  e, posteriormente, para a recta  $x = 0$ .

Consideremos uma curva  $g(x, y) = 0$  que contém a origem, onde

$$g(x, y) = sx + ty + h(x, y),$$

sendo  $h(x, y)$  um polinómio de grau maior ou igual a dois. Esta curva não tem termo constante, pois contém a origem. Consideremos também a recta  $y = mx$ . Como  $g(x, mx)$  é diferente de zero, a multiplicidade das intersecções vai ser dada pelo menor grau de todos os termos diferentes de zero de  $g(x, mx)$  (teorema 3.10), onde

$$g(x, mx) = sx + tmx + h(x, mx).$$

Se  $g(x, mx) = 0$ , a multiplicidade é infinita e  $y = mx$  é factor de  $g(x, y) = 0$  [teoremas 3.6 e 3.8(ii)].

Ora, a multiplicidade é pelo menos dois se e só se  $s + mt = 0$ . Para isso temos duas hipóteses a considerar:

- (i)  $s = t = 0$
- (ii)  $t \neq 0$  ou  $s \neq 0$ .

Estudemos estes dois casos.

(i) Quando  $s = t = 0$ , independentemente da recta do tipo  $y = mx$  a considerar, esta intersecta  $g$  na origem pelo menos duas vezes.

(ii) Quando  $t \neq 0$  e tendo  $y = mx$  e  $sx + ty = 0$  obtemos  $s = -tm$ . Assim,

$$sx + ty = 0 \Leftrightarrow -tmx + ty = 0 \Leftrightarrow y - mx = 0 \Leftrightarrow y = mx.$$

Logo, para  $t \neq 0$ , as rectas  $sx + ty = 0$  e  $y = mx$  são a mesma, e esta é a única que intersecta  $g(x, y)$  na origem mais do que uma vez.

Analogamente se mostra, para  $s \neq 0$ , que  $s = -tm$ , permitindo-nos tirar as mesmas conclusões.

Caso  $s + mt \neq 0$ , ou seja todas as outras rectas que passam na origem, intersectam  $g(x, y)$  na origem apenas uma vez.

#### IV. Cúbicas

Vejamos agora o caso em que a recta  $l$  é  $x = 0$ . Neste caso aplicamos a transformação que troca as coordenadas  $x$  e  $y$ , em que a recta  $x = 0$  é transformada na recta  $y = 0$ , que é do tipo anterior  $y = mx$  (com  $m = 0$ ). Como as transformações preservam a multiplicidade das intersecções, temos o resultado pretendido.  $\square$

O teorema 4.6 pode ser generalizado para um ponto  $P$  qualquer que não a origem no plano projectivo, isto porque, existe uma transformação que envia o ponto  $P$  para a origem preservando a multiplicidade de intersecções. Assim, seja  $P$  definido por  $(a, b)$ , um ponto que pertence à curva  $g(x, y) = 0$  no plano euclidiano em que

$$g(x, y) = s(x - a) + t(y - b) + \sum e_{ij}(x - a)^i(y - b)^j,$$

onde  $i + j \geq 2$  para todo o termo da soma, onde  $s$  e  $t$  não são ambos iguais a zero. Então se a recta

$$s(x - a) + t(y - b) = 0,$$

for a única que intersecta  $g$  mais do que uma vez no ponto  $(a, b)$ , dizemos que é *tangente a  $g$  no ponto  $(a, b)$*  conforme iremos ver na definição seguinte.

#### **Definição 4.7**

Seja  $P$  um ponto de uma curva  $G(x, y, z) = 0$  do plano projectivo.

A curva  $G$  diz-se *singular* em  $P$  se toda a recta que passa por  $P$  intersecta  $G$  pelo menos duas vezes.

A curva  $G$  diz-se *não singular* se existe uma única recta que intersecta  $G$  mais do que uma vez em  $P$ , a que denominamos de *tangente a  $P$* . Todas as outras rectas que passam por  $P$  intersectam  $G$  exactamente uma vez nesse ponto.

Pela definição 4.7 uma curva não tem tangente num ponto singular. Este é um ponto onde a curva tem uma estrutura complicada. Se considerarmos a curva

$$x^4 + 2x^2y^2 + y^4 - x^2 + y^2 = 0,$$

esta tem um ponto singular na origem porque não existem termos de grau menor a 2. Outro exemplo de um ponto singular é a origem da curva  $x^3 = y^2$  (Fig. 18 A). A este tipo de singularidade denominamos *cúspide*. Temos outros exemplos de pontos singulares tais como a origem das curvas  $x^3 + x^2 = y^2$  (Fig. 19 B) e  $x^3 - x^2 = y^2$  (Fig. 18 C), encontrando-se nesta

#### IV. Cúbicas

última isolado. Ao ponto singular, apresentado Fig. 18 B, denominamos *nó*. Nestes pontos é possível definimos uma infinidade de rectas distintas cuja multiplicidade de intersecção é superior a um. Visto o estudo das singularidades<sup>14</sup> sair do âmbito do presente trabalho, ficam apenas alguns registos deste assunto.

Como exemplo de um ponto não singular temos a origem da curva  $y = x^2$ , que tem aí uma recta tangente ( $y = 0$ ), enquanto que todas as outras rectas do tipo  $y = mx$  ( $m \neq 0$ ), intersectam a curva neste ponto uma única vez. Neste caso, a curva diz-se não singular e a recta  $y = 0$  é a tangente no ponto  $(0, 0)$ .

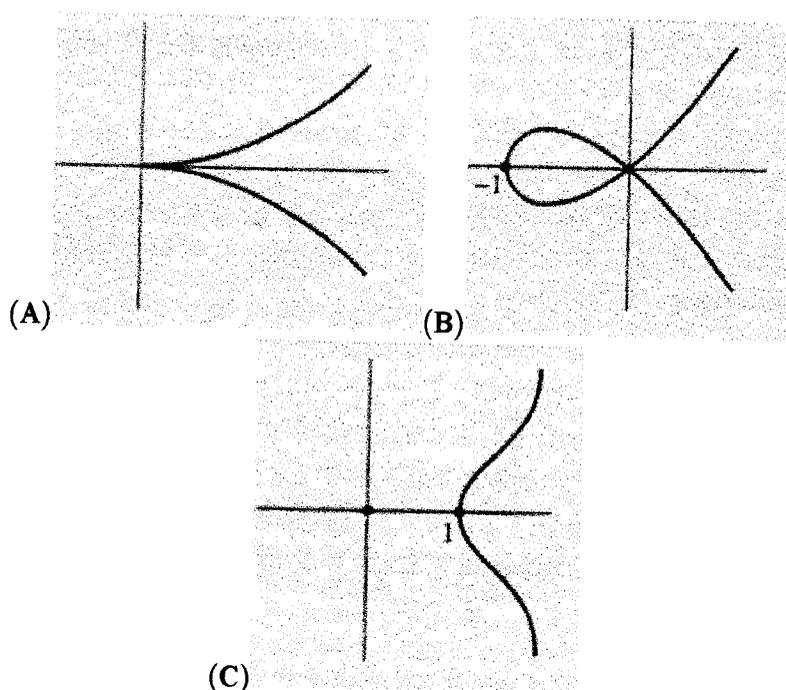


Fig. 18 Curva (A):  $y^2 = x^3$ ; Curva (B):  $y^2 = x^3 + x^2$ ;  
Curva (C):  $y^2 = x^3 - x^2$ .

Como já referimos as transformações preservam a multiplicidade de intersecções. Assim, quando temos uma tangente a uma curva  $C$  num ponto  $P$ , e se os transformarmos na curva  $C'$  e no ponto  $P'$ , a condição de tangência mantém-se. A transformação envia a tangente a  $C$  no ponto  $P$  para a tangente a  $C'$  no ponto  $P'$ . Também  $C$  é não singular em  $P$  se e só se  $C'$  for não singular em  $P'$ .

<sup>14</sup> V. Eduardo Casas-Alvero, *Singularities of Plane Curves*, London Mathematical Society Lecture Notes Series 276, Cambridge University Press, 2000, pp.12–13.

Até agora vimos que a tangente a uma curva  $C$  num ponto  $P$  é a única recta  $l$  que intersecta a curva nesse ponto pelo menos duas vezes. Se, no entanto, essa intersecção for superior a dois dizemos que o ponto  $P$  tem uma flexão. Se estivermos a trabalhar no plano euclidiano uma flexão não é mais do que um ponto de inflexão. No entanto, este conceito vai ser generalizado para o plano projectivo e, consequentemente, para pontos no infinito — é a esta generalização de um ponto de inflexão que chamamos flexão.

Uma flexão de uma curva  $C$  é um ponto  $P$  de  $C$ , em que  $C$  é não singular em  $P$ , e  $C$  intersecta a tangente  $l$  em  $P$  pelo menos três vezes, estando incluídos os casos em que  $I_P(C, l) = \infty$ . Desta forma, se  $C$  tem uma flexão em  $P$ , então tem uma tangente nesse ponto.

Vejamos o seguinte exemplo. Consideremos as curvas  $y = x^3$  e  $y = x^2$ , ambas com tangentes  $y = 0$ , na origem. No entanto, o eixo das abcissas intersecta duas vezes a curva  $y = x^2$  e três vezes a curva  $y = x^3$  na origem, portanto temos, respectivamente, uma tangente e uma flexão nesse ponto.

Como as transformações preservam as tangentes e a multiplicidade de intersecções, então preservam as flexões.

## §4.2 Cúbicas irredutíveis

Formalmente, uma cúbica é uma curva que consiste num polinómio de grau 3, que no plano projectivo real e em coordenadas homogéneas, é definida pela seguinte equação

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + iyz^2 + jz^3 = 0, \quad (1)$$

onde  $a, \dots, j$  representam números reais nem todos iguais a zero. A restrição da cúbica ao plano euclidiano é dada pela equação

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

de grau três.

Uma cúbica é *irredutível* quando não pode ser definida como produto de polinómios de graus menores a três. Caso seja possível tal factorização, a cúbica diz-se *reductível*. Uma cúbica em coordenadas homogéneas que é irredutível, não tem  $z$  como factor, logo pelo menos um dos coeficientes  $a, \dots, d$  é diferente de zero, sendo a sua restrição ao plano euclidiano ainda de grau três.

O nosso estudo vai incidir nas cúbicas irredutíveis. Quanto às reductíveis, dependendo da factorização, vão reduzir-se ou a rectas e/ou a cónicas (uma recta e uma cónica ou três rectas).

#### IV. Cúbicas

Como cúbicas irredutíveis podemos definir *a priori* três categorias. Uma referente a cúbicas não singulares e duas referentes a cúbicas singulares. Nestas duas últimas categorias temos pontos singular que designamos ou por *nó* ou por *ponto cúspide*.

Com o estudo das intersecções em pontos específicos destas curvas, podemos obter informação útil que nos poderá ajudar na classificação das cúbicas.

Desta forma, e recorrendo ao teorema 4.6 e definição 4.7, sabemos que uma cúbica no plano euclidiano tem uma tangente  $y = 0$  na origem se e só se tiver equação

$$ay + bx^2 + cxy + dy^2 = ex^3 + fx^2y + gxy^2 + hy^3,$$

para as constantes  $a, \dots, h$ , com  $a \neq 0$ , estando no primeiro membro os termos de ordem 1 e 2, e no segundo os termos de ordem três. Assumindo que  $a = 1$ , mesmo que para isso seja necessário dividir a equação anterior por  $a$ , obtemos assim uma nova equação para novos valores de  $b, c, d, e, f, g$  e  $h$ ,

$$y + bx^2 + cxy + dy^2 = ex^3 + fx^2y + gxy^2 + hy^3. \quad (2)$$

Vamos iniciar esta secção com o estudo de tangentes e flexões em pontos no infinito. Segue-se o estudo das condições de singularidade das cúbicas do tipo  $y^2 = q(x)$ , onde  $q(x)$  é um polinómio de grau três. Por fim, fazemos a caracterização de todas as cúbicas irredutíveis que têm uma flexão ou um ponto singular.

Antes, porém, gostaríamos de fazer uma breve referência a este tipo de curvas de equação  $y^2 = q(x)$ , em que  $q(x) = ax^3 + bx^2 + cx + d$ . Estas cúbicas foram classificadas em 1710 por Newton, sendo conhecidas pela família das "*Parábolas Divergentes*". Newton classificou esta família, de acordo com as raízes do polinómio cúbico  $q(x)$ , em cinco grupos. Assim, definiu dois grupos de cúbicas não singulares, em que  $q(x)$  não tem raízes repetidas, e três grupos de cúbicas singulares onde  $q(x)$  tem raízes repetidas. Por sua vez, dentro do grupo das cúbicas não singulares, o polinómio  $q(x)$  pode ter três raízes reais diferentes (Fig. 19 B) ou uma raiz real e duas complexas (Fig. 19 A). Relativamente ao grupo das cúbicas singulares,  $q(x)$  pode ter duas raízes iguais ou ter as três raízes iguais. No primeiro caso ou temos um *ponto isolado* (Fig. 18 C) ou temos um *ponto duplo ordinário* — *nó* (Fig. 18 B). A cúbica cujo polinómio  $q(x)$  apresenta três raízes iguais é também denominada de *parábola semicubical* e apresenta um ponto cúspide (Fig. 18 A).

Começemos por caracterizar uma cúbica irredutível com uma flexão no infinito pertencente a uma recta vertical, cuja recta tangente nesse ponto é a recta no infinito.

#### IV. Cúbicas

##### Teorema 4.8

(i) Uma cúbica cuja tangente a um ponto no infinito pertencente a uma recta vertical, é a recta no infinito, tem uma flexão nesse ponto e é irredutível se e só se tiver equação

$$y^2 + cxy + dy = ex^3 + fx^2 + gx + h, \quad (3)$$

para números reais  $c, \dots, h$  com  $e \neq 0$ .

(ii) Uma cúbica  $C$  é irredutível e tem uma flexão num ponto  $P$  se e só se existe uma transformação que a transforme em

$$y^2 = x^3 + fx^2 + gx + h, \quad (4)$$

onde  $f, g$  e  $h$  são números reais, e que envia  $P$  para o infinito, para uma recta vertical.

##### Demonstração

(i) Primeiramente, vamos demonstrar este resultado para uma cúbica tangente ao eixo das abcissas na origem. Posteriormente, aplicamos uma transformação que alterna  $y$  com  $z$ , para que possamos transpor estas ideias do plano euclidiano para o infinito.

Seja  $C$  uma cúbica com equação (2) em que a tangente na origem é o eixo das abcissas,  $y = 0$ . Suponhamos  $C$  irredutível e estudemos, mais tarde, tal hipótese. Assim, supondo tal hipótese,  $y$  não é factor de  $C$ , e consequentemente  $b$  e  $e$  não poderão ser ambos iguais a zero. Pelo teorema 3.10 o número de vezes que a cúbica intersecta a recta  $y = 0$ , na origem, vai ser igual ao expoente da menor potência de  $x$  quando substituímos  $y = 0$  em (2). Este expoente é igual a dois se  $b \neq 0$ , ou igual a três se  $b = 0$  e  $e \neq 0$ . Desta forma, uma cúbica irredutível é tangente à recta  $y = 0$  na origem e tem uma flexão nesse ponto, se tiver equação

$$y + cxy + dy^2 = ex^3 + fx^2y + gxy^2 + hy^3,$$

com  $e \neq 0$ .

Em coordenadas homogéneas, uma cúbica irredutível é tangente a  $y = 0$  no ponto  $(0, 0, 1)$  e tem aí uma flexão, se a sua equação for

$$yz^2 + cxyz + dy^2z = ex^3 + fx^2y + gxy^2 + hy^3,$$

para  $e \neq 0$ .

Para trabalharmos estas mesmas ideias mas para pontos no infinito, onde a recta tangente coincide com a recta no infinito, vamos aplicar uma transformação que alterna  $y$  com  $z$ . Esta transformação envia a recta tangente  $y = 0$  para  $z = 0$  (recta no infinito) e o ponto  $(0, 0, 1)$

#### IV. Cúbicas

para o ponto  $(0, 1, 0)$  do infinito pertencente a uma recta vertical. Como as transformações preservam a irreduzibilidade e a multiplicidade de intersecções, verificamos que uma cúbica irreduzível é tangente a  $z = 0$  no ponto  $(0, 1, 0)$  e tem aí uma flexão, se a sua equação for do tipo

$$zy^2 + cxyz + dz^2y = ex^3 + fx^2z + gxz^2 + hz^3,$$

com  $e \neq 0$ . Esta é a equação (3) quando  $z = 1$ .

Falta-nos demonstrar que a cúbica de equação (2) com  $b = 0$ , é irreduzível. Para isso comecemos por mostrar que existe uma transformação que transforma (3) em (4), quando  $e \neq 0$ .

Assim, ao completarmos o quadrado em  $y$  do membro esquerdo de (3), temos

$$y^2 + (cx + d)y + \left(\frac{cx + d}{2}\right)^2 = ex^3 + fx^2 + gx + h + \left(\frac{cx + d}{2}\right)^2,$$

ou seja,

$$\left(y + \frac{c}{2}x + \frac{d}{2}\right)^2 = ex^3 + \left(f + \frac{c^2}{4}\right)x^2 + \left(g + \frac{cd}{2}\right)x + \left(h + \frac{d^2}{4}\right).$$

Aplicando a transformação  $x' = x$ ,  $y' = y + \frac{c}{2}x + \frac{d}{2}$ ,  $z' = z$ , obtemos para novos valores de  $f$ ,  $g$ , e  $h$  a equação

$$y'^2 = ex'^3 + fx'^2 + gx' + h.$$

Aplicando, novamente, uma outra transformação  $x' = \sqrt[3]{ex}$ ,  $y' = y$ ,  $z' = z$  ( $e$  não foi alterado, logo temos a certeza de que  $e \neq 0$ ) obtemos, para novos valores de  $f$ ,  $g$ , e  $h$ , a equação (4), O polinómio correspondente vai ser

$$y'^2 - x'^3 - fx'^2 - gx' - h.$$

Este polinómio é irreduzível, pois, caso contrário, teria uma factorização do tipo  $(y - q(x)) \times (y + q(x))$ , onde o quadrado do polinómio  $q(x)$  teria grau três, o que não é possível. Como as transformações preservam a irreduzibilidade (justificação que antecede o teorema 4.5), logo (3) é irreduzível e consequentemente a cúbica de equação (2) com  $b = 0$  é irreduzível.

(ii) Seja  $C$  uma cúbica irreduzível com uma flexão em  $P$ , cuja recta tangente nesse ponto representaremos por  $l$ . Existe uma transformação  $T$ , que envia  $l$  para a recta no infinito de modo a  $P$  pertencer a uma recta vertical. Consideremos um segundo ponto pertencente à

#### IV. Cúbicas

tangente  $l$ . A transformação  $T$  também vai enviar esse ponto para o infinito. Por (i)  $C$  é transformada na curva de equação (3) com  $e \neq 0$ , que como vimos, pode ser transformada na equação (4).

Reciprocamente, toda a curva que pode ser transformada na curva de equação (4) é irredutível e tem uma flexão (propriedades que são preservadas pelas transformações), sendo (4) um caso especial de (3) em que  $c = d = 0$  e  $e = 1$ .  $\square$

Vamos agora estabelecer a relação existente entre os factores repetidos de uma cúbica de equação (4) e as condições de singularidade dessa curva.

#### **Teorema 4.9**

Seja  $C$  uma cúbica  $y^2 - q(x) = 0$  com  $q(x) = x^3 + fx^2 + gx + h$ .

(i)  $C$  é não singular em todos os pontos do plano euclidiano que não pertencem ao eixo das abcissas e a tangente a  $C$ , em cada um desses pontos, é não vertical.

(ii) Um ponto  $(r, 0)$  do plano euclidiano pertence a  $C$  se e só se  $x - r$  é um factor de  $q(x)$ . Se  $x - r$  é um factor não repetido de  $q(x)$ , então  $C$  é não singular em  $(r, 0)$  e tem uma tangente vertical nesse ponto. Se  $x - r$  é um factor repetido de  $q(x)$ , então  $C$  é singular em  $(r, 0)$ .

(iii) Se um ponto de  $C$  do infinito pertence a uma recta vertical, então  $C$  é não singular nesse ponto e a tangente a  $C$  nesse mesmo ponto é a recta no infinito.

#### **Demonstração**

(i) Seja  $(a, b)$  um ponto do plano euclidiano pertencente a  $C$  que não pertence ao eixo das abcissas ( $b \neq 0$ ). Substituindo  $x = x' + a$  e  $y = y' + b$  em  $y^2 - q(x)$  temos

$$(y' + b)^2 - q(x' + a). \quad (5)$$

Sejam  $s$  e  $2b$  os coeficientes de  $x'$  e  $y'$ , respectivamente. A cúbica  $C$  é não singular em  $(a, b)$  se  $s$  e  $2b$  não são ambos iguais a zero, logo, pela justificação que antecede a definição 4.7, a tangente em  $(a, b)$  é definida por

$$s(x - a) + 2b(y - b) = 0.$$

Como  $b \neq 0$  então  $C$  é não singular em  $(a, b)$ . A tangente a esse ponto vai ser  $y = b$ , quando  $s = 0$ , ou  $y = mx + c$ , onde  $m = -\frac{s}{2b}$  e  $c = \frac{sa}{2b} + b$ , quando  $s \neq 0$ , ou seja a tangente é não vertical.

#### IV. Cúbicas

(ii) Seja  $(r, 0)$  um ponto do plano euclidiano. Este ponto pertence a  $C$  se e só se  $q(r) = 0$ . Pelo teorema 3.9 (ii),  $q(r) = 0$  se  $x - r$  é um factor de  $q(x)$  e neste caso escrevemos, para um polinómio  $h(x)$ ,  $q(x) = (x - r)h(x)$ .

Se tomarmos  $a = r$  e  $b = 0$  em (5) obtemos

$$y'^2 - q(x' + r),$$

ou seja,

$$y'^2 - x'h(x' + r).$$

Depois de simplificada a expressão anterior obtemos  $-h(r)$  e  $0$  como coeficientes de  $x'$  e  $y'$ , respectivamente. Assim, se  $h(r) \neq 0$  então  $C$  é não singular e tem uma tangente vertical em  $(r, 0)$ . Se  $h(r) = 0$ ,  $C$  é singular em  $(r, 0)$ .

Pelo teorema 3.9 (ii),  $h(r) = 0$  se e só se  $x - r$  é um factor de  $h(x)$ , ou seja se e só se  $x - r$  é um factor repetido de  $q(x)$ .

(iii) A curva  $C$  em coordenadas homogéneas é definida por

$$y^2z = x^3 + fx^2z + gxz^2 + hz^3.$$

Tomando  $z = 0$  na equação anterior concluímos que  $x = 0$ , logo  $(0, 1, 0)$  é o único ponto no infinito que pertence a  $C$ .

Pelo teorema 4.8 (i) concluímos que  $C$  tem uma tangente,  $z = 0$ , no ponto  $(0, 1, 0)$ , sendo este um ponto não singular.  $\square$

Se associarmos os resultados obtidos pelos teoremas 4.8 e 4.9, conseguimos uma caracterização das cúbicas irredutíveis não singulares e singulares. Esta caracterização é dada pelos teoremas 4.10 e 4.11.

Antes, porém, necessitamos de rever algumas ideias relativamente ao número de raízes que um polinómio de grau ímpar, mais concretamente de grau três, tem. Consideremos o polinómio  $q(x) = ax^3 + bx^2 + cx + d$ , com  $a > 0$ . Este pode ser escrito na forma  $q(x) = ax^3(1 + \frac{b}{ax} + \frac{c}{ax^2} + \frac{d}{ax^3})$ . Assim temos o  $\lim_{x \rightarrow +\infty} q(x) = +\infty$  e o  $\lim_{x \rightarrow -\infty} q(x) = -\infty$  [note-se que este limite é igual a  $-\infty$  porque o grau do polinómio é ímpar e considerámos  $a > 0$ ]. Como  $y = q(x)$  é uma função contínua, logo não pode passar de um valor positivo para um valor negativo sem passar pelo zero, concluímos que este polinómio tem pelo menos uma raiz. Obviamente que para valores de  $a < 0$  temos o  $\lim_{x \rightarrow +\infty} q(x) = -\infty$  e o

$\lim_{x \rightarrow -\infty} q(x) = +\infty$  e, pelo mesmo motivo, concluímos que o polinómio tem pelo menos uma raiz.

Este resultado é necessário para a demonstração do teorema seguinte.

**Teorema 4.10**

Uma cúbica é não singular e irredutível e tem uma flexão se e só se puder ser transformada em

$$y^2 = x(x^2 + kx + 1) \tag{6}$$

ou

$$y^2 = x(x - 1)(x - w) \tag{7}$$

para  $w > 1$  e  $-2 < k < 2$ .

A Fig. 19 permite-nos tirar algumas ilações relativamente às cúbicas (6) e (7), das quais destacamos apenas as mais importantes. A cúbica (6) tem uma raiz ( $x = 0$ ), enquanto a cúbica (7) tem três raízes ( $x = 0$ ,  $x = 1$  e  $x = w$ ). Estes pontos de intersecção com o eixo das abcissas são pontos não singulares, onde as cúbicas têm tangentes verticais (teorema 4.9).

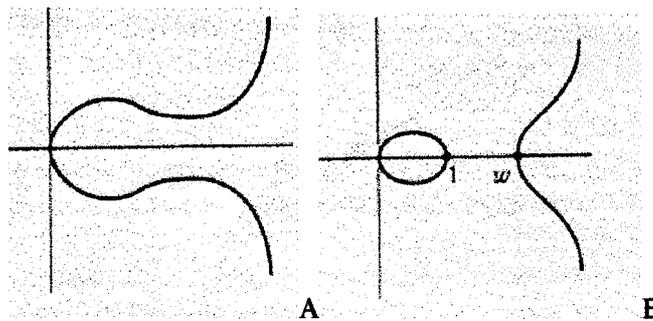


Fig. 19 A. Curva (6):  $y^2 = x(x^2 + kx + 1)$ ;  
 B. Curva (7):  $y^2 = x(x - 1)(x - w)$ .

**Demonstração**

Seja  $C$  uma cúbica não singular e irredutível com uma flexão. Pelo teorema 4.8, a cúbica  $C$  pode ser escrita na forma

$$y^2 = x^3 + fx^2 + gx + h.$$

Como o segundo membro é um polinómio de grau três em  $x$ , tem uma raiz real que designamos por  $r$ . Assim, podemos escrever a curva como sendo

#### IV. Cúbicas

$$y^2 = (x - r)(x^2 + bx + c), \quad (8)$$

com  $b, c \in \mathbb{R}$ .

Dois casos podem ocorrer: (i)  $x^2 + bx + c$  é irredutível e não tem raízes reais; (ii)  $x^2 + bx + c$  é redutível e tem duas raízes reais que designaremos por  $s$  e  $t$ .

(i) Seja  $x^2 + bx + c$  irredutível.

Neste caso, vamos aplicar a transformação  $x' = x - rz$ ,  $y' = y$  e  $z' = z$  de forma a obtermos a equação (6)

$$y^2 = x(x^2 + dx + e),$$

para valores de  $d$  e  $e \in \mathbb{R}$ . Como  $x^2 + dx + e$  é irredutível é necessário que  $d^2 - 4e$  seja negativo e portanto que  $e$  seja positivo. Desta forma, podemos fazer a substituição  $x = \sqrt{e}x'$ ,  $y = \sqrt[4]{e^3}y'$  e  $z = z'$  e obtemos

$$\sqrt{e^3}y^2 = \sqrt{e}x(ex^2 + d\sqrt{e}x + e).$$

Dividindo a equação membro a membro por  $\sqrt{e^3}$ , obtemos  $y^2 = x(x^2 + kx + 1)$ .

(ii) Sejam  $s$  e  $t$  as raízes de  $x^2 + bx + c$ .

Neste caso a equação (8) vem

$$y^2 = (x - r)(x - s)(x - t).$$

Como  $C$  é não singular, pelo teorema 4.9, nenhum destes factores é repetido. Consideremos, sem perda de generalidade, que  $r < s < t$ . Aplicando a transformação  $x' = x - rz$ ,  $y' = y$  e  $z' = z$ , temos

$$y^2 = x(x - u)(x - v),$$

com  $u = s - r$  e  $v = t - r$ , onde  $0 < u < v$ .

Substituindo  $x = ux'$ ,  $y = \sqrt{u^3}y'$  e  $z = z'$ , obtemos

$$u^3y^2 = ux(ux - u)(ux - v),$$

ou seja,

$$y^2 = x(x - 1)(x - w),$$

com  $w = \frac{v}{u} > 1$ .

#### IV. Cúbicas

Reciprocamente, consideremos as equações (6) e (7). Como nenhuma delas tem factores repetidos, então, pelo teorema 4.9 e porque as transformações preservam os pontos singulares, estas curvas não são singulares. Pelo teorema 4.8 (ii), concluímos que as curvas são irredutíveis e têm uma flexão.  $\square$

Depois de caracterizadas todas as cúbicas irredutíveis não singulares que têm uma flexão, é chegado o momento de caracterizarmos todas as cúbicas irredutíveis e singulares.

#### **Teorema 4.11**

*Uma cúbica irredutível é singular se e só puder ser transformada numa das seguintes formas*

$$y^2 = x^3, \quad (9)$$

$$y^2 = x^2(x+1), \quad (10)$$

$$y^2 = x^2(x-1). \quad (11)$$

As curvas (9), (10) e (11) neste último teorema estão representadas na Fig. 18, correspondendo às curvas A, B e C, respectivamente. Analisemos algumas características interessantes que estas três cúbicas possuem. Como todas têm  $x$  como factor repetido, todas são singulares na origem [teorema 4.9 (ii)]. As curvas (10) e (11) cujos gráficos intersectam o eixo das abcissas noutros pontos que não a origem, têm aí uma tangente vertical (teorema 4.9). No caso da cúbica (11) observamos um ponto isolado na origem.

#### **Demonstração**

Consideremos as cúbicas de equações (9), (10) e (11), todas com um ponto singular e portanto singulares. Estes três tipos de cúbicas são irredutíveis, pois, caso contrário, teriam uma factorização do tipo  $(y - q(x)) \times (y + q(x))$ , onde o quadrado do polinómio  $q(x)$  teria grau três, o que não é possível.

Assim, qualquer cúbica que possa ser transformada numa destas três equações é singular e irredutível.

#### IV. Cúbicas

Reciprocamente, seja  $C$  singular e irredutível. Pelo teorema 3.14, podemos enviar o ponto singular para a origem. Pelo teorema 4.6 e definição 4.7,  $C$  pode ser representada pela equação

$$ax^2 + bxy + cy^2 = dx^3 + ex^2y + fxy^2 + gy^3, \quad (12)$$

no plano euclidiano.

Vamos demonstrar, primeiramente, que a equação (12) pode ser transformada numa outra com  $c = 1$ ,  $b = 0$  e  $a = 0, -1, 1$ . Posteriormente, demonstraremos que, dependendo do valor de  $a$ , temos: para  $a = 0$  a equação (9), para  $a = -1$  a equação (10) e para  $a = 1$  a equação (11).

Como as três demonstrações, para  $a = 0$ ,  $a = -1$  e  $a = 1$ , são análogas e muito longas, cuja técnica consiste na manipulação de transformações de forma a eliminar termos ou coeficientes indesejáveis, apenas faremos de forma exhaustiva a primeira demonstração ( $a = 0$ ), que nos permite chegar à equação (9).

Para isso, vamos definir vários casos e estudar cada um deles, de forma a garantir que uma cúbica singular e irredutível representada pela equação (12), tem o coeficiente de  $y^2$  diferente de zero ( $c \neq 0$ ).

(i) Consideremos  $a = b = c = 0$  na equação (12). Porque  $C$  irredutível, não tem  $y$  como factor, logo  $d \neq 0$ . Assim, o polinómio  $dx^3 + ex^2 + fx + g$  tem pelo menos uma raiz real que denominaremos por  $r$ . Desta forma, pelo teorema 3.9 (ii),  $(x - r)$  é um factor do polinómio. e portanto  $(x - ry)$  é um factor de  $C$ , o que é um absurdo pois  $C$  é irredutível.

Assim, concluímos que  $a$ ,  $b$  e  $c$  não são simultaneamente iguais a zero.

(ii) Sejam  $c = 0$ ,  $a \neq 0$  e  $b \neq 0$  em (12). Aplicando uma transformação que alterne o  $x$  com o  $y$  podemos garantir  $c \neq 0$ .

(iii) Se tomarmos  $a = c = 0$  na equação (12) e  $b \neq 0$ . Aplicando a transformação  $x = x' + y'$ ,  $y = y'$  e  $z = z'$ , chegamos a uma outra equação do mesmo tipo, onde o coeficiente do termo  $y^2$  é diferente de zero, ou seja

$$b(x + y)y = d(x + y)^3 + e(x + y)^2y + f(x + y)y^2 + gy^3.$$

Logo

$$by^2 + cxy + ax^2 = dx^3 + ex^2y + fxy^2 + gy^3,$$

para novos valores de  $a-g$  onde  $b \neq 0$ .

Assim, em qualquer dos casos, (ii) ou (iii), podemos garantir que  $c \neq 0$  na equação (12).  $c \neq 0$ . Posteriormente, dividimos a equação anterior membro a membro por  $c$ , e obtemos, para

#### IV. Cúbicas

novos valores de  $a, b, d, e, f$  e  $g$  a equação

$$y^2 + bxy + ax^2 = dx^3 + ex^2y + fxy^2 + gy^3.$$

Completando o quadrado em  $y$ , temos

$$\left(y + \frac{1}{2}bx\right)^2 + \left(a - \frac{1}{4}b^2\right)x^2 = dx^3 + ex^2y + fxy^2 + gy^3.$$

Pretendemos ter  $b = 0$  e  $c = 1$  em (12). Para isso, vamos considerar a transformação  $x' = x, y' = y + \frac{1}{2}bx$  e  $z' = z$ , de forma a obtermos

$$y^2 + ax^2 = dx^3 + ex^2y + fxy^2 + gy^3 \quad (13)$$

para novos valores de  $a, d, e, f$  e  $g$ .

Temos então duas hipóteses a considerar para o valor de  $a$ : ou  $a = 0$  ou  $a \neq 0$ .

Tomemos  $a = 0$ . Como a equação (13) não tem  $y$  como factor então  $d \neq 0$ . Assim, aplicando a transformação  $x' = \sqrt[3]{d}x, y' = y$  e  $z' = z$ , obtemos

$$y^2 = x^3 + ex^2y + fxy^2 + gy^3, \quad (14)$$

para novos valores de  $e, f$  e  $g$ . Tendo como finalidade eliminar o termo  $ex^2y$  de (14), vamos aplicar a transformação

$$x = x' - \frac{e}{3}y', y = y' \text{ e } z = z'.$$

Desta forma, o coeficiente de  $x^2y$  da expressão  $(x - \frac{e}{3}y)^3$  vai ser  $-e$ , ou seja, o simétrico do coeficiente de  $x^2y$  da expressão  $(x - \frac{e}{3}y)^2y$ . Assim, como resultado desta transformação, temos a equação

$$y^2 = x^3 + fxy^2 + gy^3,$$

para novos valores de  $f$  e  $g$ .

A equação homogénea correspondente é

$$y^2z = x^3 + fxy^2 + gy^3,$$

que pode ser escrita da forma

$$y^2(z - fx - gy) = x^3.$$

Por último, aplicando a transformação  $x' = x, y' = y$  e  $z' = z - fx - gy$ , obtemos a curva de equação (9).

Assumindo  $a \neq 0$  em (13) e aplicando a transformação  $x' = |a|^{\frac{1}{2}}x$ ,  $y' = y$  e  $z' = z$ , concluímos que  $a = 1$  ou  $a = -1$ . Quando  $a = -1$ , e através de uma demonstração análoga à anterior, obtemos a equação (10). Tomando  $a = 1$  obtemos a equação (11)<sup>15</sup>.  $\square$

Como as cúbicas de equações (9), (10) e (11) são casos especiais da equação (4) do teorema 4.8 (ii), concluímos que estas cúbicas têm uma flexão no ponto  $(0, 1, 0)$  pertencente a uma recta vertical. Assim, ao considerarmos a homogeneizada da cúbica (9), que representamos por  $y^2z = x^3$ , e aplicarmos a transformação que alterna as coordenadas  $z$  e  $y$ , obtemos a cúbica  $yz^2 = x^3$  onde o ponto de coordenadas  $(0, 1, 0)$  é transformado no ponto de coordenadas  $(0, 0, 1)$ . No plano euclidiano, a curva  $y = x^3$  (Fig. 17) tem uma flexão na origem tal como referimos no final da secção 4.1. Desta forma, este ponto de inflexão na origem mostra que as duas "extremidades" da curva (9) formam uma flexão no infinito.

## §4.3 Teorema de Bézout

Nesta secção vamos apresentar os fundamentos necessários para atingirmos o objectivo a que nos propusemos de início, ou seja, mostrar que toda a cúbica irreduzível e não singular tem uma flexão. Para isso necessitamos de alguns resultados que irão sendo demonstrados, dos quais destacamos o teorema de Bézout. Este teorema, que relaciona a multiplicidade de intersecções entre duas curvas, com o produto dos seus graus, irá ser enunciado primeiramente para curvas complexas e posteriormente para curvas no plano projectivo real. Contudo, para que possamos estabelecer estes desenvolvimentos, necessitamos de trabalhar sobre os números complexos, sendo por isso necessário rever alguns conceitos, nomeadamente o conceito de conjugado relativamente a um polinómio.

Seja  $F = \sum_{i=0}^n a_i x_i$  um polinómio sobre os complexos na indeterminada  $x$ . O polinómio conjugado  $\overline{F}$  é definido do seguinte modo:  $\overline{F} = \sum \overline{a_i} x_i$ , onde  $\overline{a_i}$  representa o conjugado de  $a_i$ . Por sua vez, o conjugado de um número complexo  $Z = c + di$  define-se como sendo  $\overline{Z} = c - di$ .

<sup>15</sup> V. Robert Bix, *Conic and Cubics, A concrete Introduction to Algebraic Curves*, Springer, New York, 1998, pp.140–144.

#### IV. Cúbicas

Exemplo: seja  $F$  um polinómio homogéneo sobre os complexos

$$F(x, y, z) = (4 - i)xy^2 - 3ixyz + 2z^3.$$

Definimos o conjugado deste polinómio, que designaremos por  $\overline{F}$ , como sendo o polinómio

$$\overline{F}(x, y, z) = (4 + i)xy^2 + 3ixyz + 2z^3.$$

O conjugado verifica algumas propriedades que facilmente se demonstram, das quais destacamos as seguintes:

- O conjugado do produto é igual ao produto dos conjugados, ou seja  $\overline{F} \overline{G} = \overline{FG}$ .
- O conjugado da soma é igual à soma dos conjugados, ou seja  $\overline{F} + \overline{G} = \overline{F + G}$ .
- O conjugado de um polinómio com coeficientes reais é igual ao próprio polinómio.
- Se  $w$  e  $z$  são dois números complexos, então  $w = \overline{z}$  se e só se  $\overline{w} = z$ .
- Seja  $F$  um polinómio sobre os complexos e  $\overline{F}$  o seu conjugado então  $F\overline{F} = H$ , onde  $H$  é um polinómio de coeficientes reais.

Iniciamos esta secção com a demonstração de um resultado da álgebra dos polinómios.

#### **Teorema 4.12**

*Sejam  $F$ ,  $G$  e  $H$  polinómios homogéneos sobre o corpo dos complexos tais que  $H$  não contém  $y$  e não contém factores de grau positivo em comum com  $G$ . Então todo o factor de grau positivo comum a  $HF$  e  $G$  é também factor de  $F$ .*

#### **Demonstração**

Consideremos  $R$  um factor de grau positivo comum a  $HF$  e  $G$ . Assim, existe um polinómio homogéneo  $S$  tal que  $HF = RS$ . Dependendo do grau de  $H$  temos três situações a considerar:

(i)  $H$  é um polinómio de grau zero, representado por uma constante  $c$  diferente de zero. Neste caso escrevemos  $F = c^{-1}RS$  e, assim sendo,  $R$  é também factor de  $F$ .

(ii)  $H$  é um polinómio de grau um, ou seja,  $H = 0$  representa uma recta. Como as transformações preservam a factorização, podemos aplicar uma transformação de modo a termos  $H = x$ .

Por hipótese,  $H$  não tem nenhum factor de grau positivo em comum com  $G$ , logo  $x$  não é factor de  $R$ . Contudo, para que seja válida a igualdade  $HF = RS$  é necessário que  $x$  seja

#### IV. Cúbicas

factor de  $S$ . Deste modo, existe um polinómio homogéneo  $T$  tal que  $xT = S$ . Temos então  $xF = xRT$ , ou seja  $F = RT$  (lei do corte). Assim,  $R$  é factor de  $F$ .

(iii)  $H$  é um polinómio de grau  $m$  superior a um. Como  $H$  é um polinómio homogéneo que não contém  $y$ , pode ser visto como um polinómio de duas variáveis  $H(x, z)$ . Pelo Teorema Fundamental da Álgebra, podemos escrever

$$H(x, z) = r(x - w_1z)^{s_1} \cdots (x - w_kz)^{s_k} z^t,$$

para certo inteiro  $t > 0$ . Sabemos que  $H$  tem grau positivo sobre os números complexos, logo podemos associar  $r$  a um dos factores e escrevê-lo como produto de factores lineares, ou seja  $H = L_1 \cdots L_m$ , onde  $L_i$  representa uma recta para  $i = 1, \dots, m$ , não sendo necessário que estas recta sejam distintas. Desta forma, e pela explicação anterior, consideremos  $H = L_1 H'$ , onde  $L_1$  é uma recta e  $H'$  um polinómio homogéneo de grau  $m - 1$ . Como  $H$  não tem factores de grau positivo em comum com  $G$ , também  $L_1$  e  $H'$  não têm. Assim,  $R$  é um factor comum a  $H'F = L_1 H'F$  e  $G$  e é, por (ii), um factor comum a  $H'F$  e  $G$ . Considerando  $H'F = L_2 H''F$  e procedendo ao mesmo tipo de raciocínio, vamos reduzindo o grau de  $H$  até que este desapareça, obtendo-se  $R$  como factor de  $F$ .  $\square$

Definimos  $I(F, G)$  como sendo o número total de vezes, contando as multiplicidades, que duas curvas complexas  $F$  e  $G$  se intersectam em todos os pontos do plano projectivo complexo. Tendo presente esta definição e somando todas as intersecções de todos os pontos, podemos generalizar o Teorema 3.16 (iv) e (v) do capítulo 3 para todos os pontos  $P$  do plano projectivo complexo. Assim temos:

$$I(F, G) = I(F, G + FH) \tag{15}$$

$$I(F, GH) = I(F, G) + I(F, H), \tag{16}$$

onde  $G + FH$  é ainda um polinómio homogéneo.

Neste momento, podemos demonstrar o Teorema de Bézout para curvas que verifiquem certas condições. Pelo Teorema 4.5 e pela observação que o precede, podemos concluir que dada uma recta  $L$  e uma curva  $G$  de grau  $n$ , em que  $L$  não é factor de  $G$ ,  $L$  e  $G$  intersectam-se  $n$  vezes no plano projectivo complexo, contando as multiplicidades.

Se no plano projectivo complexo tivermos uma curva  $F$  de grau  $m$  que não contém  $y$  e não tenha factores de grau positivo em comum com a curva  $G$  de grau  $n$ , podemos escrever

$F(x, z) = L_1 \cdots L_m$ . Neste caso temos:

$$\begin{aligned} I(F, G) &= I(L_1 \cdots L_m, G) \\ &= I(L_1, G) + \cdots + I(L_m, G) \quad [\text{por (16)}] \\ &= mn, \end{aligned}$$

verificando-se o Teorema de Bézout.

Resumidamente, concluímos que dadas duas curvas  $F = 0$  e  $G = 0$  de graus  $m$  e  $n$ , respectivamente, em que  $F = 0$  não contém  $y$  e não tem factores comuns de grau positivo com  $G = 0$ , elas intersectam-se  $mn$  vezes, contando as multiplicidades, no plano projectivo complexo.

Até agora temos trabalhado com curvas em que uma delas não contém  $y$ . Surge então uma questão. Se quisermos maior generalização e considerarmos uma curva que contém  $y$ , como se demonstrará o Teorema de Bézout?

Suponhamos que o grau em  $y$  num polinómio homogéneo  $F$  é superior a zero. Neste caso provamos o Teorema de Bézout através da redução sucessiva do grau de  $y$ , recorrendo a uma técnica semelhante à utilizada no exemplo que fecha a secção 3.1, onde se pretende determinar a multiplicidade de intersecções entre duas curvas. O Teorema 3.21 formaliza este procedimento, onde o grau de uma das curvas complexas  $F$  ou  $G$  vai diminuindo. Apesar desta redução do grau, o teorema de Bézout verifica-se para as curvas  $F$  e  $G$  se e só se for verificado para as curvas que vão resultar da técnica referida no teorema 3.21.

Estamos agora nas condições de enunciar e demonstrar o Teorema de Bézout.

#### **Teorema 4.13 (Teorema de Bézout)**

*Sejam  $F = 0$  e  $G = 0$  duas curvas complexas de graus  $m$  e  $n$  tais que  $F$  e  $G$  não têm factores comuns de grau positivo. Então  $F = 0$  e  $G = 0$  intersectam-se exactamente  $mn$  vezes, contando as multiplicidades, no plano projectivo complexo.*

#### **Demonstração**

Sejam  $F = 0$  e  $G = 0$  duas curvas de grau positivo em  $y$ . Aplicamos o teorema 3.21, de forma a reduzir o grau de  $y$  de uma delas. Repetindo este procedimento até uma das curvas ter grau zero em  $y$ , e mediante a explicação que antecede este teorema, concluímos o resultado pretendido.  $\square$

#### IV. Cúbicas

Pelo Teorema de Bézout, dadas duas curvas  $F$  e  $G$  de graus positivos e sem factores comuns, elas intersectam-se finitas vezes no plano projectivo complexo. Caso estas curvas tenham factores comuns então intersectar-se-ão infinitas vezes, sendo por isso  $I(F, G) = \infty$ .

Chegámos ao momento de mostrar que um dado factor sobre os números complexos de um polinómio homogéneo com coeficientes reais, pode dar origem a um factor sobre o corpo dos reais. Este resultado é apresentado no teorema seguinte.

#### **Teorema 4.14**

*Sejam  $F$  um polinómio homogéneo sobre os reais e  $G$  um polinómio homogéneo e irreduzível sobre os complexos.  $G$  é factor de  $F$  sobre os complexos. Então, ou existe um número complexo  $k$ , diferente de zero, tal que  $kG$  tem coeficientes reais, ou  $G\bar{G}$  é um polinómio homogéneo sobre os reais que é factor de  $F$  sobre os números reais.*

#### **Demonstração**

Seja  $G$  um polinómio homogéneo de coeficientes complexos irreduzível e  $a$  um coeficiente de um termo diferente de zero de  $G$ . Construimos o polinómio  $G_1$  com a finalidade de garantirmos que este tem, pelo menos, um termo com coeficiente igual a um. Assim, definimos  $G_1$  como sendo:

$$G_1 = a^{-1}G. \quad (17)$$

Se  $G_1$  tiver todos os coeficientes reais temos o teorema demonstrado, basta, para isso, considerarmos  $k = a^{-1}$ . Caso contrário, existe pelo menos um coeficiente em  $G_1$  que não é real.

Suponhamos essa segunda hipótese e que  $G$  é factor de  $F$ . Então  $G_1$  é factor de  $F$  e escrevemos

$$F = G_1S,$$

para um polinómio homogéneo  $S$  com coeficientes complexos.

Aplicando o conjugado e tendo em conta que o conjugado de um polinómio com coeficientes reais é o próprio polinómio, obtemos

$$F = \overline{G_1S}. \quad (18)$$

Assim,  $I(G_1, F) = I(G_1, \overline{G_1S}) = I(G_1, \overline{G_1}) + I(G_1, \overline{S})$ .

Como  $G_1$  é factor de  $F$ , então  $I(G_1, F) = \infty$ .

#### IV. Cúbicas

Por sua vez  $G_1$  não tem todos os coeficientes reais daí concluímos que  $G_1 \neq \overline{G_1}$ . Logo  $G_1$  e  $G$  não são múltiplos escalares e  $I(G_1, \overline{G_1}) < \infty$ . Assim,  $I(G_1, F) = \infty$  e  $I(G_1, \overline{G_1}) < \infty$  donde se conclui que  $I(G_1, \overline{S}) = \infty$ . Logo, pelo Teorema de Bézout,  $G_1$  e  $\overline{S}$  têm factores de grau positivo comuns.

Temos  $G_1$  irreduzível e factor de  $\overline{S}$ . Assim, existe um polinómio  $T$  sobre os complexos tal que  $\overline{S} = G_1 T$ . Donde, por (18), temos

$$F = G_1 \overline{G_1} T.$$

Conjugando (17) obtemos  $\overline{G_1} = \overline{\alpha^{-1} G}$  e, assim, definimos a seguinte igualdade

$$F = G_1 \overline{G_1} U,$$

onde  $U$  é um polinómio sobre os complexos. Mas  $G_1 \overline{G_1}$  e  $F$  são polinómios de coeficientes reais, consequentemente,  $U$  tem também coeficientes reais. Assim,  $G_1 \overline{G_1}$  é factor de  $F$  sobre os reais.  $\square$

Põe-se agora uma questão. Será que, dadas duas curvas no plano projectivo real que contêm um factor de grau positivo comum sobre os complexos têm, ainda, em comum um factor de grau positivo sobre os números reais? A resposta é afirmativa e é nos dada pelo teorema seguinte.

#### **Teorema 4.15**

*Sejam  $F$  e  $G$  polinómios homogéneos sobre os reais. Se  $F$  e  $G$  têm um factor comum de grau positivo sobre os complexos, então têm um factor comum de grau positivo sobre os reais.*

#### **Demonstração**

Denominemos  $H$  o factor comum a  $F$  e  $G$  de grau positivo e irreduzível sobre os complexos. Se existir um número complexo  $k$  tal que  $kH$  tenha coeficientes reais, então  $kH$  é factor de  $F$  e  $G$  sobre os números complexos, sendo também um factor de  $F$  e  $G$  sobre os números reais. Se tal número não existir, então pelo teorema 4.14,  $H\overline{H}$  é um polinómio homogéneo de coeficientes reais que é factor de  $F$  e  $G$  sobre os números reais.  $\square$

Por fim, o teorema seguinte dá-nos uma restrição do Teorema de Bézout para curvas no plano projectivo real.

**Teorema 4.16**

Sejam  $F = 0$  e  $G = 0$  duas curvas com coeficientes reais de graus  $m$  e  $n$ , sem factores comuns de grau positivo sobre os reais. Então  $F = 0$  e  $G = 0$  intersectam-se no máximo  $mn$  vezes, contando as multiplicidades, no plano projectivo real.

**Demonstração**

Como  $F$  e  $G$  não têm factores comuns de grau positivo sobre os números reais, logo pelo Teorema 4.15 também não têm sobre os números complexos. Pelo teorema de Bézout,  $F = 0$  e  $G = 0$  intersectam-se  $mn$  vezes, contando as multiplicidades, no plano projectivo complexo. Como podem existir pontos, onde estas duas curvas se intersectam, pertencentes ao plano projectivo complexo que não pertencem ao plano projectivo real, logo  $I(F, G)$  é no máximo igual  $mn$ .  $\square$

Resumidamente, dadas duas curvas  $F = 0$  e  $G = 0$  com coeficientes reais de graus  $m$  e  $n$  sem factores comuns, em que um dos pontos de intersecção é um número complexo, elas intersectam-se no plano projectivo real num número de vezes inferior a  $mn$ , contando as multiplicidades. No entanto, se todos os pontos de intersecção forem números reais, intersectam-se  $nm$  vezes. Os teoremas 4.4 e 4.5, referem-se a este resultado, tendo presente o facto de que uma das curvas ser uma recta.

**§4.4 Hessiana**

Tal como referimos anteriormente, nesta secção vamos completar a classificação das cúbicas irredutíveis, demonstrando que toda a cúbica irredutível não singular tem uma flexão. Para isso, vamos definir *hessiana*  $H$  de uma curva  $C$ , que consiste na matriz definida pelas segundas derivadas parciais do polinómio associado a  $C$ . As flexões e os pontos singulares de uma curva  $C$  no plano euclidiano, vão ser os pontos pertencentes a  $C$  que satisfazem a igualdade  $\det H = 0$ , em que  $\det H$  representa o determinante da matriz  $H$  associada ao polinómio homogéneo de  $C$ . Se  $C$  é uma cúbica irredutível e não singular, provamos que o determinante da sua hessiana é também uma cúbica diferente de  $C$  e os pontos que pertencem a  $C$  e que verificam a igualdade  $\det H = 0$ , vão ser apenas as flexões de  $C$ .

O Teorema de Bézout, demonstrado na secção anterior, irá possibilitar a prova de que  $C$  e  $\det H = 0$  intersectam exactamente nove vezes, contando as multiplicidades, sobre os números

#### IV. Cúbicas

complexos e, portanto, pelo menos uma vez sobre os números reais. Os pontos de intersecção existem aos pares de conjugados e nove é um número ímpar, daí a obrigatoriedade de pelo menos um ponto ser real. Desta forma, concluímos que toda a cúbica  $C$  irredutível e não singular, tem uma flexão no plano projectivo real.

Nesta secção, caso não seja explicitada nenhuma outra situação, vamos considerar polinómios e curvas com coeficientes reais.

Comecemos por definir hessiana de uma curva  $C$  cujo polinómio homogéneo associado iremos representar por  $F$ .

##### **Definição 4.17**

Seja  $F(x, y, z) = 0$  a homogeneizada de  $f(x, y) = 0$  em que  $F(x, y, z)$  é um polinómio homogéneo de grau  $d$ . Chamamos *matriz hessiana de  $f$*  à matriz  $2 \times 2$  simétrica definida pelas segundas derivadas parciais de  $f$ :

$$H_f = \begin{pmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{pmatrix}.$$

Obs:  $f_{ji}$  representa a segunda derivada parcial de  $f_j$  em relação a  $i$ , ou seja  $f_{ji} = (f_j)_i$ .

Estamos a trabalhar com polinómios, logo com funções diferenciáveis. Pelo *Teorema de Schwarz*, sabemos que “se  $f$  é um campo escalar, tal que as suas derivadas  $f_x$  e  $f_y$  existem num conjunto aberto  $S$ , e se  $(a, b)$  é um ponto de  $S$  em que ambas as derivadas  $f_{xy}$  e  $f_{yx}$  existem e são contínuas, tem-se  $f_{xy}(a, b) = f_{yx}(a, b)$ ”. Assim as segundas derivadas parciais cruzadas são iguais.

Naturalmente que, se trabalharmos com um polinómio homogéneo de grau  $d$  sobre os reais,  $F(x, y, z) = \sum e_{ij} x^i y^j z^k$ , onde  $i + j + k = d$ , a matriz hessiana de  $F$  é uma matriz  $3 \times 3$  simétrica definida pelas segundas derivadas parciais de  $F$ :

$$H_F = \begin{pmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{pmatrix}.$$

Neste caso, definimos as primeiras derivadas parciais do seguinte modo:

$$F_x = \sum i e_{ij} x^{i-1} y^j z^k, F_y = \sum j e_{ij} x^i y^{j-1} z^k \text{ e } F_z = \sum k e_{ij} x^i y^j z^{k-1}.$$

Cada derivada parcial ou é zero, ou um polinómio homogéneo de grau  $d - 1$ , enquanto que as segundas, vão ser zero ou um polinómio homogéneo de grau  $d - 2$ . Exemplificando alguns

#### IV. Cúbicas

casos de segundas derivadas parciais temos

$$F_{xy} = \sum i j e_{ij} x^{i-1} y^{j-1} z^k \text{ ou } F_{yz} = \sum j k e_{ij} x^i y^{j-1} z^{k-1}.$$

Tal como anteriormente, pelo Teorema de Schwarz, as derivadas parciais cruzadas são iguais, ou seja  $F_{xy} = F_{yx}$ ,  $F_{xz} = F_{zx}$  e  $F_{yz} = F_{zy}$  e, conseqüentemente, a matriz hessiana é simétrica.

Algumas considerações e deduções importantes devem ser feitas antes de prosseguirmos, a saber:

- Definimos as derivadas parciais do polinómio zero, como sendo iguais a zero;
- Num polinómio homogéneo  $F$  com coeficientes reais e de grau  $d$  é válida a igualdade

$$xF_x + yF_y + zF_z = dF; \quad (19)$$

- O determinante da matriz hessiana de grau 3 é dado por:

$$\det H = F_{xx}F_{yy}F_{zz} + 2F_{xy}F_{yz}F_{xz} - F_{xx}F_{yz}^2 - F_{yy}F_{xz}^2 - F_{zz}F_{xy}^2.$$

Devido à simetria da matriz hessiana, o seu determinante mantém-se inalterado quando alternamos o  $z$  com o  $x$  ou com o  $y$ ;

- Existe uma relação entre as derivadas parciais de  $f(x, y)$  e da homogeneizada  $F(x, y, 1)$ . Assim, temos as seguintes igualdades:  $F_x = f_x$ ;  $F_y = f_y$ ;  $F_{xy} = f_{xy}$ ;  $F_{yx} = f_{yx}$ . Vamos demonstrar apenas as igualdades  $F_x = f_x$  e  $F_{xy} = f_{xy}$  no ponto  $(a, b, 1)$ . A demonstração dos restantes casos é análoga a estes dois. Para isso consideremos

$$F_x(x, y, z) = \sum i e_{ij} x^{i-1} y^j z^{d-i-j},$$

$$\begin{aligned} F_x(x, y, 1) &= \sum i e_{ij} x^{i-1} y^j \\ &= f_x(x, y) \end{aligned}$$

Derivando novamente  $F_x(x, y, z)$ , mas agora em ordem a  $y$ , obtemos

$$F_{xy}(x, y, z) = \sum i j e_{ij} x^{i-1} y^{j-1} z^{d-i-j},$$

$$\begin{aligned} F_{xy}(x, y, 1) &= \sum i j e_{ij} x^{i-1} y^{j-1} \\ &= f_{xy}(x, y). \end{aligned}$$

É possível, através da segunda derivada parcial, identificarmos pontos singulares e flexões de uma curva no plano euclidiano. Para isso, necessitamos de encontrar a equação da tangente

#### IV. Cúbicas

a uma curva no ponto  $(a, b)$ , mas agora envolvendo as primeiras derivadas parciais. Na secção 4.1, vimos que no plano euclidiano uma curva  $f(x, y) = 0$  não singular no ponto  $(a, b)$  pode ser escrita na forma:

$$f(x, y) = s(x - a) + t(y - b) + \sum e_{ij}(x - a)^i(y - b)^j, \quad (20)$$

onde  $i + j \geq 2$  para todos os termos do somatório, não sendo  $s$  e  $t$  simultaneamente iguais a zero. Neste caso a equação da tangente no ponto  $(a, b)$  é dada por

$$s(x - a) + t(y - b) = 0.$$

Quando determinamos  $f_x$  obtemos

$$f_x = s + \sum i e_{ij}(x - a)^{i-1}(y - b)^j, \text{ para } (i - 1) + j \geq 1,$$

em que pelo menos um dos expoentes  $i - 1$  ou  $j$  é positivo. No ponto  $(a, b)$  o somatório vai ser igual a zero e conseqüentemente  $f_x(a, b) = s$ . Analogamente, verificamos que  $f_y(a, b) = t$ . Assim, pelo teorema 4.6 e pela explicação que antecede a definição 4.7,  $f$  é uma curva singular em  $(a, b)$  se e só se  $f_x(a, b)$  e  $f_y(a, b)$  não são ambas iguais a zero. No caso de ser não singular, a tangente a  $f$  no ponto  $(a, b)$  é dada pela recta

$$f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0.$$

Definidas as segundas derivadas parciais num determinado ponto, podemos identificar esse ponto com sendo singular ou uma flexão. Para isso segue-se o teorema 4.18.

#### **Teorema 4.18**

*Sejam  $f(x, y)$  uma curva no plano euclidiano e  $(a, b)$  um ponto pertencente a essa curva. Então  $(a, b)$  é uma flexão ou um ponto singular se e só se no ponto  $(a, b)$  temos a igualdade*

$$f_{xx}f_y^2 + f_{yy}f_x^2 - 2f_{xy}f_xf_y = 0 \quad (21)$$

#### **Demonstração**

Seja  $(a, b)$  um ponto singular de  $f$ . As derivadas  $f_x$  e  $f_y$  são ambas iguais a zero e conseqüentemente a equação (21) é satisfeita no ponto  $(a, b)$ . Assim, podemos assumir que  $f$  é não singular em  $(a, b)$  e mostrar que  $(a, b)$  é uma flexão se e só se é válida a igualdade (21) para o ponto  $(a, b)$ .

Consideremos  $(a, b)$  uma flexão de  $f$ . Pela igualdade (20) podemos escrever

#### IV. Cúbicas

$$f(x, y) = s(x - a) + t(y - b) + u(x - a)^2 + v(y - b)^2 + w(x - a)(y - b) + \sum e_{ij}(x - a)^i(y - b)^j, \quad (22)$$

onde  $i + j \geq 3$  para todos os termos do somatório e em que  $s$  e  $t$  não são simultaneamente iguais a zero. A equação da tangente no ponto  $(a, b)$  é dada por  $s(x - a) + t(y - b) = 0$ .

Como (21) é simétrica em relação a  $x$  e  $y$ , podemos, se necessário, alternar  $x$  com  $y$  de forma a garantirmos  $t \neq 0$ . Resolvendo a equação da tangente no ponto  $(a, b)$  em ordem a  $y$ , obtemos  $y(x) = b - \frac{s}{t}(x - a)$ . Substituindo a expressão encontrada para  $y$  na igualdade (22) obtemos

$$f(x, y(x)) = \left[ u + \frac{vs^2}{t^2} - \frac{ws}{t} \right] (x - a)^2 + \sum e_{ij} \left( \frac{-s}{t} \right)^j (x - a)^{i+j}, \quad (23)$$

onde  $i + j \geq 3$  para todos os termos do somatório. Pondo em evidência em (23) o factor  $(x - a)^2$ , concluímos

$$f(x, y(x)) = (x - a)^2 h(x),$$

para  $h(a) = u + \frac{vs^2}{t^2} - \frac{ws}{t}$  [todos os termos do somatório têm o factor  $(x - a)$  com expoente superior a dois]. Se  $h(a) \neq 0$  então, pelo teorema 4.2,  $f(x)$  intersecta a recta tangente no ponto  $(a, b)$  duas vezes, logo não tem uma flexão nesse mesmo ponto. Se  $h(a) = 0$  e o polinómio (23) é diferente de zero, então a maior potência de  $(x - a)$ , que podemos factorizar, tem pelo menos expoente três e  $f$  intersecta a sua tangente no ponto  $(a, b)$  pelo menos três vezes. Por fim, se o polinómio (23) é igual a zero, pelo teorema 3.8 (ii), a tangente no ponto  $(a, b)$  é um factor de  $f$ . Neste caso  $f$  intersecta a sua tangente nesse ponto, infinitas vezes. Assim,  $f$  intersecta a sua tangente pelo menos três vezes no ponto  $(a, b)$  se e só se  $h(a) = 0$ .

Vamos agora considerar  $h(a) = 0$  ou seja  $u + \frac{vs^2}{t^2} - \frac{ws}{t} = 0$ . Multiplicando  $h(a)$  por  $t^2$  obtemos  $t^2 h(a) = ut^2 + vs^2 - wst = 0$ . Derivando (22) em ordem a  $x$  obtemos

$$f_x(x, y) = s + 2u(x - a) + w(y - b) + \sum i e_{ij}(x - a)^{i-1}(y - b)^j.$$

Assim, concluímos  $f_x(a, b) = s$ . Seguindo um raciocínio análogo, obtemos  $f_y(a, b) = t$ . Derivando novamente  $f_x(x, y)$  em ordem a  $x$  e a  $y$ , temos

$$f_{xx}(x, y) = 2u + \sum i(i - 1)e_{ij}(x - a)^{i-2}(y - b)^j \text{ e}$$

$$f_{xy}(x, y) = w + \sum i j e_{ij}(x - a)^{i-1}(y - b)^{j-1}.$$

#### IV. Cúbicas

Como nas igualdades anteriores  $i + j \geq 3$  deduzimos que pelo menos um dos factores  $(x - a)$  ou  $(y - b)$  tem expoente positivo. Substituindo  $x = a$  e  $y = b$  nestas igualdade, temos  $f_{xx}(a, b) = 2u$  e  $f_{xy}(a, b) = w$ . Através de um procedimento análogo e alternando o  $x$  com o  $y$  em (22), obtemos  $f_{yy}(a, b) = 2v$ .

Substituindo novamente estas quantidades na equação  $ut^2 + vs^2 - wst = 0$  temos, para o ponto  $(a, b)$ , a seguinte equação

$$\frac{1}{2}f_{xx}f_y^2 + \frac{1}{2}f_{yy}f_x^2 - f_{xy}f_xf_y = 0.$$

Multiplicando por 2 a equação anterior obtemos (21).

Assim,  $(a, b)$  é uma flexão ou um ponto singular em  $f$  se e só se nesse ponto  $f_{xx}f_y^2 + f_{yy}f_x^2 - 2f_{xy}f_xf_y = 0$ .  $\square$

Vamos agora mostrar que a equação  $\det H = 0$ , em coordenadas homogéneas, é equivalente à equação (21) do teorema 4.18.

#### **Teorema 4.19**

Seja  $P$  um ponto pertencente à curva  $F = 0$  de grau superior a 1 no plano projectivo real. Então  $P$  é uma flexão ou um ponto singular de  $F$  se e só se  $P$  satisfaz a equação  $\det H = 0$ , onde  $H$  é a hessiana de  $F$ .

#### **Demonstração**

Seja  $P$  um ponto pertencente à curva  $F$ . Assumimos que  $P$  tem a última coordenada,  $z$ , diferente de zero, nem que para isso seja necessário aplicar uma transformação que altere esta com a coordenada  $x$  ou  $y$ . Esta transformação, para além de preservar as flexões e os pontos singulares, não altera o valor do determinante de  $H$ . Assim, dividindo as coordenadas do ponto  $P$  por  $z$ , obtemos o ponto de coordenadas  $(a, b, 1)$ .

Vamos agora provar que o ponto  $(a, b, 1)$  é uma flexão ou um ponto singular se e só se  $(a, b, 1)$  satisfaz a equação  $\det H = 0$ .

Assim, temos:

$$\det H_{(a,b,1)} = \begin{vmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{vmatrix}$$

IV. Cúbicas

$$\begin{aligned}
 \det H_{(a,b,1)} &= \begin{vmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ aF_{xx} + bF_{yx} + F_{zx} & aF_{xy} + bF_{yy} + F_{zy} & aF_{xz} + bF_{yz} + F_{zz} \end{vmatrix} \\
 &= \begin{vmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ (d-1)F_x & (d-1)F_y & (d-1)F_z \end{vmatrix} \quad \begin{array}{l} \text{[por (19) e } F_{yz} = F_{zy}, \\ F_{zx} = F_{xz} \text{ e } F_{xy} = F_{yx}] \end{array} \\
 &= \begin{vmatrix} F_{xx} & F_{xy} & aF_{xx} + bF_{xy} + F_{zx} \\ F_{yx} & F_{yy} & aF_{yx} + bF_{yy} + F_{yz} \\ (d-1)F_x & (d-1)F_y & (d-1)(aF_x + bF_y + F_z) \end{vmatrix} \\
 &= \begin{vmatrix} F_{xx} & F_{xy} & (d-1)F_x \\ F_{yx} & F_{yy} & (d-1)F_y \\ (d-1)F_x & (d-1)F_y & (d-1)dF \end{vmatrix} \\
 &= \begin{vmatrix} F_{xx} & F_{xy} & (d-1)F_x \\ F_{yx} & F_{yy} & (d-1)F_y \\ (d-1)F_x & (d-1)F_y & 0 \end{vmatrix} \quad \text{[(a, b, 1) pertence a F].}
 \end{aligned}$$

Concluimos que  $\det H_{(a,b,1)} = (d-1)^2(2F_{xy}F_xF_y - F_{xx}F_y^2 - F_{yy}F_x^2)$ . Nesta expressão não está envolvida a diferenciabilidade em relação a  $z$  podendo, por esse motivo, ser interpretada como o determinante da hessiana relativamente ao plano euclidiano. Considerando  $f(a, b) = F(a, b, 1)$ , as derivadas  $F_x, F_y, F_{xx}, F_{xy}$  e  $F_{yy}$  vão ser iguais às derivadas  $f_x, f_y, f_{xx}, f_{xy}$  e  $f_{yy}$ , respectivamente. Assim,

$$2F_{xy}F_xF_y - F_{xx}F_y^2 - F_{yy}F_x^2 = -(f_{xx}f_y^2 + f_{yy}f_x^2 - 2f_{xy}f_xf_y) = 0,$$

donde, pelo teorema 4.18, concluimos que  $\det H_{(a,b,1)} = 0$  se e só se o ponto  $(a, b, 1)$  é uma flexão ou um ponto singular.  $\square$

Veremos, de seguida, que o  $\det H$  de uma cúbica  $C$  irreduzível e não singular, não é um múltiplo escalar de  $C$  sobre os números reais. Posteriormente, pelo teorema de Bézout e teorema 4.15, concluimos que  $C$  e  $\det H$  intersectam-se nove vezes no plano projectivo complexo.

**Teorema 4.20**

*Sobre os números reais, se  $C = 0$  é uma cúbica irredutível não singular então o determinante da sua hessiana é um polinómio homogéneo de grau 3 que não é múltiplo escalar de  $C$ .*

**Demonstração**

Seja  $C$  uma cúbica irredutível e não singular. Como o grau  $d$  da curva  $C$  é três, cada entrada da matriz é zero ou  $(d - 2)$ . Assim, o  $\det H$  é o polinómio zero ou um polinómio homogéneo de grau  $3(d - 2) = 3$ . Pela explicação anterior e para que o  $\det H$  não seja múltiplo escalar de  $C$ , vamos demonstrar que  $\det H \neq 0$ .

Pelo teorema 4.19 sabemos que, a existir um ponto  $P$  pertencente a  $C$ , não sendo ele uma flexão nem um ponto singular, o  $\det H \neq 0$ . Por hipótese  $C$  é não singular, basta-nos portanto verificar que esse ponto não é uma flexão.

Primeiramente, mostraremos a existência de um ponto no plano projectivo real pertencente a  $C$  para que, posteriormente, possamos verificar que esse ponto não é uma flexão.

Sendo  $C$  uma cúbica não singular e irredutível tem equação do tipo

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + iz^2 + jz^3 = 0.$$

Se  $C$  contém o ponto  $(1, 0, 0)$ , temos o primeiro objectivo atingido. Caso contrário,  $x^3$  tem em  $C$  coeficiente diferente de zero. Tomando por exemplo  $y$  e  $z$  iguais a 1, temos um polinómio  $C(x, 1, 1)$  de grau 3 em  $x$ . Este polinómio tem pelo menos uma raiz  $r$  real. Deste modo a curva  $C$  contém um ponto pertencente ao plano projectivo real.

O segundo objectivo é provar que existe um ponto que não é uma flexão.

Vamos supor que  $C$  tem uma flexão de forma a chegarmos a um absurdo.

Através do teorema 4.10,  $C$  pode ser transformada na equação

$$y^2 = x^3 + fx^2 + gx,$$

onde  $f$  e  $g$  são números reais e  $g \neq 0$ . Pelo teorema 4.8 (ii), o eixo das ordenadas,  $x = 0$ , é tangente a  $C$  na origem e contém o ponto no infinito  $(0, 1, 0)$ . No entanto, o ponto  $(0, 1, 0)$  também pertence a  $C$ . Segue-se, pelo teorema 4.5 e definição 4.7, que  $C$  intersecta a tangente  $x = 0$  na origem no máximo duas vezes, e portanto a origem não é uma flexão.

Temos um ponto pertencente a  $C$  que não é uma flexão nem um ponto singular ( $C$  é não singular) logo, pelo teorema 4.19, concluímos que  $\det H \neq 0$ . Assim, o  $\det H$  e  $C$  são

#### IV. Cúbicas

polinómios homogéneos de grau 3 e  $C$  é irreduzível. Como o  $\det H$  e  $C$  são dois polinómios homogéneos diferentes, de grau três, concluímos que  $\det H$  não é múltiplo escalar de  $C$ .  $\square$

Se aplicarmos o conjugado à equação  $F(a, b, c) = 0$ , obtemos a equação  $\overline{F}(\overline{a}, \overline{b}, \overline{c}) = 0$ . Estas duas equações são equivalentes. Assim,  $P$  pertence a  $F$  se e só se  $\overline{P}$  pertencer a  $\overline{F}$ . Esta é a ideia base da propriedade seguinte, que nos permite afirmar que o conjugado preserva a multiplicidade de intersecções.

#### **Propriedade 4.21**

*Sejam  $F$  e  $G$  duas curvas com coeficientes complexos e  $P$  um ponto pertencente ao plano projectivo complexo. Temos  $I_P(F; G) = I_{\overline{P}}(\overline{F}, \overline{G})$ .*

#### **Demonstração**

Para demonstrarmos esta propriedade, vamos recorrer a alguns teoremas e definições apresentados na secção 3.3, bem como a algumas das propriedades do conjugado que foram apresentadas no início da secção 4.3. A demonstração desta igualdade é feita através de duas desigualdades. Começemos pela desigualdade

$$I_P(F, G) \leq I_{\overline{P}}(\overline{F}, \overline{G}). \quad (24)$$

Para  $I_{\overline{P}}(\overline{F}, \overline{G}) = \infty$  a desigualdade é imediata. Vamos portanto assumir que  $I_{\overline{P}}(\overline{F}, \overline{G})$  é um inteiro não negativo. Seja  $n$  um inteiro maior que  $I_{\overline{P}}(\overline{F}, \overline{G})$ . Consideremos  $n$  polinómios homogéneos em  $x, y$  e  $z$  que representamos por  $Q_1, \dots, Q_n$ , cujos graus são  $k_1, \dots, k_n$ , respectivamente. Seja  $k$  o maior de todos os graus. Seja  $L = 0$  uma recta que não contém  $P$ . Então  $\overline{L} = 0$  é uma recta que não contém  $\overline{P}$ . Ora,  $n$  é maior que  $I_{\overline{P}}(\overline{F}, \overline{G})$ , portanto os polinómios  $\overline{Q}_1, \dots, \overline{Q}_n$  são dependentes em relação a  $\overline{F}$  e  $\overline{G}$  no ponto  $\overline{P}$  através de  $\overline{L}$  (definição 3.30 e 3.34). Assim, pela definição 3.29, existem  $R, S, T$ , polinómios homogéneos em  $x, y$  e  $z$  ou polinómios zero e números complexos  $b_1, \dots, b_n$  tais que a equação

$$R(b_1 \overline{L}^{k-k_1} \overline{Q}_1 + \dots + b_n \overline{L}^{k-k_n} \overline{Q}_n) = S \overline{F} + T \overline{G},$$

é verificada, onde  $R$  não contém  $\overline{P}$  e  $b_1, \dots, b_n$  não são todos iguais a zero. Conjugando ambos os membros da equação anterior, obtemos

$$\overline{R}(b_1 L^{k-k_1} Q_1 + \dots + b_n L^{k-k_n} Q_n) = \overline{S} F + \overline{T} G.$$

#### IV. Cúbicas

Pela explicação que antecede este teorema e porque  $R$  não contém  $\bar{P}$  e, ainda, porque  $b_1, \dots, b_n$  não são todos iguais a zero, então  $\bar{R}$  não contém  $P$  e  $\bar{b}_1, \dots, \bar{b}_n$  não são todos iguais a zero. Donde os polinómios  $Q_1, \dots, Q_n$  são dependentes em relação a  $F$  e  $G$  em  $P$  através de  $L$ . Como esta igualdade é válida para quaisquer  $n$  polinómios homogéneos  $Q_1, \dots, Q_n$ , e  $n$  é maior que  $I_{\mathcal{P}}(\bar{F}, \bar{G})$ , segue-se a desigualdade  $I_{\mathcal{P}}(F, G) \leq I_{\mathcal{P}}(\bar{F}, \bar{G})$ .

Se substituirmos  $F, G, P$  por  $\bar{F}, \bar{G}, \bar{P}$  na desigualdade (24) obtemos  $I_{\mathcal{P}}(\bar{F}, \bar{G}) \leq I_{\bar{\mathcal{P}}}(\bar{\bar{F}}, \bar{\bar{G}})$  logo a desigualdade  $I_{\bar{\mathcal{P}}}(\bar{\bar{F}}, \bar{\bar{G}}) \leq I_{\mathcal{P}}(F, G)$ . Demonstradas as duas desigualdades, temos a igualdade pretendida.  $\square$

Chegámos ao momento de demonstrar que toda a cúbica irredutível não singular tem uma flexão no plano projectivo real. Através do teorema de Bézout concluímos que  $C$  e  $\det H$  intersectam-se nove vezes no plano projectivo complexo. Como nove é um número ímpar, então intersectam-se pelo menos uma vez no plano projectivo real.

#### Teorema 4.22

*Toda a cúbica irredutível não singular tem uma flexão no plano projectivo real.*

#### Demonstração

Sejam  $C$  uma cúbica irredutível não singular com coeficientes reais em que  $\det H$  representa o determinante da sua hessiana. Como  $C$  é uma cúbica irredutível e não singular, pelo teorema 4.20, o  $\det H$  não é múltiplo escalar de  $C$ . Assim,  $C$  e  $\det H$  não têm factores comuns de grau positivo sobre os reais. Pelo teorema 4.15, concluímos que não têm factores de grau positivo em comum sobre os complexos.

O grau de  $C$  e do  $\det H$  é três. Pelo teorema de Bézout sabemos que estas duas curvas intersectam-se nove vezes, contando as multiplicidades, no plano projectivo complexo. Pela propriedade 4.21 e sabendo que  $C$  e  $\det H$  têm coeficientes reais concluímos que  $I_{\mathcal{P}}(C; \det H) = I_{\bar{\mathcal{P}}}(C; \det H)$ . Assim, se  $P$  pertence à intersecção de  $C$  e  $\det H = 0$ , então o seu conjugado também pertence. Porque 9 é um número ímpar, existe pelo menos um ponto com coordenadas reais que pertence a esta intersecção. Chamemos  $R$  a esse ponto. Como as coordenadas de  $R$  não são todas zero, podemos pensar nele como tendo a última coordenada diferente de zero, nem que para isso seja necessário alternar  $z$  com  $x$  ou  $y$ . Multiplicando as coordenadas de  $R$  por  $c^{-1}$  obtemos  $R = (a, b, 1)$  para  $a$  e  $b$  reais. Sendo assim,  $R$  pertence ao

#### IV. Cúbicas

plano projectivo real e pertence a  $C$  e a  $\det H = 0$ . Como por hipótese  $C$  não tem pontos singulares então, pelo teorema 4.19,  $R$  é uma flexão de  $C$ .  $\square$

Com este último resultado ficam classificadas todas as cúbicas irredutíveis no plano projectivo real. Pelo teorema 4.10, concluímos que uma cúbica é irredutível e não singular se e só se puder ser transformada numa das duas equações (6) e (7). O teorema 4.11 caracteriza todas as cúbicas irredutíveis singulares.

## Referências bibliográficas

- Adler, A. & Coury, J.E.** (1995) — *The theory of Numbers: A text and Source Book of Problems*, Jones and Bartlett Publishers, Boston.
- Aczel, A.D.** (1996) — *O Último Teorema de Fermat, A descoberta do segredo de um problema matemático secular*, Gradiva.
- Baart, M.L. & Mcleod, R.Y.** (1998) — *Geometry and Interpolation of Curves and Surfaces*, Cambridge University Press.
- Bix, R.** (1998) — *Conic and Cubics, A concrete Introduction to Algebraic Curves*, Springer, New York.
- Brieskorn, E. & Knörrer, H.** (1986) — *Plane Algebraic Curves*, Birkhäuser-Verlag.
- Brisson, O.J.** (1998) — *Teoria de Galois*, Textos de Matemática, Universidade de Lisboa. Faculdade de Ciências, Departamento de Matemática.
- Boyer, C.B.** (1996) — *História da Matemática*, Edgard Blücher Ltda Brasil.
- David M.B.** (1991) — *The History of Mathematics, An introduction*, Wm. C. Brown Publishers.
- Dieudonné, J.** (1972) — *The History of Algebraic Geometry*, The American Mathematical Monthly, Vol 76.
- Casas-Alvero, E.** (2000) — *Singularities of Plane Curves*, London Mathematical Society, Lecture Notes Series 276, Cambridge University Press.
- Fischer, G.** (2000) — *Plane Algebraic Curves*, Student Mathematical Library, Volume 15, American Mathematical Society.
- Gibson, C.G.** (1998) — *Elementary Geometry of Curves, an Undergraduate Introduction*, Cambridge University Press.
- Griffiths, P.A.** (1989) — *Introduction to Algebraic Curves*, Translations of Mathematical Monographs, Volume 76, American Mathematical Society, Providence, Rhode Island.

- Hartshorne, R.** (1977) — *Algebraic Geometry*, Springer-Verlag.
- Itô, K.** (Editor, 1993) — *Encyclopedic Dictionary of Mathematics*, vol. I e II, Second edition, MIT Press, Cambridge.
- Kirwan, F.** (1992) — *Complex Algebraic Curves*, London Mathematical Society, Student Texts 23, Cambridge University Press.
- Lockwood, E.H.** (1961) — *A Book of Curves*, Cambridge University Press.
- Needham, T.** (1997) — *Visual Complex Analysis*, Department of Mathematics, University of San Francisco, Clarendon Press, Oxford.
- Neto, O.** (1994) — *Equações diferenciais em Superfícies de Riemann*, Universidade de Lisboa, Faculdade de Ciências.
- Reid, M.** (1988) — *Undergraduate Algebraic Geometry*, Mathematics Institute, University of Warwick, London Mathematical Society, Student Texts 12, Cambridge University Press.
- Sebastião e Silva, J.** (1999) — *Análise Superior*, Parte II.2 da obra *Textos Didáticos*, vol. II, Fundação Calouste Gulbenkian.
- Sierpinski, W.** (1964) — *Elementary Theory of Numbers*, Translated by A. Hulaniki, Varsóvia.
- Struik, D.J.** (1987) — *História Concisa das Matemáticas*, Gradiva.
- Walker, R.J.** (1950) — *Algebraic Curves*, Springer-Verlag.

## Internet

<http://mathforum.org/> – The Math Forum, A Math Education Community Center on the Internet, Swarthmore College.

<http://mathworld.wolfram.com/>

[http://www.math.niu.edu/~beachy/abstract\\_algebra](http://www.math.niu.edu/~beachy/abstract_algebra) – Abstract Algebra On-line, John Beachy, Northern Illinois University.

[http://xahlee.org/SpecialPlaneCurves\\_dir/specialPlaneCurves.html](http://xahlee.org/SpecialPlaneCurves_dir/specialPlaneCurves.html) – A Visual Dictionary of Special Plane Curves, Xah Lee.