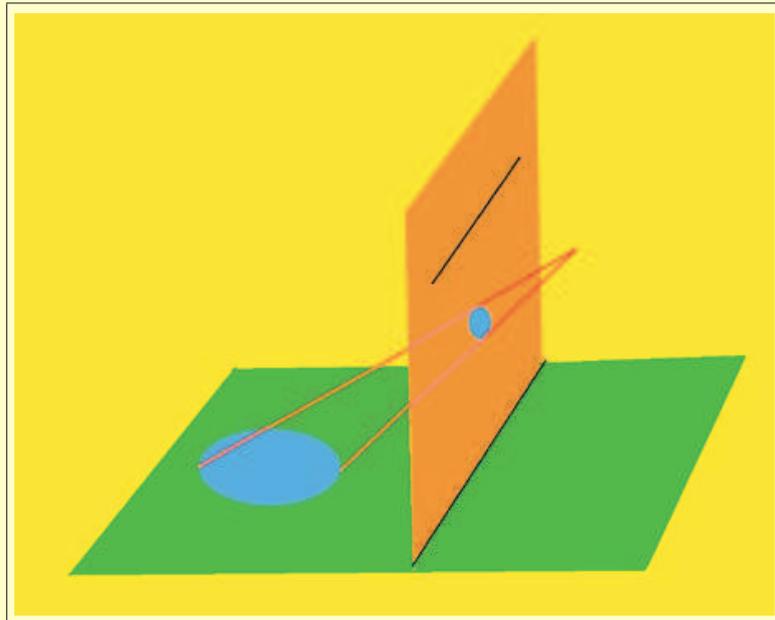

FCUP
Dep. Matemática Pura

Tópicos de Geometria



Licenciatura em Matemática

Ano lectivo de 2005/06

João Nuno Tavares

Centro de Matemática da Universidade do Porto

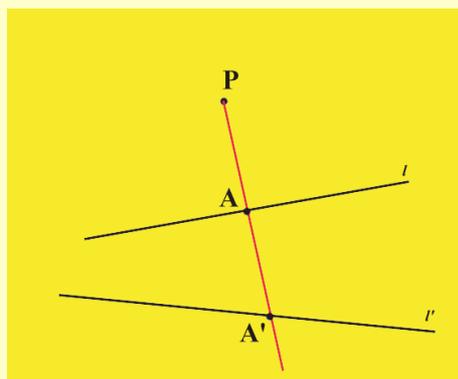
ÍNDICE:

1	Perspectiva no plano. Homografias	2
2	Perspectiva no espaço	9
3	A recta projectiva \mathbb{P}^1	12
4	O plano projectivo \mathbb{P}^2	15
5	Fecho Projectivo do plano afim \mathbb{A}^2	18
6	Dualidade no plano	28
7	Teoremas de Desargues e Pappus	32
8	Cónicas. Polaridade	38
9	Equações tangenciais das cónicas. Assíptotas e focos	43
10	Homografias e Cónicas. Teoremas de Pascal e Brianchon	47
11	Pontos racionais em cónicas	52
12	Curvas algébricas planas afins. Mais exemplos	55
13	Curvas algébricas planas afins. Pontos simples e múltiplos	58
14	Tangentes afins	63
15	Curvas planas projectivas. Tangentes	66
16	Inflexões	71
17	Teorema de Bézout. Aplicações	75
18	Teorema dos nove pontos. Aplicações	81
19	Pontos racionais em cúbicas. Estrutura de grupo numa cúbica	85

Tópico 1

Perspectiva no plano. Homografias

► **1.1 Perspectiva. Projecção central** ... No plano afim $\mathbb{A} = \mathbb{A}^2$, consideremos duas rectas distintas ℓ, ℓ' e um ponto P (o ponto de vista, ou o olho) não pertencente a qualquer delas.



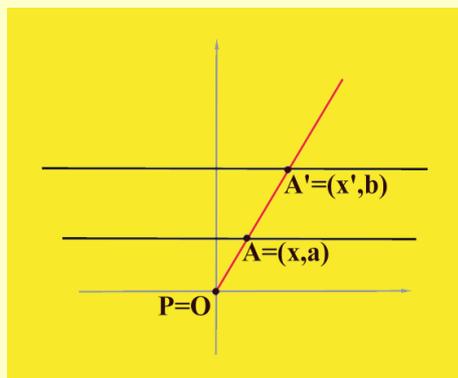
Definamos uma aplicação $\Pi = \Pi_P : \ell \rightarrow \ell'$, chamada **projecção central** de centro P , de ℓ sobre ℓ' , ou **perspectiva** de ℓ sobre ℓ' , com ponto de vista P , da seguinte forma - a cada ponto $A \in \ell$ associamos o ponto $A' \in \ell'$, intersecção da recta AP , que une A com P , com a recta ℓ' :

$$\begin{aligned} \Pi : \ell &\rightarrow \ell' \\ A &\mapsto A' = AP \cap \ell' \end{aligned} \quad (1.1)$$

Diz-se então que a pontual (A) , de suporte ℓ , está em correspondência perspectiva, de centro P , com a pontual (A') , de suporte ℓ' , e nota-se por:

$$(A) \stackrel{P}{\wedge} (A') \quad (1.2)$$

► **1.2** Suponhamos que as rectas são paralelas.



Escolhamos um referencial de origem em $O \equiv P$ e com eixos como se indica na figura. A condição de colinearidade dos pontos $O = (0, 0)$, $A = (x, a)$ e $A' = (x', b)$ é:

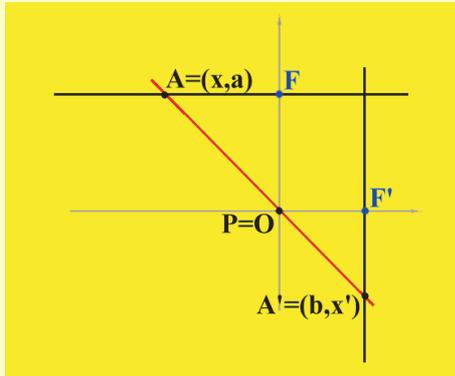
$$\begin{vmatrix} 0 & 0 & 1 \\ x & a & 1 \\ x' & b & 1 \end{vmatrix} = 0 \quad \Rightarrow \quad bx - ax' = 0$$

isto é:

$$x' = kx \quad (1.3)$$

onde $k = b/a$. Π é pois uma **homotetia** de razão $k = b/a$.

► 1.3 Suponhamos agora que as rectas são perpendiculares.



Escolhamos um referencial de origem em $O \equiv P$ e com eixos como se indica na figura, de tal forma que as rectas ℓ e ℓ' são dadas por $y = a$ e $x = b$, respectivamente. A condição de colinearidade dos pontos $O = (0, 0), A = (x, a) \in \ell$ e $A' = (b, x') \in \ell'$ é:

$$\begin{vmatrix} 0 & 0 & 1 \\ x & a & 1 \\ b & x' & 1 \end{vmatrix} = 0 \quad \Rightarrow \quad xx' - ab = 0$$

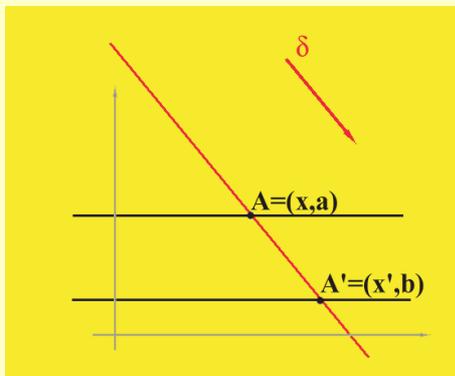
isto é

$$x' = \frac{c}{x}, \quad x \neq 0 \quad (1.4)$$

onde $c = ab$. Π é pois proporcional a uma **inversão**.

Note que Π não está definida no ponto $F = (0, a) \in \ell$, intersecção com a recta ℓ do raio que passa em O e é paralelo à recta ℓ' . Este ponto diz-se o **ponto de fuga** de Π sobre ℓ . É claro que podemos prolongar a definição de Π , juntando um ponto $\infty' \in \ell'$ e ponto $\Pi(F) = \infty'$. Por outro lado, o ponto $F' = (b, 0) \in \ell'$ não é imagem de qualquer ponto de ℓ . Se adicionarmos um ponto $\infty \in \ell$ e definirmos $\Pi(\infty) = F'$, prolongamos Π a uma bijecção de $\ell \cup \infty$ sobre $\ell' \cup \infty'$.

► 1.4 Projectão paralela ...

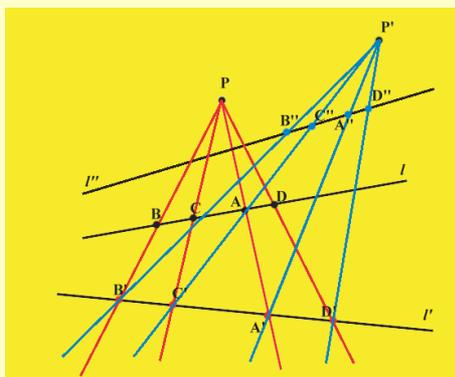


Suponhamos agora o ponto de vista P está no “infinito”. Mais exactamente, suponhamos que todos os raios são paralelos a uma dada direcção comum δ . Definamos de novo uma aplicação $\Pi : \ell \rightarrow \ell'$, chamada **projectão paralela** de direcção δ , de ℓ sobre ℓ' , - a cada ponto $A \in \ell$ associamos o ponto $A' \in \ell'$, intersecção do raio que passa em A , e é paralelo a δ , com a recta ℓ' . É fácil ver que, escolhendo o referencial como se indica na figura, se tem:

$$x' = x + l \quad (1.5)$$

Π é pois uma **translação**.

► 1.5 Projectividades ...



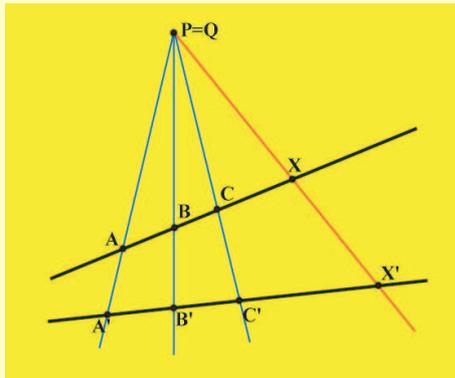
Qualquer aplicação de uma recta sobre uma outra, que seja a composta de um número finito de projecções (centrais ou paralelas), diz-se uma **projectividade**. A geometria projectiva de uma recta é o conjunto de propriedades invariantes sob projectividades.

► **1.6 Construção de projectividades** ... Suponhamos que (A, B, C) são 3 pontos distintos numa recta ℓ e (A', B', C') são 3 pontos distintos numa outra recta ℓ' . Suponhamos que existe uma projectividade de ℓ sobre ℓ' que envia A, B, C respectivamente em A', B', C' . Como construir a imagem X' de um quarto ponto $X \in \ell$? Para representar que os pontos referidos estão em correspondência projectiva escrevemos:

$$(A, B, C, X) \bar{\wedge} (A', B', C', X') \tag{1.6}$$

Suponhamos que a recta AA' intersecta a recta BB' num ponto P e a recta CC' num ponto Q .

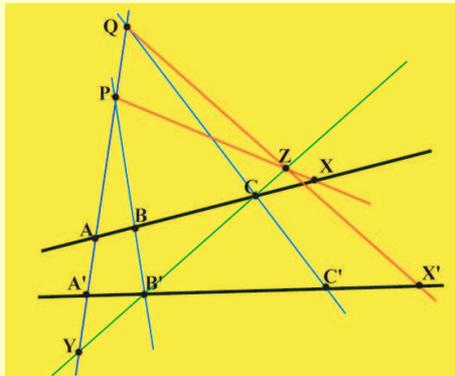
Temos então duas possibilidades:



[I]. $P = Q$. Neste caso, basta pôr $X' =$ ponto de interseção da recta PX com ℓ' . Então:

$$(A, B, C, X) \stackrel{P}{\bar{\wedge}} (A', B', C', X')$$

isto é a projectividade é uma perspectiva de centro $P = Q$.



[II]. $P \neq Q$. Suponhamos que (i). a recta PQ intersecta $B'C$ num ponto Y , (ii). a recta PX intersecta $B'C$ num ponto Z .

Põe-se $X' =$ ponto de intersecção da recta QZ com ℓ' . Tem-se então que:

$$(A, B, C, X) \stackrel{P}{\bar{\wedge}} (Y, B', C, Z) \stackrel{Q}{\bar{\wedge}} (A', B', C', X')$$

A projectividade é pois a composta de duas perspectivas de centros P e Q , respectivamente.

Concluimos ainda que *qualquer projectividade entre duas rectas ou é uma perspectiva ou é a composta de duas perspectivas.*

► **1.7 Homografias** ... As aplicações que encontramos nas secções anteriores são todas do tipo:

$$x' = \frac{ax + b}{cx + d}, \quad \text{com} \quad ad - bc \neq 0 \tag{1.7}$$

que se chamam **homografias** da recta. A condição $ad - bc \neq 0$ garante que a aplicação não é constante.

Escrevendo:

$$\frac{ax + b}{cx + d} = \frac{ax + \frac{ad}{c} + b - \frac{ad}{c}}{cx + d} = \frac{\frac{a}{c}(cx + d) + \frac{1}{c}(bc - ad)}{cx + d}$$

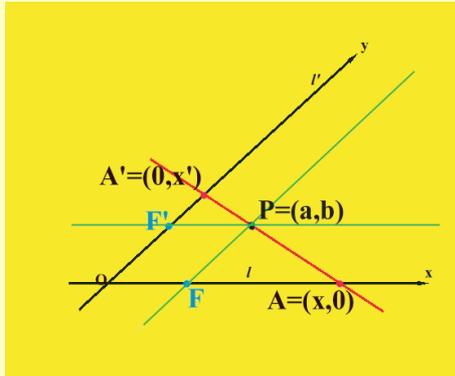
vemos que toda a homografia, com $c \neq 0$, pode ser escrita na forma:

$$x' = \frac{a}{c} + \frac{bc - ad}{c(cx + d)}$$

o que mostra que é a composta de funções do tipo $x \mapsto x + l$, $x \mapsto kx$ e $x \mapsto 1/x$, para valores adequados de k e l . Para $c = 0$ a homografia é do tipo $x' = \frac{a}{d}x + \frac{b}{d}$ e o resultado é evidente.

Portanto qualquer homografia da recta pode ser obtida através de uma sequência de projecções do tipo considerado nas secções anteriores. Vejamos o recíproco.

► **1.8 Teorema** ... *Qualquer sequência finita de projecções (centrais ou paralelas) da recta pode ser expressa através de uma homografia.*



Como já vimos, isto é verdade para uma projecção de uma recta sobre uma recta paralela. Resta ver qual a função associada a uma projecção de uma recta sobre uma recta concorrente.

Quando as rectas são concorrentes, escolhemos um referencial com origem no ponto de intersecção, o eixo dos xx como sendo a recta ℓ , o eixo dos yy como sendo a recta ℓ' , e supomos que a projecção se faz a partir do centro $V = (a, b)$.

Os cálculos prosseguem como no caso anterior:

$$\begin{vmatrix} a & b & 1 \\ x & 0 & 1 \\ 0 & x' & 1 \end{vmatrix} = 0 \quad \Rightarrow \quad -ax' - bx + xx' = 0$$

isto é:

$$x' = \frac{bx}{x - a}, \quad x \neq a \tag{1.8}$$

Note que Π não está definida no ponto $F = (a, 0) \in \ell$, intersecção com a recta ℓ do raio que passa em O e é paralelo à recta ℓ' . Este ponto diz-se o ponto de fuga de Π sobre ℓ . É claro que podemos prolongar a definição de Π , juntando um ponto ∞' a ℓ' e pondo $\Pi(F) = \infty'$.

► **1.9** $\widehat{\mathbb{k}} = \mathbb{k} \cup \{\infty\}$... Definamos $\widehat{\mathbb{k}} = \mathbb{k} \cup \{\infty\}$ e prolonguemos a definição de homografia a $\widehat{\mathbb{k}}$ de acordo com as regras seguintes:

$$x \rightarrow x' = \phi(x) = \frac{ax + b}{cx + d}, \quad x \in \mathbb{k} \cup \{\infty\}, \quad ad - bc \neq 0 \tag{1.9}$$

com:

$$\begin{cases} \text{se } c \neq 0 : & \phi(-d/c) = \infty \\ & \phi(\infty) = a/c \\ \text{se } c = 0 : & \phi(\infty) = \infty \end{cases} \tag{1.10}$$

► **1.10 Razão anarmónica** ... Dados quatro pontos distintos $a, b, c, d \in \mathbb{k}$, definamos a sua **razão anarmónica** através de:

$$(abcd) = \frac{c - a}{b - c} : \frac{d - a}{b - d} \tag{1.11}$$

Se $A, B, C, D \in r$ são quatro pontos distintos de uma recta afim r , com abcissas a, b, c, d , respectivamente, relativamente a um referencial afim de r , define-se a razão anarmónica desses quatro pontos através de:

$$(ABCD) = \frac{c - a}{b - c} : \frac{d - a}{b - d} = \frac{\overline{AC}}{\overline{CB}} : \frac{\overline{AD}}{\overline{DB}} \tag{1.12}$$

Note que esta razão anarmónica é um quociente de duas razões: a primeira $\frac{\overline{AC}}{\overline{CB}}$ é a razão segundo a qual o ponto C divide o segmento AB , e a segunda $\frac{\overline{AD}}{\overline{DB}}$ é a razão segundo a qual o ponto D divide esse mesmo segmento AB .

► **1.11 Propriedades da razão anarmónica** ... É fácil ver que:

$$(abcd) = (abdc)^{-1} = (cdab) \quad (1.13)$$

$$(abcd) + (acbd) = 1 \quad (1.14)$$

Quando três dos pontos estão fixos, a razão anarmónica é uma homografia relativamente ao outro ponto. Por outras palavras, a razão anarmónica é uma homografia quando considerada como função de cada uma das suas variáveis.

Podemos pois prolongar a definição (1.11) ao caso em que um dos pontos é ∞ , usando as convenções $1/\infty = 0$ e $1/0 = \infty$. Assim, se, por exemplo, $a = \infty$, põmos $a = 1/t$ na fórmula anterior, simplificamos e fazemos $t = 0$:

$$(\infty bcd) = \frac{c - \frac{1}{t}}{b - c} : \frac{d - \frac{1}{t}}{b - d} = \frac{(ct - 1)(b - d)}{(dt - 1)(b - c)} = \frac{b - d}{b - c}$$

onde pusemos $t = 0$ na última igualdade. Analogamente:

$$\begin{aligned} (a\infty cd) &= \frac{c - a}{d - a} \\ (ab\infty d) &= \frac{d - b}{d - a} \\ (abc\infty) &= \frac{c - a}{b - a} \end{aligned} \quad (1.15)$$

Podemos ainda prolongar a definição (1.11) ao caso em que dois dos pontos são iguais. Por exemplo:

$$\begin{aligned} (aacd) &= (abcc) = 1 \\ (abad) &= (abcb) = 0 \\ (abca) &= (abbd) = \infty \end{aligned} \quad (1.16)$$

Fixemos agora três pontos distintos a, b, c em $\widehat{\mathbb{k}}$. Então a aplicação:

$$h : d \mapsto (abcd) \quad (1.17)$$

é uma homografia $h : \widehat{\mathbb{k}} \rightarrow \widehat{\mathbb{k}}$ tal que:

$$h(a) = \infty, \quad h(b) = 0, \quad h(c) = 1$$

De facto é a única homografia com esta propriedade, como veremos em breve.

► **1.12 Teorema** ... Toda a homografia $h : \widehat{\mathbb{k}} \rightarrow \widehat{\mathbb{k}}$ preserva a razão anarmónica de quatro pontos:

$$(h(a)h(b)h(c)h(d)) = (abcd) \quad (1.18)$$

De facto basta ver que isto é verdadeiro para as três homografias geradoras $h(x) = x + l$, $h(x) = kx$ e $h(x) = 1/x$, o que pode ser facilmente feito por cálculo directo.

► **1.13 Teorema** ... Dados três pontos distintos $a, b, c \in \widehat{\mathbb{K}}$, qualquer outro ponto $x \in \widehat{\mathbb{K}}$ fica univocamente determinado pela razão anarmónica $(abcx) = y$

De facto basta observar que a equação:

$$y = (abcx) = \frac{c-a}{b-c} : \frac{x-a}{b-x}$$

pode ser resolvida univocamente em ordem a x , como função de a, b, c e y .

► **1.14 Teorema** ... Dados três pontos distintos $a, b, c \in \widehat{\mathbb{K}}$, e outros três pontos distintos $a', b', c' \in \widehat{\mathbb{K}}$ existe uma e uma só homografia $h : \widehat{\mathbb{K}} \rightarrow \widehat{\mathbb{K}}$ tal que $h(a) = a', h(b) = b'$ e $h(c) = c'$.

Basta tomar duas cópias de $\widehat{\mathbb{K}}$, digamos ℓ e ℓ' , com $a = a'$, e projectar a partir de um ponto C exterior a essas duas rectas.

h deve enviar qualquer $x \neq a, b, c$ em x' que satisfaça $(abcx) = (a'b'c'x')$, uma vez que h preserva razão anarmónica. Mas este x' é único, como vimos no teorema anterior.

► **1.15 Teorema** ... Uma aplicação $f : \widehat{\mathbb{K}} \rightarrow \widehat{\mathbb{K}}$ é uma homografia se e só se preserva a razão anarmónica.

Suponhamos que $f : \widehat{\mathbb{K}} \rightarrow \widehat{\mathbb{K}}$ é uma aplicação que preserva a razão anarmónica:

$$(f(a)f(b)f(c)f(d)) = (abcd)$$

Podemos encontrar uma homografia $h : \widehat{\mathbb{K}} \rightarrow \widehat{\mathbb{K}}$ que coincide com f em a, b, c . Mas, como f preserva razão anarmónica, h coincide com f também no ponto d . Logo $f \equiv h$.

► **1.16 Divisão harmónica** ... Quando:

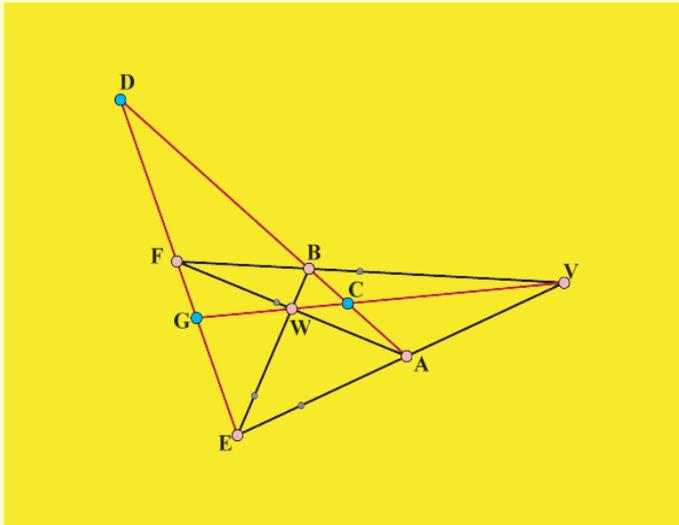
$$(ABCD) = -1 \tag{1.19}$$

diz-se que o par ordenado de pontos (C, D) **divide harmonicamente** o par ordenado de pontos (A, B) . Diz-se ainda que o quádruplo ordenado (A, B, C, D) é harmónico e que D é o **quarto harmónico** do terno ordenado (A, B, C) .

Esta propriedade é preservada se permutamos os pares (A, B) com (C, D) e ainda se permutamos os elementos dentro de qualquer destes pares.

Por exemplo, na recta $\widehat{r} = r \cup \{\infty\}$, o par (M, ∞) , onde M é o ponto médio do segmento AB , divide harmonicamente o par ordenado de pontos (A, B) .

► **1.17 Quadrilátero completo** ... É a figura do plano que consiste de quatro rectas e dos seus seis pontos de intersecção V, A, B, W, E, F .



As rectas VW , AB e EF , dizem-se as **diagonais** do quadrilátero completo.

Consideremos uma das diagonais, por exemplo a diagonal AB na figura, e os pontos nela determinados pelas intersecções das outras duas. Na figura os pontos C e D . Então $(ABCD) = -1$, isto é, o par (C, D) separa harmonicamente o par de vértices (A, B) .

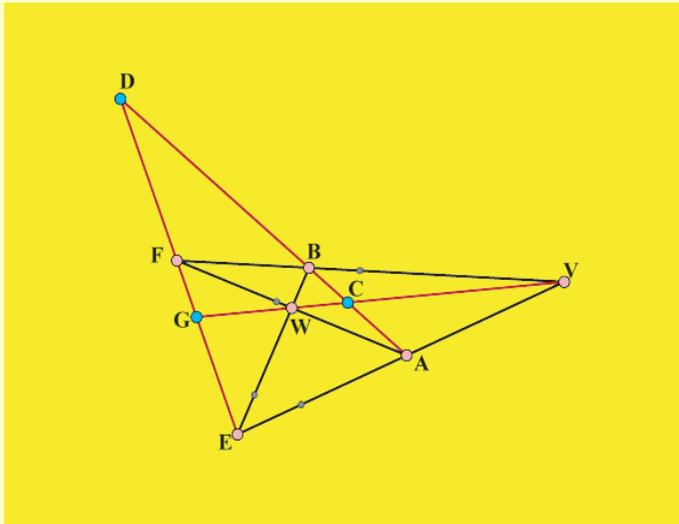
Portanto, *num quadrilátero completo, os pontos de intersecção de uma das diagonais com as outras duas, separa os vértices dessa diagonal harmonicamente.*

De facto:

$$\begin{aligned} x &= (ABCD) = (EFGD) \text{ por projecção de centro } V \\ &= (BACD) \text{ por projecção de centro } W \end{aligned}$$

Mas $(BACD) = 1/(ABCD)$, donde se deduz que $x = 1/x$, i.e., $x^2 = 1$, ou ainda $x = \pm 1$. Mas como o par (A, B) separa (C, D) , a razão anarmónica x é negativa e portanto $x = -1$, como se pretendia.

► 1.18 Construção do quarto harmónico ...



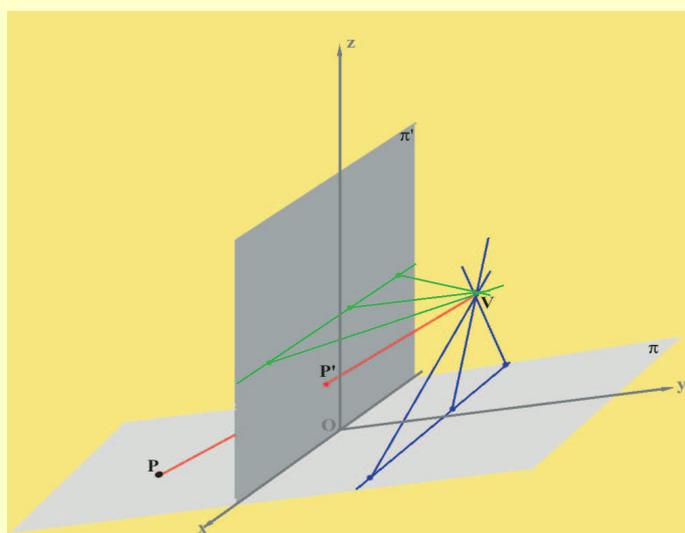
A propriedade anterior do quadrilátero completo, permite construir, apenas com régua (não graduada), o quarto harmónico D de um terço ordenado (A, B, C) de pontos colineares.

Para isso, basta escolher um ponto V fora da recta AB , traçar as rectas VA, VB e VC , escolher um ponto W em VC e traçar AW e BW que intersectam VB e VA , respectivamente em E e F , e finalmente traçar EF que intersectará AB no quarto harmónico D .

Tópico 2

Perspectiva no espaço

► 2.1 Perspectiva. Projecção central ...



No espaço afim $\mathbb{E} = \mathbb{A}^3$, consideremos dois planos distintos π, π' e um ponto V (o ponto de vista) não pertencente a qualquer deles. Suponhamos que os planos se intersectam numa recta i (quando são paralelos a análise é análoga).

Definamos uma aplicação $\Pi : \pi \rightarrow \pi'$, chamada **projecção central** de centro V , de π sobre π' , ou **perspectiva** de π sobre π' , com ponto de vista V , da seguinte forma - a cada ponto $P \in \pi$ associamos o ponto $P' \in \pi'$, intersecção da recta VP , que une V com P , com o plano π' :

$$\Pi : \pi \rightarrow \pi', \quad P' = \Pi(P) = VP \cap \pi' \quad (2.1)$$

Escolhamos um referencial afim com origem num ponto $O \in i = \pi \cap \pi'$, com o eixo dos x coincidente com a recta i e o eixos dos y e dos z coincidentes com rectas respectivamente em π e π' . Os planos π e π' são dados pois pelas equações $z = 0$ e $y = 0$.

Suponhamos que $V = (a, b, c)$ nesse referencial. A condição de colinearidade dos pontos $V = (a, b, c)$, $P = (x, y, 0)$ e $P' = (x', 0, y')$ é:

$$(a, b, c) = (x, y, 0) + t((x', 0, y') - (x, y, 0))$$

ou:

$$\frac{x - x'}{x - a} = \frac{y}{y - b} = \frac{y'}{c}$$

Resolvendo em ordem a x' e a y' , vem:

$$x' = \frac{ay - bx}{y - b}, \quad y' = \frac{cy}{y - b}, \quad P \neq (x, b, 0) \quad (2.2)$$

e a aplicação inversa é dada por:

$$x = \frac{ay' - cx'}{y' - c}, \quad y = \frac{by'}{y' - c}, \quad P' \neq (x', 0, c) \quad (2.3)$$

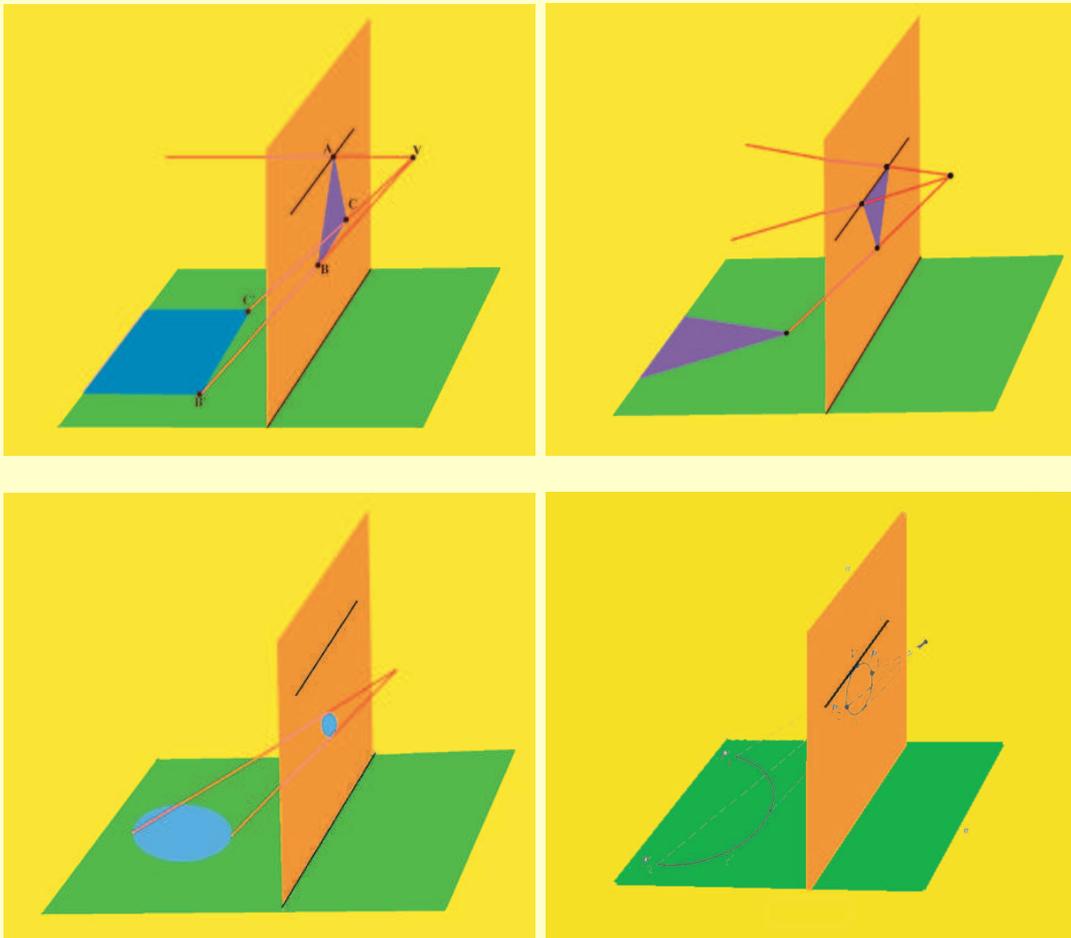
Π é uma colineação - a imagem de uma recta $\ell \subset \pi$ é a recta $\ell' \subset \pi'$ obtida intersectando o plano π' com o plano gerado por V e ℓ .

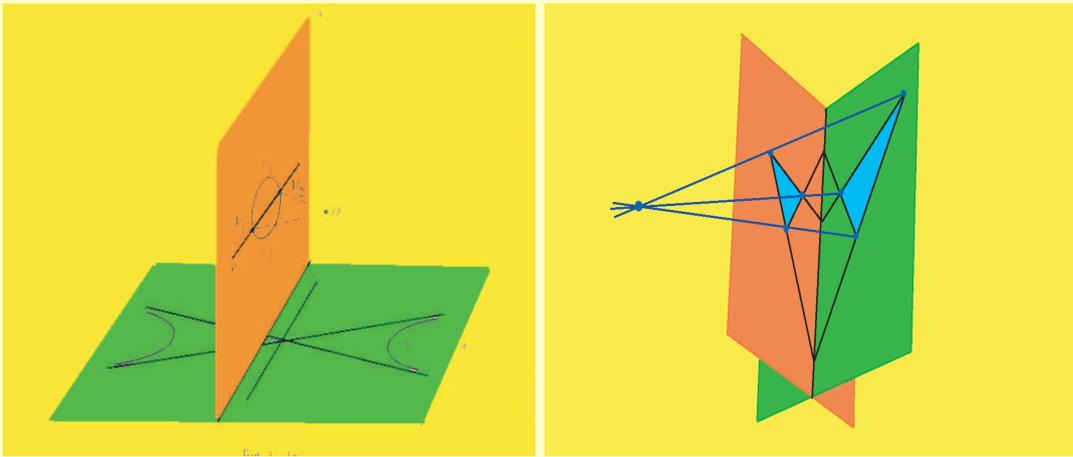
Note que $\Pi : \pi \rightarrow \pi'$ não está definida nos pontos da forma $(x, b, 0) \in \pi$ que estão sobre uma recta π_∞ de π que se diz a linha de fuga (ou linha do horizonte) de Π em π .

A aplicação inversa $\Lambda : \pi' \rightarrow \pi$ não está definida nos pontos da forma $(x', 0, c) \in \pi'$ que estão sobre uma recta π'_∞ de π' que se diz a linha de fuga (ou linha do horizonte) de ψ em π' .

A imagem de duas rectas de π , concorrentes num ponto $I \in \pi_\infty$, consiste de duas rectas em π' , paralelas à recta VI .

Nas figuras seguintes ilustram-se alguns efeitos geométricos da perspectiva $\Pi : \pi \rightarrow \pi'$.





► **2.2 Projectividades** ... Qualquer aplicação de um plano sobre um outro, que seja a composta de um número finito de projecções (centrais ou paralelas), diz-se uma **projectividade**. A geometria projectiva de um plano é o conjunto de propriedades invariantes sob projectividades.

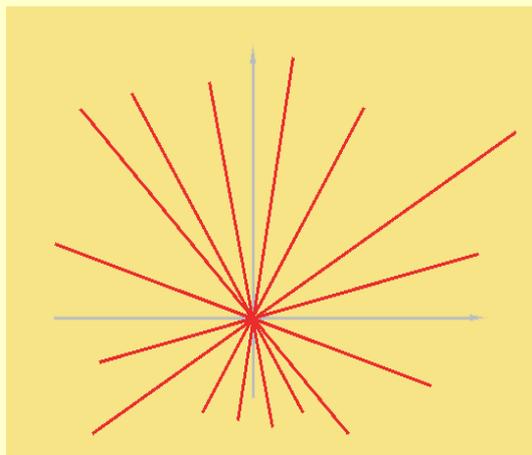
Tópico 3

A recta projectiva \mathbb{P}^1

► **3.1 Recta projectiva \mathbb{P}^1** ... Seja $\mathbb{k} = \mathbb{R}$ ou \mathbb{C} . A **recta projectiva** $\mathbb{P}^1 = \mathbb{P}_{\mathbb{k}}^1$ é, por definição, o conjunto constituído por todas as rectas vectoriais de \mathbb{k}^2 :

$$\mathbb{P}^1 \stackrel{\text{def}}{=} \{ \ell : \ell \text{ é subespaço de dimensão 1 em } \mathbb{k}^2 \} \quad (3.1)$$

Quando $\mathbb{k} = \mathbb{R}$ põe-se $\mathbb{P}_{\mathbb{R}}^1 = \mathbb{P}^1(\mathbb{R})$ para a recta projectiva real, e quando $\mathbb{k} = \mathbb{C}$ põe-se $\mathbb{P}_{\mathbb{C}}^1 = \mathbb{P}^1(\mathbb{C})$ para a recta projectiva complexa.



► **3.2** Temos então uma aplicação natural sobrejectiva:

$$\begin{array}{ccc} \pi : \mathbb{k}^2 - \{0\} & \longrightarrow & \mathbb{P}^1 \\ \mathbf{a} & \longmapsto & A = \pi(\mathbf{a}) = [\mathbf{a}] \end{array} \quad (3.2)$$

onde $[\mathbf{a}] = \mathbb{k}\mathbf{a}$ representa a recta vectorial gerada pelo vector $\mathbf{a} \in \mathbb{k}^2 - \{0\}$. \mathbf{a} diz-se um representante do ponto $A \in \mathbb{P}^1$.

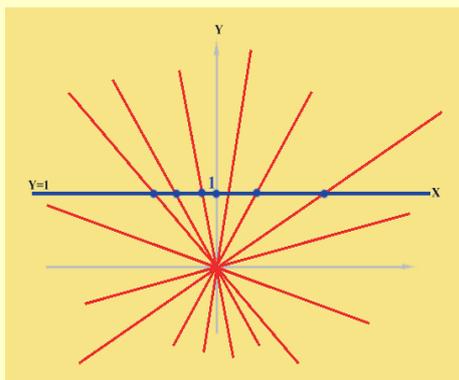
► **3.3 Coordenadas homogéneas** ... Se $\mathbf{a} = (X, Y) \in \mathbb{k}^2 - \{0\}$, os números X e Y dizem-se as **coordenadas homogéneas** do ponto $A = [\mathbf{a}]$. Escreve-se então:

$$A = [X, Y]$$

ou, por vezes, $A = (X : Y)$. As coordenadas homogéneas X e Y do ponto $A = [\mathbf{a}]$ estão definidas a menos de um múltiplo escalar não nulo, isto é, λX e λY , com $\lambda \neq 0$, são também coordenadas homogéneas do ponto $A = [\mathbf{a}]$:

$$A = [X, Y] = [\lambda X, \lambda Y], \quad \forall \lambda \neq 0$$

► 3.4



O complementar do ponto $A = (1 : 0) = [i]$, em \mathbb{P}^1 , é uma recta afim. De facto pode ser posto em correspondência bijectiva com a recta afim $Y = 1$ em \mathbb{k}^2 :

$$\begin{aligned} \mathbb{P}^1 - \{[1, 0]\} &\longrightarrow \{Y = 1\} \subset \mathbb{k}^2 \\ [X, Y] &\rightleftharpoons (x = X/Y, 1) \end{aligned} \quad (3.3)$$

Portanto \mathbb{P}^1 pode ser considerado como a reunião da recta afim $Y = 1$ em \mathbb{k}^2 , com o ponto do infinito $[1, 0] = \infty_X$.

► 3.5 $\mathbb{P}^1(\mathbb{R})$ é homeomorfo a um círculo \mathbf{S}^1 , enquanto que $\mathbb{P}^1(\mathbb{C})$ é homeomorfo a uma esfera \mathbf{S}^2 !

► 3.6 Como vimos, existe uma bijecção entre $\mathbb{P}^1 = \mathbb{P}_{\mathbb{k}}^1$ e $\mathbb{k} \cup \{\infty\}$:

$$\begin{aligned} \Psi : \quad \mathbb{P}^1 &\longrightarrow \mathbb{k} \cup \{\infty\} \\ [X, Y] &\longmapsto x = \frac{X}{Y}, \quad \text{se } Y \neq 0 \\ [X, 0] &\longmapsto \infty, \quad \text{se } X \neq 0 \end{aligned} \quad (3.4)$$

A bijecção recíproca é dada por:

$$\begin{aligned} \Psi^{-1} : \quad \mathbb{k} \cup \{\infty\} &\longrightarrow \mathbb{P}^1 \\ x \neq \infty &\longmapsto [x, 1] = [X, Y], \quad \text{pondo } x = X/Y \text{ com } Y \neq 0 \\ \infty &\longmapsto [1, 0] \end{aligned} \quad (3.5)$$

► 3.7 Uma homografia $h : \mathbb{P}^1 \rightarrow \mathbb{P}^1$, é uma aplicação induzida por uma transformação linear inversível $H : \mathbb{k}^2 \rightarrow \mathbb{k}^2$.

Suponhamos que a matriz de H , relativamente à base canónica de \mathbb{k}^2 , é:

$$H = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad a, b, c, d \in \mathbb{k}, \quad ad - bc \neq 0$$

Portanto:

$$H(X, Y) = (aX + bY, cX + dY)$$

e, em coordenadas homogéneas, h escreve-se na forma:

$$h[X, Y] = [aX + bY, cX + dY]$$

Finalmente, utilizando as bijecções Ψ e Ψ^{-1} atrás referidas, podemos escrever:

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{h} & \mathbb{P}^1 \\ \Psi \downarrow & & \downarrow \Psi \\ \mathbb{k} \cup \infty & \xrightarrow{\Psi \circ h \circ \Psi^{-1}} & \mathbb{k} \cup \infty \end{array}$$

$$\left\{ \begin{array}{l} x \neq \infty \\ x = -\frac{d}{c}, c \neq 0 \\ x = \infty \end{array} \right. \begin{array}{l} \xrightarrow{\Psi^{-1}} [x, 1] \\ \xrightarrow{\Psi^{-1}} [-\frac{d}{c}, 1] \\ \xrightarrow{\Psi^{-1}} [1, 0] \end{array} \begin{array}{l} \xrightarrow{h} [ax + b, cx + d] \\ \xrightarrow{h} [-\frac{ad-cb}{c}, 0] = [1, 0] \\ \xrightarrow{h} [a, c] \end{array} \begin{array}{l} \xrightarrow{\Psi} \frac{ax+b}{cx+d} \\ \xrightarrow{\Psi} \infty \\ \xrightarrow{\Psi} \begin{cases} \frac{a}{c} & \text{se } c \neq 0 \\ \infty & \text{se } c = 0 \end{cases} \end{array} \quad \text{se } x \neq -\frac{d}{c}$$

Estas expressões reúnem-se na expressão única seguinte:

$$\boxed{x \xrightarrow{h} x' = \frac{ax+b}{cx+d}, \quad x \in \mathbb{k} \cup \{\infty\}, \quad ad - bc \neq 0} \quad (3.6)$$

onde identificamos (como conjuntos) $\mathbb{P}^1 = \mathbb{k} \cup \{\infty\}$ e h com $\Psi \circ h \circ \Psi^{-1}$, e lembrando que $h(-\frac{d}{c}) = \infty$, se $c \neq 0$, e $h(\infty) = \frac{a}{c}$, se $c \neq 0$, ou ∞ , se $c = 0$.

A expressão (3.6) é a expressão usual das homografias em $\mathbb{P}^1 = \mathbb{k} \cup \{\infty\}$.

► **3.8 Involução ...** Uma involução é uma homografia h tal que $h^{-1} = h$.

Se $h(x) = \frac{ax+b}{cx+d}$ então $h^{-1}(x) = \frac{-dx+b}{cx-a}$ e h é uma involução sse $a + d = 0$, isto é, sse o traço da matriz H , que dá origem a h , é nulo.

► **3.9 Pontos fixos (ou duplos) ...** Um número $t \in \widehat{\mathbb{k}}$ diz-se um ponto fixo (ou duplo) de h se $h(t) = t$.

$$h(t) = \frac{at+b}{ct+d} = t \Leftrightarrow ct^2 + (d-a)t - b = 0$$

- se $c = 0$ (e $d \neq 0$) então $h(t) = \frac{a}{d}t + \frac{b}{d}$. Se $a = d$, h é uma translacção e ∞ é um ponto fixo. Se $a \neq d$, $\frac{b}{d-a} \in \mathbb{k}$ é também um ponto fixo.
- Se $c \neq 0$, ∞ não é ponto fixo e estes podem ser calculados como as raízes da equação quadrática $ct^2 + (d-a)t - b = 0$.

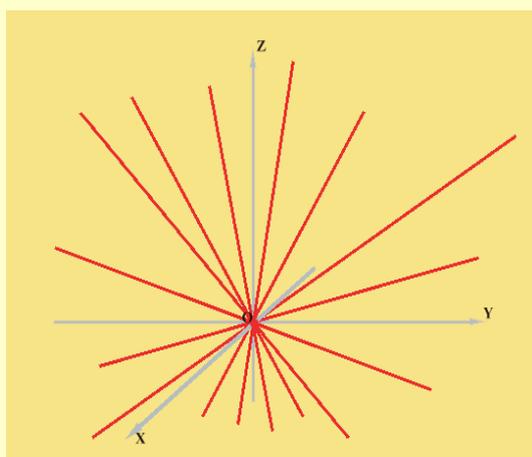
Tópico 4

O plano projectivo \mathbb{P}^2

► **4.1 Plano projectivo \mathbb{P}^2** ... Seja $\mathbb{k} = \mathbb{R}$ ou \mathbb{C} . O **plano projectivo** $\mathbb{P}^2 = \mathbb{P}_{\mathbb{k}}^2$ é, por definição, o conjunto constituído por todas as rectas vectoriais de \mathbb{k}^3 :

$$\mathbb{P}^2 \stackrel{\text{def}}{=} \{ \ell : \ell \text{ é subespaço de dimensão 1 em } \mathbb{k}^3 \} \quad (4.1)$$

Quando $\mathbb{k} = \mathbb{R}$ põe-se $\mathbb{P}_{\mathbb{R}}^2 = \mathbb{P}^2(\mathbb{R})$ para o plano projectivo real, e quando $\mathbb{k} = \mathbb{C}$ põe-se $\mathbb{P}_{\mathbb{C}}^2 = \mathbb{P}^2(\mathbb{C})$ para o plano projectivo complexo.



► **4.2** Temos então uma aplicação natural sobrejectiva:

$$\begin{aligned} \pi : \mathbb{k}^3 - \{0\} &\longrightarrow \mathbb{P}^2 \\ \mathbf{a} &\longmapsto A = \pi(\mathbf{a}) = [\mathbf{a}] \end{aligned} \quad (4.2)$$

onde $[\mathbf{a}] = \mathbb{k}\mathbf{a}$ representa a recta vectorial gerada pelo vector $\mathbf{a} \in \mathbb{k}^3 - \{0\}$. \mathbf{a} diz-se um representante do ponto $A \in \mathbb{P}^2$.

► **4.3 Rectas** ... Uma recta s em \mathbb{P}^2 é um subconjunto da forma $\pi(\mathbf{S})$ onde \mathbf{S} é um plano vectorial de \mathbb{k}^3 .

► **4.4 Coordenadas homogéneas** ... Se $\mathbf{a} = (X, Y, Z) \in \mathbb{k}^3 - \{0\}$, os números X , Y e Z dizem-se as **coordenadas homogéneas** do ponto $A = [\mathbf{a}]$. Escreve-se então:

$$A = [X, Y, Z]$$

ou, por vezes, $(X : Y : Z)$. As coordenadas homogéneas X , Y e Z do ponto $A = [\mathbf{a}]$ estão definidas a menos de um múltiplo escalar não nulo, isto é, λX , λY e λZ , com $\lambda \neq 0$, são também coordenadas homogéneas do ponto $A = [\mathbf{a}]$:

$$A = [X, Y, Z] = [\lambda X, \lambda Y, \lambda Z], \quad \forall \lambda \neq 0$$

Em coordenadas homogéneas X , Y e Z , a equação de uma recta em \mathbb{P}^2 é da forma:

$$aX + bY + cZ = 0 \quad (4.3)$$

Portanto duas rectas distintas em \mathbb{P}^2 intersectam-se sempre num único ponto, uma vez que dois planos vectoriais distintos em \mathbb{k}^3 intersectam-se sempre segundo uma recta vectorial.

► **4.5 Representação paramétrica das rectas** ... Sejam $A = [\mathbf{a}] = [a_1, a_2, a_3]$, $B = [\mathbf{b}] = [b_1, b_2, b_3]$ dois pontos distintos em \mathbb{P}^2 . Como \mathbf{a} e \mathbf{b} são vectores linearmente independentes em \mathbb{k}^3 , qualquer vector do plano por eles gerado é da forma:

$$\mathbf{c} = \lambda \mathbf{a} + \mu \mathbf{b}$$

Portanto qualquer ponto da recta $\ell = AB$ é da forma

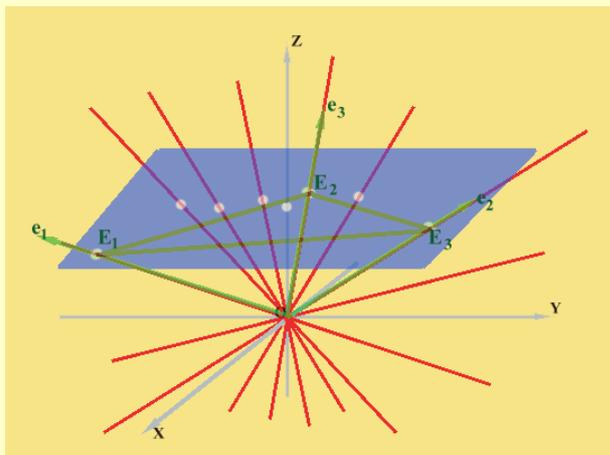
$$C = [\mathbf{c}] = [\lambda \mathbf{a} + \mu \mathbf{b}]$$

onde $\lambda, \mu \in \mathbb{k}$ não são simultaneamente nulos.

Cada ponto da recta ℓ é pois representado por um par de coordenadas homogéneas $[\lambda, \mu]$, relativas aos pontos base A e B , a que correspondem as coordenadas $[1, 0]$ e $[0, 1]$, respectivamente.

Se pômos $t = \mu/\lambda$ então todo o ponto de ℓ , com excepção de B , tem coordenadas homogéneas $\mathbf{a} + t\mathbf{b}$. Se fazemos corresponder B a $t = \infty$ então todo o ponto de ℓ pode ser parametrizado pelo **parâmetro projectivo** $t \in \widehat{\mathbb{k}} = \mathbb{k} \cup \{\infty\}$.

► 4.6 Referenciais projectivos



Fixemos, mais uma vez, uma base $\mathcal{B} = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ para \mathbb{k}^3 . Um sistema de coordenadas homogéneas em \mathbb{P}^2 fica unívocamente determinado pelos 3 pontos $E_1 = [\mathbf{e}_1] = [1, 0, 0]$, $E_2 = [\mathbf{e}_2] = [0, 1, 0]$, $E_3 = [\mathbf{e}_3] = [0, 0, 1]$ e ainda o ponto $U = [\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3] = [1, 1, 1]$, em \mathbb{P}^2 .

Ao conjunto $\mathcal{T} = \{E_1, E_2, E_3\}$ constituído pelos primeiros 3 pontos chama-se o **triângulo de referência de vértices** E_i , e ao ponto $U = [1, 1, 1]$ chama-se o **ponto unidade** (relativamente à base \mathcal{B} inicialmente considerada para \mathbb{k}^3).

► **4.7 Nota** ... Note que os 3 vértices $E_i = [\mathbf{e}_i]$, $i = 1, 2, 3$ do triângulo de referência, onde $\{\mathbf{e}_i\}_{i=1,2,3}$ é a base \mathcal{B} de \mathbb{k}^3 , inicialmente considerada, não são suficientes para determinar as coordenadas homogéneas em \mathbb{P}^2 .

De facto não são suficientes sequer para determinar a base de \mathbb{k}^3 , relativamente à qual se definem as coordenadas homogéneas. Com efeito, $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ e $\{\lambda_1 \mathbf{e}_1, \lambda_2 \mathbf{e}_2, \lambda_3 \mathbf{e}_3\}$, onde $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{k} - \{0\}$, são ambas bases tais que $E_i = [\mathbf{e}_i] = [\lambda_i \mathbf{e}_i]$.

No entanto se essas duas bases atribuem ao ponto unidade U as coordenadas homogéneas $[1, 1, 1]$, então isso significa que:

$$\begin{aligned} U &= \pi(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3) \\ &= \pi(\lambda_1 \mathbf{e}_1 + \lambda_2 \mathbf{e}_2 + \lambda_3 \mathbf{e}_3) \\ &\Rightarrow \lambda_1 \mathbf{e}_1 + \lambda_2 \mathbf{e}_2 + \lambda_3 \mathbf{e}_3 = \lambda(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3), \quad \text{para algum } \lambda \in \mathbb{k} - \{0\} \\ &\Rightarrow \lambda = \lambda_1 = \lambda_2 = \lambda_3 \end{aligned}$$

Isto é, duas bases de \mathbb{k}^3 , $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ e $\{\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3\}$, que sejam determinadas pelos 3 vértices $E_i = \pi(\mathbf{e}_i) = \pi(\mathbf{f}_i)$, $i = 1, 2, 3$, e que atribuam ao ponto U as coordenadas homogéneas $[1, 1, 1]$ - $U = \pi(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3) = \pi(\mathbf{f}_1 + \mathbf{f}_2 + \mathbf{f}_3)$ - são necessariamente proporcionais:

$$\{\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3\} = \{\lambda \mathbf{e}_1, \lambda \mathbf{e}_2, \lambda \mathbf{e}_3\}$$

para algum $\lambda \in \mathbb{k} - \{0\}$.

Se agora $P \in \mathbb{P}^2$ é um ponto cujas coordenadas homogéneas na primeira base são $[X_1, X_2, X_3]$, então

$$\begin{aligned} P &= \pi(X_1 \mathbf{e}_1 + X_2 \mathbf{e}_2 + X_3 \mathbf{e}_3) \\ &= \pi\left(\frac{X_1}{\lambda}(\lambda \mathbf{e}_1) + \frac{X_2}{\lambda}(\lambda \mathbf{e}_2) + \frac{X_3}{\lambda}(\lambda \mathbf{e}_3)\right) \\ &= \pi\left(\frac{X_1}{\lambda} \mathbf{f}_1 + \frac{X_2}{\lambda} \mathbf{f}_2 + \frac{X_3}{\lambda} \mathbf{f}_3\right) \end{aligned} \tag{4.4}$$

e portanto:

$$\left[\frac{X_1}{\lambda}, \frac{X_2}{\lambda}, \frac{X_3}{\lambda}\right]$$

são as coordenadas homogéneas de P relativamente à segunda base. Como

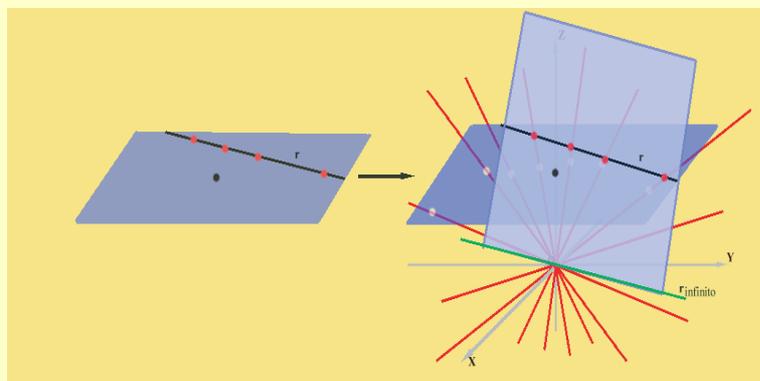
$$[X_1, X_2, X_3] = \left[\frac{X_1}{\lambda}, \frac{X_2}{\lambda}, \frac{X_3}{\lambda}\right]$$

as coordenadas homogéneas de P ficam unívocamente determinadas.

Tópico 5

Fecho Projectivo do plano afim \mathbb{A}^2

► 5.1 Fecho (ou completamento) projectivo



Seja $\mathbb{A}^2 = \mathbb{A}_{\mathbb{k}}^2$ o plano \mathbb{k}^2 , sobre o corpo $\mathbb{k} = \mathbb{R}$ ou \mathbb{C} , com a sua estrutura afim usual. Identifiquemos \mathbb{A}^2 com o hiperplano afim $\{Z = 1\} \subset \mathbb{k}^3$, através de:

$$\begin{aligned} \mathbb{A}^2 &\xrightarrow{\cong} \mathbb{k}^2 \times \{1\} \\ (x, y) &\longrightarrow (x, y, 1) \end{aligned} \quad (5.1)$$

Identificaremos pois o ponto $(x, y) \in \mathbb{A}^2$ com o vector $(x, y, 1) \in \mathbb{k}^3$, e uma qualquer variedade afim $\mathcal{L} \subset \mathbb{A}^2$ com o subconjunto correspondente em \mathbb{k}^3 (não haverá risco de confusão...).

Define-se o fecho (ou completamento) projectivo de \mathbb{A}^2 , como sendo o espaço projectivo:

$$\widehat{\mathbb{A}^2} \stackrel{\text{def}}{=} \mathbb{P}(\mathbb{k}^3) = \mathbb{P}^2 \quad (5.2)$$

Com as convenções atrás referidas, podemos definir uma injeção canónica através de:

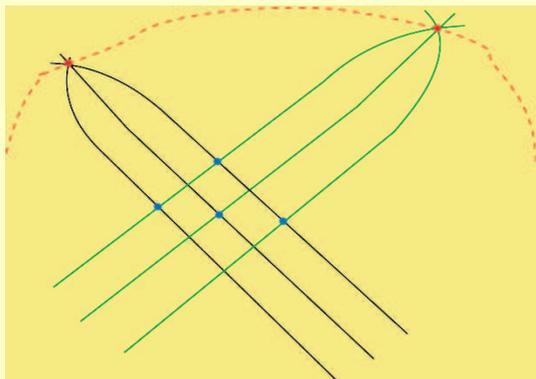
$$\begin{aligned} \mathbb{A}^2 &\hookrightarrow \mathbb{P}^2 \\ (x, y) &\rightarrow \pi(x, y, 1) = [x, y, 1] \end{aligned} \quad (5.3)$$

onde $\pi : \mathbb{k}^3 \rightarrow \mathbb{P}^2$ é a projecção canónica. Esta injeção é a composta de π com a identificação (5.1).

► **5.2 Recta do infinito** ... A imagem de $\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$, pela injeção canónica (5.3), é evidentemente o complementar da recta $Z = 0$ em \mathbb{P}^2 (ou do plano $Z = 0$ em \mathbb{k}^3). Esta recta chama-se a **recta no infinito** de $\widehat{\mathbb{A}^2}$, e nota-se por \mathbb{A}_∞ .

Como conjuntos, o fecho projectivo $\widehat{\mathbb{A}^2}$, do plano afim \mathbb{A}^2 é obtido adicionando a \mathbb{A}^2 os “pontos no infinito” de \mathbb{A}^2 , isto é, os elementos de \mathbb{A}_∞ :

$$\widehat{\mathbb{A}^2} = \mathbb{A}^2 \cup \mathbb{A}_\infty, \quad (\text{como conjuntos})$$



Note que $\mathbb{A}_\infty \cong \mathbb{P}^1 = \mathbb{P}(\mathbb{k}^2 \times \{0\})$ é o conjunto das rectas vectoriais de dimensão 1 no plano $Z = 0$ de \mathbb{k}^3 , ou, de forma equivalente, é o conjunto das direcções das rectas (afins) em \mathbb{A}^2 . De facto, no fecho projectivo, a cada recta afim $r : \{A + \lambda \mathbf{v} : \lambda \in \mathbb{k}\}$ em \mathbb{A}^2 , de direcção \mathbf{v} , adiciona-se o ponto no infinito $r_\infty = [\mathbf{v}] \in \mathbb{A}_\infty$:

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\text{direcções de rectas em } \mathbb{A}^2\}$$

► **5.3 Exemplo ...** Seja $\mathbb{A}^2 = \mathbb{R}^2$, com a sua estrutura afim canónica. Qual é o fecho projectivo \mathbb{R}^2 ?

Por definição:

$$\widehat{\mathbb{R}^2} = \mathbb{P}^2(\mathbb{R})$$

que é exactamente o plano projectivo real. Se (x, y) são as coordenadas usuais em \mathbb{R}^2 , relativamente à base canónica, a injecção canónica (5.3) é dada por:

$$\begin{array}{ccc} \mathbb{R}^2 & \hookrightarrow & \mathbb{R}^2 \times \{1\} \subset \mathbb{R}^3 & \xrightarrow{\pi} & \mathbb{P}^2(\mathbb{R}) \\ (x, y) & \longmapsto & (x, y, 1) & \longmapsto & [x, y, 1] \end{array} \quad (5.4)$$

A recta no infinito é $\mathbb{R}_\infty = \pi(\mathbb{R}^2 \times \{0\}) = \mathbb{P}(\mathbb{R}^2) = \mathbb{P}^1(\mathbb{R}) \cong \mathbb{S}^1$. Como conjuntos, existe portanto uma bijecção entre $\mathbb{P}^2(\mathbb{R})$ e $\mathbb{R}^2 \cup \mathbb{S}^1$.

Seja r uma recta afim em \mathbb{R}^2 de equação:

$$ax + by = c, \quad \text{com } (a, b) \neq \mathbf{0}$$

A direcção desta recta é a do vector $(-b, a) \in \mathbb{R}^2$. Qual é o fecho projectivo \widehat{r} desta recta, em $\mathbb{P}^2(\mathbb{R})$?

Através da identificação $(x, y) \cong (x, y, 1)$, atrás referida, a recta r é identificada com o conjunto dos pontos $(x, y, 1) \in \mathbb{R}^2 \times \{1\}$ tais que $ax + by = c$, que constituem uma recta afim no hiperplano afim $Z = 1$, de \mathbb{R}^3 , que continuamos a designar por r .

Um ponto de $\mathbb{P}^2(\mathbb{R})$ é uma recta vectorial de \mathbb{R}^3 . Esse ponto estará em \widehat{r} se e só se a recta vectorial correspondente intersecta ℓ , digamos num ponto $(x, y, 1)$. Designemos por (X, Y, Z) as coordenadas usuais de \mathbb{R}^3 . A equação da recta vectorial de \mathbb{R}^3 , que passa em $(x, y, 1)$ é:

$$(X, Y, Z) = \lambda(x, y, 1), \quad \lambda \in \mathbb{R}$$

Como $(x, y, 1) \in \ell$, então $ax + by = c$, o que implica que $a\lambda x + b\lambda y = c\lambda$, donde se deduz que:

$$aX + bY = cZ$$

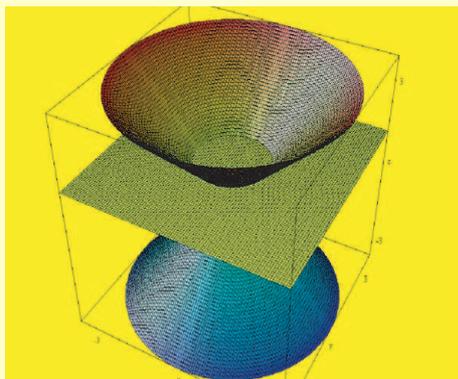
que é exactamente a equação do plano vectorial em \mathbb{R}^3 , que contem r , e é também a equação da recta projectiva \widehat{r} , em coordenadas homogéneas, relativas à base canónica de \mathbb{R}^3 .

Qual é o ponto do infinito r_∞ da recta \widehat{r} ? Por definição $r_\infty = \widehat{r} - r$, é exactamente o ponto de $\mathbb{R}_\infty \cong \mathbb{S}^1$, que corresponde à recta de $\mathbb{R}^2 \times \{0\}$, paralela a ℓ (ver a figura do número anterior). Esta é a recta gerada por $(-b, a, 0)$, que é a intersecção do plano $aX + bY = cZ$ com o plano $Z = 0$. Portanto r_∞ é o ponto de \mathbb{R}_∞ , que, em coordenadas homogéneas, é dado pelo sistema:

$$\begin{cases} aX + bY = cZ \\ Z = 0 \end{cases}$$

isto é, o ponto $[-b, a, 0] \simeq [-b, a] \in \mathbb{R}_\infty$.

► 5.4 Pontos cíclicos. Rectas isotrópicas



Se \mathcal{C} é a circunferência de equação $x^2 + y^2 = 1$, em \mathbb{A}^2 , a sua imagem em \mathbb{P}^2 , calcula-se da mesma forma: um ponto $[X, Y, Z] \in \mathbb{P}^2$ estará em $\widehat{\mathcal{C}}$ se e só se $(X, Y, Z) = \lambda(x, y, 1)$, onde $(x, y, 1) \in \mathcal{C}$, isto é, $x^2 + y^2 = 1$.

Daqui se deduz que $(\lambda x)^2 + (\lambda y)^2 = \lambda^2$ e portanto:

$$X^2 + Y^2 = Z^2$$

que é a equação do fecho projectivo $\widehat{\mathcal{C}}$ de \mathcal{C} , em coordenadas homogéneas.

Por simplicidade de notações continuamos a notar por \mathcal{C} o fecho projectivo $\widehat{\mathcal{C}}$, a que continuamos a chamar a circunferência de equação $X^2 + Y^2 = Z^2$.

Se $\mathbb{k} = \mathbb{R}$, a circunferência \mathcal{C} não tem pontos no infinito. Mas considerando-a como uma curva em $\mathbb{P}^2(\mathbb{C})$, ela tem dois pontos no infinito dados pelo sistema:

$$\begin{cases} X^2 + Y^2 = Z^2 \\ Z = 0 \end{cases}$$

que são os chamados **pontos cíclicos** ou **circulares**:

$$I = [1, i, 0] \quad \text{e} \quad J = [1, -i, 0]$$

em \mathbb{C}_∞ . Note que dada uma “circunferência” do tipo:

$$(X - a)^2 + (Y - b)^2 = r^2 \tag{5.5}$$

em \mathbb{C}^2 , o seu fecho projectivo, em $\mathbb{P}^2(\mathbb{C})$, tem sempre os mesmos dois pontos cíclicos $I = [1, i, 0]$ e $J = [1, -i, 0]$ em \mathbb{C}_∞ ! Com efeito esses pontos são dados pelo sistema:

$$\begin{cases} X^2 - 2aXZ - a^2Z^2 + Y^2 - 2bYZ + b^2Z^2 = r^2Z^2 \\ Z = 0 \end{cases}$$

Toda a recta que passa em I , ou em J , tem por equação homogénea:

$$X \pm iY + \lambda Z = 0$$

Estas rectas dizem-se **isotrópicas** ou **minimais**. Em particular as rectas isotrópicas, que passam no centro (a, b) do círculo (5.5), têm por equação, em coordenadas homogéneas:

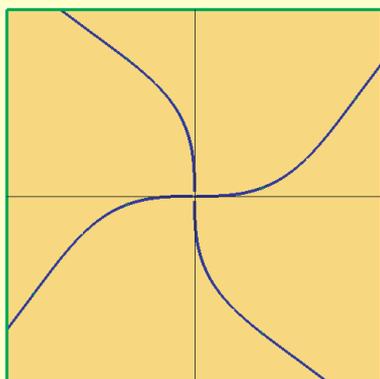
$$\begin{vmatrix} X & Y & Z \\ a & b & 1 \\ 1 & \pm i & 0 \end{vmatrix} = 0 \quad \text{isto é} \quad -iX + Y + (a(\pm i) - b)Z = 0 \tag{5.6}$$

e em coordenadas afins (x, y) (fazendo $X = x, Y = y$ e $Z = 1$, na equação homogénea):

$$y - b = \pm i(x - a) \tag{5.7}$$

Estas rectas são as chamadas **assíptotas** desse círculo.

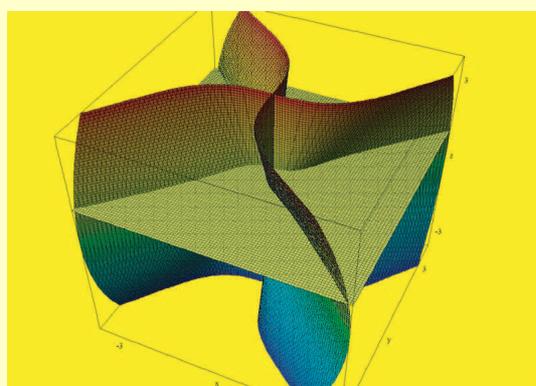
Em particular, se $r = 0$ (círculo de raio nulo), a equação (5.5) reduz-se a (5.7), o que significa que um círculo de raio nulo degenera em duas rectas isotrópicas.

► 5.5 Exemplo ...

Seja $\mathcal{C} \subset \mathbb{A}^2$ a curva (algébrica afim) dada por

$$f(x, y) = x^4 - y^4 - xy = 0$$

Qual o fecho projectivo desta curva, que continuamos a notar por \mathcal{C} , em \mathbb{P}^2 ?



Um ponto $[X, Y, Z] \in \mathbb{P}^2$ estará em \mathcal{C} se e só se $(X, Y, Z) = \lambda(x, y, 1)$, onde $(x, y, 1)$ satisfaz $x^4 - y^4 - xy = 0$.

Daqui se deduz que $(\lambda x)^4 - (\lambda y)^4 - (\lambda x)(\lambda y) = 0$ e portanto:

$$X^4 - Y^4 - XYZ^2 = 0$$

que é a equação do fecho projectivo de \mathcal{C} , em coordenadas homogéneas. Note que esta curva em \mathbb{P}^2 é dada pelo polinómio homogéneo de grau 4:

$$F(X, Y, Z) = X^4 - Y^4 - XYZ^2$$

Os pontos de \mathcal{C}_∞ verificam:

$$\begin{cases} X^4 - Y^4 - XYZ^2 = 0 \\ Z = 0 \end{cases}$$

isto é $X^4 = Y^4$ e $Z = 0$. Se $\mathbb{k} = \mathbb{R}$ os pontos de \mathcal{C}_∞ são $[1, 1, 0]$ e $[1, -1, 0]$.

► 5.6 O complementar da recta $Z = 0$, em \mathbb{P}^2 , é um plano afim. De facto, esse complementar:

$$\mathbb{P}^2 - \{Z = 0\}$$

pode ser posto em correspondência bijectiva com o plano afim $Z = 1$ em \mathbb{k}^3 :

$$\begin{aligned} \mathbb{P}^2 - \{Z = 0\} &\longrightarrow \{Z = 1\} \subset \mathbb{k}^3 \\ [X, Y, Z] &\iff (x = X/Y, y = Y/Z, 1) \end{aligned} \quad (5.8)$$

Portanto \mathbb{P}^2 pode ser considerado como a reunião do plano afim $Z = 1$ em \mathbb{k}^3 , com a recta do infinito $Z = 0$.

► 5.7 Analogamente, o complementar da recta $X = 0$, em \mathbb{P}^2 , é um plano afim. De facto, esse complementar pode ser posto em correspondência bijectiva com o plano afim $X = 1$ em \mathbb{k}^3 :

$$\begin{aligned} \mathbb{P}^2 - \{X = 0\} &\longrightarrow \{X = 1\} \subset \mathbb{k}^3 \\ [X, Y, Z] &\iff (1, y = Y/X, z = Z/X) \end{aligned} \quad (5.9)$$

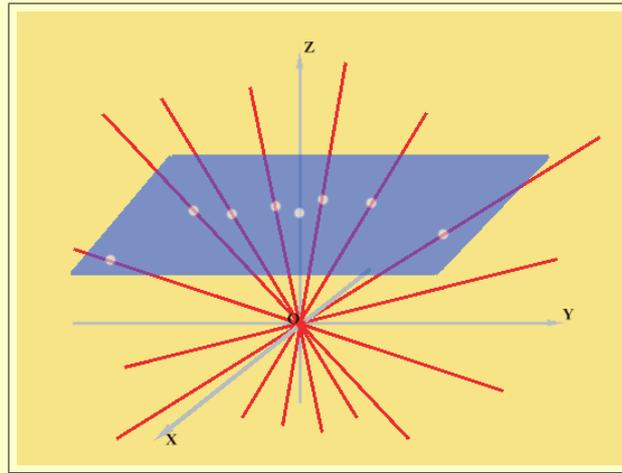


Figura 5.1:

Portanto \mathbb{P}^2 pode ser considerado como a reunião do plano afim $X = 1$ em \mathbb{k}^3 , com a recta do infinito $X = 0$.

Da mesma forma, o complementar da recta $Y = 0$, em \mathbb{P}^2 , é um plano afim. De facto, esse complementar pode ser posto em correspondência bijectiva com o plano afim $Y = 1$ em \mathbb{k}^3 :

$$\begin{aligned} \mathbb{P}^2 - \{Y = 0\} &\longrightarrow \{Y = 1\} \subset \mathbb{k}^3 \\ [X, Y, Z] &\rightleftharpoons (x = X/Y, 1, z = Z/Y) \end{aligned} \quad (5.10)$$

Portanto \mathbb{P}^2 pode ser considerado como a reunião do plano afim $Y = 1$ em \mathbb{k}^3 , com a recta do infinito $Y = 0$.

Mais geralmente o complementar da recta $aX + bY + cZ = 0$, em \mathbb{P}^2 , é um plano afim. Assim, por exemplo, o complementar da recta $X - Y + Z = 0$, em \mathbb{P}^2 , pode ser posto em correspondência bijectiva com o plano afim $X - Y + Z = 1$ em \mathbb{k}^3 :

$$\begin{aligned} \mathbb{P}^2 - \{Z = 0\} &\longrightarrow \{Z = 1\} \subset \mathbb{k}^3 \\ [X, Y, Z] &\rightleftharpoons (X, Y, 1 - X + Y) \end{aligned} \quad (5.11)$$

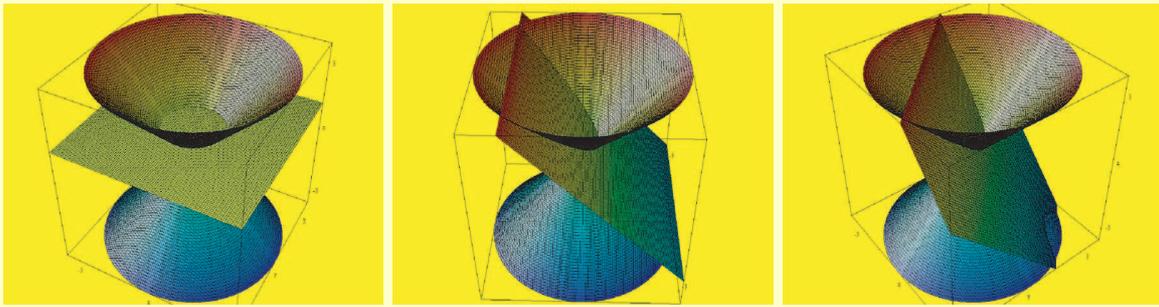
► **5.8 Exemplo ...** Consideremos a cónica $\mathcal{C} = \{F = X^2 + Y^2 - Z^2 = 0\}$ em \mathbb{P}^2 . Como vimos antes, o complementar da recta $Z = 0$, em \mathbb{P}^2 , é um plano afim, que identificamos com o plano afim $Z = 1$ em \mathbb{k}^3 , através da chamada **carta afim** (5.8).

A intersecção de \mathcal{C} com este plano afim diz-se a **vista afim** da cónica \mathcal{C} , correspondente ao plano $Z = 1$. Para obter a equação desta vista afim usamos a (5.8), isto é, pomos $0 = X^2 + Y^2 - Z^2 = (X/Z)^2 + (Y/Z)^2 - 1 = x^2 + y^2 - 1$.

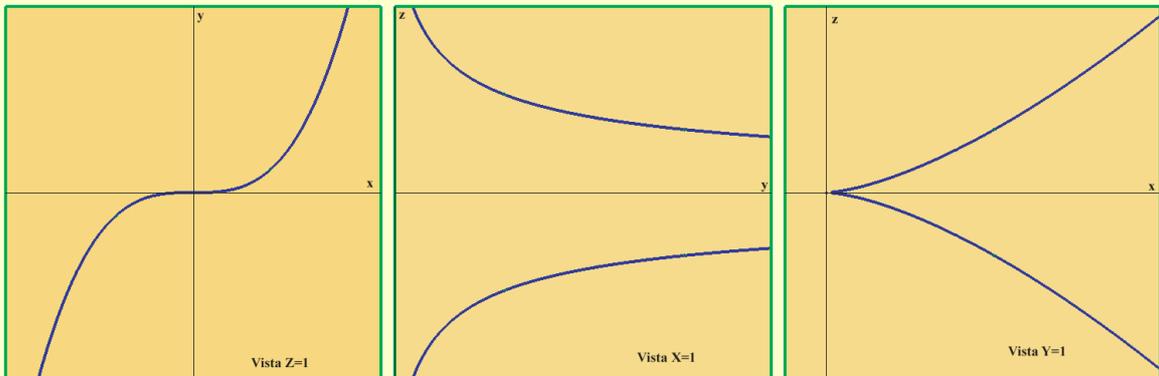
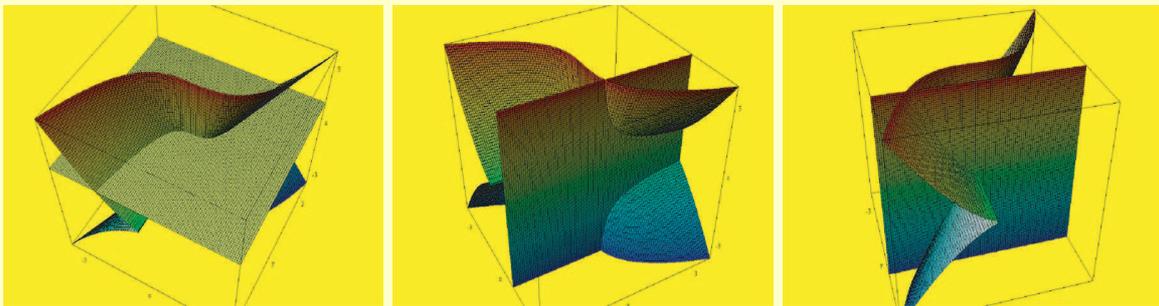
Procedendo de forma análoga para os complementares das rectas $X + Z = 0$ e $X + Y + Z = 0$, obtemos que as vistas afins de \mathcal{C} , correspondentes:

- ao plano $Z = 1$, é a elipse real $x^2 + y^2 = 1$.
- ao plano $X + Z = 1$, é a parábola $y^2 = 1 - 2x$
- ao plano $X + Y + Z = 1$, é a hipérbole $2xy = 2x + 2y - 1$

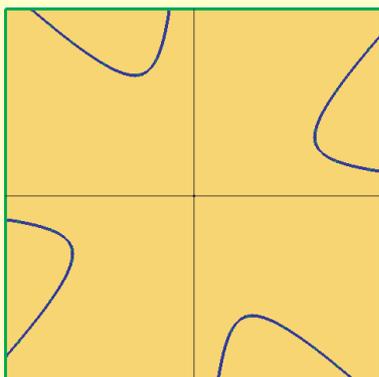
As vistas afins de uma mesma curva projectiva podem pois não ser afim equivalentes.



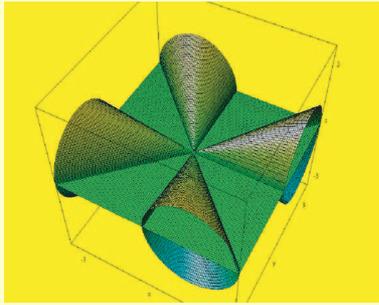
► **5.9 Exemplo ...** Consideremos a cúbica $\mathcal{C} = \{F = YZ^2 - X^3\}$ em \mathbb{P}^2 . As vistas afins correspondentes aos planos $Z = 1, X = 1$ e $Y = 1$, são respectivamente, $f = y - x^3 = 0$, $g = yz^2 - 1 = 0$, e $h = z^2 - x^3 = 0$. Nenhum par destas curvas é afim equivalente.



► **5.10 Exemplo**



A cruz de Maltese é a quártica $f = xy(x^2 - y^2) - (x^2 + y^2) = 0$.

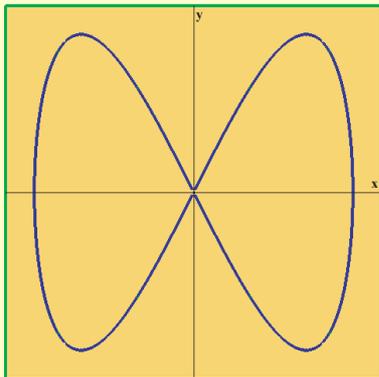


A curva projectiva associada em \mathbb{P}^2 é:

$$F = XY(X^2 - Y^2) - Z^2(X^2 + Y^2)$$

que intersecta a linha do infinito $Z = 0$ quando $XY(X^2 - Y^2) = 0$. Obtemos portanto os pontos do infinito $[0, 1, 0]$, $[1, 0, 0]$, $[1, 1, 0]$ e $[1, -1, 0]$, respectivamente nas rectas $X = 0$, $Y = 0$, $Y = X$ e $Y = -X$.

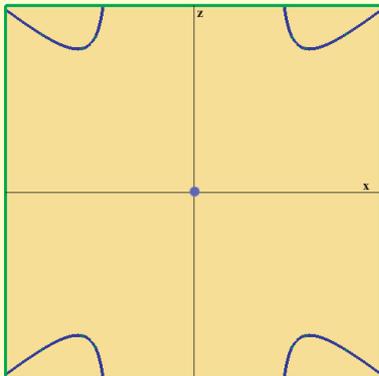
► 5.11 Exemplo



O fecho projectivo da curva $f(x, y) = y^2 - x^2 + x^4$, a "figura oito", é a curva:

$$F(X, Y, Z) = Y^2 Z^2 - X^2 Z^2 + X^4$$

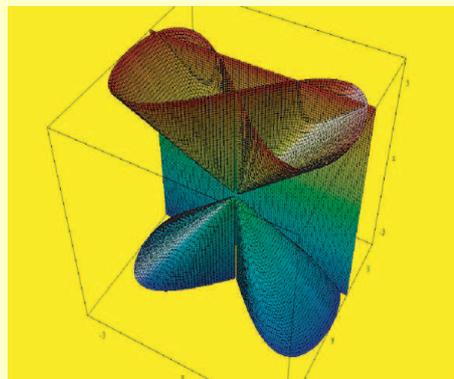
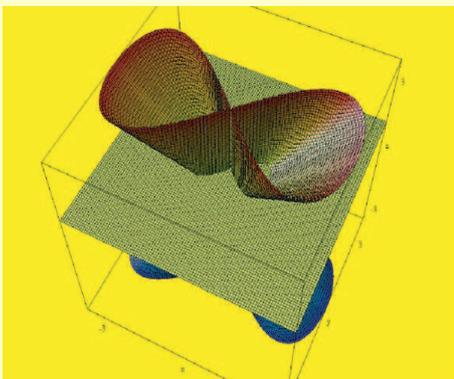
que intersecta a linha do infinito $Z = 0$, quando $X^4 = 0$, isto é, no ponto $A = [0, 1, 0]$.



A vista afim desta curva, correspondente ao plano $Y = 1$, é a curva:

$$g(x, z) = z^2 - x^2 z^2 + x^4$$

Nesta vista o ponto A corresponde à origem do plano (X, Z) , que é um ponto isolado da curva $g = 0$!



► 5.12 Projectividades ou homografias ... Consideremos uma aplicação linear bijectiva:

$$H : \mathbb{k}^3 \rightarrow \mathbb{k}^3$$

e a aplicação induzida $h : \mathbb{P}^2 \rightarrow \mathbb{P}^2$, definida por:

$$\begin{array}{ccc} \mathbb{k}^3 & \xrightarrow{H} & \mathbb{k}^3 \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{P}^2 & \xrightarrow{h=\mathbb{P}(H)} & \mathbb{P}^2 \end{array}$$

A aplicação h diz-se uma **transformação projectiva** ou uma **homografia**.

Uma aplicação projectiva (ou homografia) de \mathbb{A}^2 , é, por definição, uma homografia do fecho projectivo $\widehat{\mathbb{A}^2} = \mathbb{P}^2$.

Como sabemos:

$$\widehat{\mathbb{A}^2} = \mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{A}_\infty$$

onde a recta do infinito \mathbb{A}_∞ é a recta $Z = 0$.

Consideremos a matriz da transformação linear $H : \mathbb{k}^3 \rightarrow \mathbb{k}^3$, relativamente à base canónica:

$$\mathbf{H} = \left[\begin{array}{cc|c} a_{11} & a_{12} & c_1 \\ a_{21} & a_{22} & c_2 \\ \hline d_1 & d_2 & e \end{array} \right] = \left[\begin{array}{c|c} \mathbf{A} & \mathbf{c} \\ \hline \mathbf{d}^t & e \end{array} \right] \quad (5.12)$$

A sua acção num vector da forma $\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{x} \\ 1 \end{pmatrix} \in \mathbb{A}^2$ é:

$$\left[\begin{array}{c|c} \mathbf{A} & \mathbf{c} \\ \hline \mathbf{d}^t & e \end{array} \right] \begin{pmatrix} \mathbf{x} \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{Ax} + \mathbf{c} \\ \mathbf{d}^t \mathbf{x} + e \end{pmatrix}$$

Isto é, a homografia de $\widehat{\mathbb{A}^2} = \mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{A}_\infty$, pode ser representada na forma:

$$h : \mathbf{x} \mapsto \frac{1}{\mathbf{d}^t \mathbf{x} + e} (\mathbf{Ax} + \mathbf{c}) \quad (5.13)$$

e é a composição de:

- Uma transformação linear inversível $\mathbf{x} \mapsto \mathbf{Ax}$.
- uma translacção $\mathbf{x} \mapsto \mathbf{x} + \mathbf{c}$
- uma inversão $\mathbf{x} \mapsto \frac{\mathbf{x}}{\mathbf{d}^t \mathbf{x} + e}$

► **5.13 Teorema** ... Sejam A, B, C, D e A', B', C', D' dois referenciais projectivos para \mathbb{P}^2 . Então existe uma e uma só transformação projectiva $h : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ tal que $h(A) = A', h(B) = B', h(C) = C', h(D) = D'$.

Dem.: Levantemos A, B, C a uma base $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ de \mathbb{k}^3 , tal que $\pi(\mathbf{a} + \mathbf{b} + \mathbf{c}) = D$ e, análogamente levantemos A', B', C' a uma base $\{\mathbf{a}', \mathbf{b}', \mathbf{c}'\}$ de \mathbb{k}^3 , tal que $\pi(\mathbf{a}' + \mathbf{b}' + \mathbf{c}') = D'$.

Se h existe e é induzida por uma aplicação linear $H : \mathbb{k}^3 \rightarrow \mathbb{k}^3$, então $H(\mathbf{a})$ deverá ser da forma $H(\mathbf{a}) = \lambda \mathbf{a}'$, com $\lambda \neq 0$, e analogamente, $H(\mathbf{b}) = \eta \mathbf{b}'$, $H(\mathbf{c}) = \nu \mathbf{c}'$. Como $h(D) = D'$, o vector $H(\mathbf{a} + \mathbf{b} + \mathbf{c})$ pode ser escrito na forma $\mu(\mathbf{a}' + \mathbf{b}' + \mathbf{c}')$. Mas isto implica que $\lambda = \eta = \nu = \mu$, isto é, H fica determinada a menos da multiplicação por $\mu \in \mathbb{k} - \{0\}$, isto é, $h = \mathbb{P}(H)$ fica univocamente determinada.

Por outro lado, a existência de h é clara - basta defini-la através de $H : \mathbb{k}^3 \rightarrow \mathbb{k}^3$ com $H(\mathbf{a}) = \mathbf{a}'$, $H(\mathbf{b}) = \mathbf{b}'$, $H(\mathbf{c}) = \mathbf{c}'$.

► **5.14 Corolário** ... Sejam A, B, C e U quatro pontos independentes em \mathbb{P}^2 , isto é, 3 quaisquer desses pontos não são colineares. Então existe uma e uma só projectividade $h : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ tal que:

$$h[1, 0, 0] = A, \quad h[0, 1, 0] = B, \quad h[0, 0, 1] = C, \quad h[1, 1, 1] = U \quad (5.14)$$

Dem.: Suponhamos que $A = [\mathbf{a}]$, $B = [\mathbf{b}]$, $C = [\mathbf{c}]$ e $U = [\mathbf{u}]$. Como A, B, C não são colineares os vectores \mathbf{a}, \mathbf{b} e \mathbf{c} são linearmente independentes e formam, portanto, uma base de \mathbb{k}^3 .

Em particular:

$$\mathbf{u} = \lambda \mathbf{a} + \mu \mathbf{b} + \nu \mathbf{c}$$

onde $\lambda, \mu, \nu \in \mathbb{k}$ são não nulos (se, por exemplo, $\lambda = 0$, U, B e C seriam colineares).

Basta pôr então:

$$H = \begin{bmatrix} \lambda a_1 & \mu b_1 & \nu c_1 \\ \lambda a_2 & \mu b_2 & \nu c_2 \\ \lambda a_3 & \mu b_3 & \nu c_3 \end{bmatrix}$$

onde $\mathbf{a} = (a_1, a_2, a_3)$, $\mathbf{b} = (b_1, b_2, b_3)$, $\mathbf{c} = (c_1, c_2, c_3)$.

Esta aplicação h permite efectuar uma mudança de coordenadas homogéneas em \mathbb{P}^2 , de tal forma que o novo triângulo de referência seja constituído pelos pontos A, B e C .

Como $h^{-1}(A) = [1, 0, 0]$, $h^{-1}(B) = [0, 1, 0]$ e $h^{-1}(C) = [0, 0, 1]$ as novas coordenadas de um ponto qualquer $P \in \mathbb{P}^2$ são as coordenadas originais usuais de $h^{-1}(P)$.

► **5.15 Exemplo** ... Considere a hipérbole equilátera:

$$xy = 1$$

Em \mathbb{P}^2 , é definida pela equação:

$$XY - Z^2 = 0$$

A linha do infinito $Z = 0$ intersecta-a quando $XY = 0$, isto é, nos pontos $A = [1, 0, 0]$ e $B = [0, 1, 0]$, das rectas $Y = 0$ e $X = 0$, respectivamente.

Mas podemos olhar para a hipérbole de forma diferente. Para isso escrevemo-la como soma de quadrados, completando os quadrados:

$$\left(\frac{1}{2}(X+Y)\right)^2 - \left(\frac{1}{2}(X-Y)\right)^2 - Z^2 = 0$$

Consideremos a projectividade:

$$X' = X - Y, \quad Y' = 2Z, \quad Z' = X + Y$$

que transforma a hipérbole em $(X')^2 + (Y')^2 - (Z')^2 = 0$, ou ainda, omitindo os acentos:

$$X^2 + Y^2 - Z^2 = 0$$

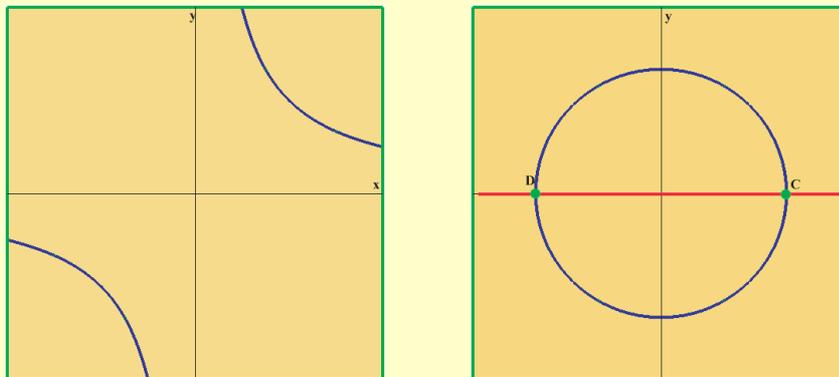
A vista afim desta cónica, correspondente ao plano $Z = 1$, é o círculo:

$$x^2 + y^2 = 1$$

Por outro lado, a projectividade anterior transforma a recta do infinito $Z = 0$ na recta $Y = 0$, e os pontos $A = [1, 0, 0]$ e $B = [0, 1, 0]$ nos pontos $C = [1, 0, 1]$ e $D = [-1, 0, 1]$. A vista afim da

recta $Y = 0$, correspondente ao plano $Z = 1$, é a recta $y = 0$, enquanto que as vistas afins dos pontos C e D , correspondente ao plano $Z = 1$, são os pontos $(1, 0)$ e $(-1, 0)$. Estes pontos são os pontos de intersecção do círculo $x^2 + y^2 = 1$ com a recta $y = 0$.

A projectividade permite pois olhar para os dois ramos da hipérbole como dois semi-círculos um de cada lado da linha do infinito.



Tópico 6

Dualidade no plano

► **6.1 Dualidade no plano** ... Nesta secção designamos por $\mathbb{P}^2 = \mathbb{P}_{\mathbb{k}}^2$ o plano projectivo sobre $\mathbb{k} = \mathbb{R}$ ou \mathbb{C} e por $(\mathbb{P}^2)^* = \mathbb{P}((\mathbb{k}^3)^*)$ o plano dual, isto é, o espaço projectivo cujos pontos são as rectas vectoriais do espaço dual $(\mathbb{k}^3)^*$ das formas lineares (vectores-linha) em \mathbb{k}^3 .

A cada ponto $A = [\mathbf{a}] \in \mathbb{P}^2$ associamos a recta $a = [\mathbf{a}^\perp]$ de $(\mathbb{P}^2)^*$, onde \mathbf{a}^\perp representa o plano de $(\mathbb{k}^3)^*$ constituído por todos os vectores-linha (formas lineares em \mathbb{k}^3) que se anulam em \mathbf{a} .

Em coordenadas homogéneas X, Y, Z para \mathbb{P}^2 e U, V, W para $(\mathbb{P}^2)^*$, se $A = [X, Y, Z]$ então a recta a , em $(\mathbb{P}^2)^*$, tem por equação:

$$XU + YV + ZW = 0 \quad (6.1)$$

Nesta equação X, Y, Z estão fixos (a menos da multiplicação por um escalar não nulo) e os U, V, W variam.

A cada recta $s = [\mathbf{S}] \in \mathbb{P}^2$ associamos o ponto $S = [\mathbf{S}^\perp]$ de $(\mathbb{P}^2)^*$, onde \mathbf{S}^\perp representa a recta vectorial de $(\mathbb{k}^3)^*$ constituída por todos os vectores-linha (formas lineares em \mathbb{k}^3) que se anulam em \mathbf{S} .

Em coordenadas homogéneas X, Y, Z para \mathbb{P}^2 , se s tem por equação $UX + VY + WZ = 0$ então $S = [U, V, W] \in (\mathbb{P}^2)^*$. Aqui os U, V, W estão fixos (a menos da multiplicação por um escalar não nulo) e os X, Y, Z variam.

► **6.2** ... Identifiquemos $(\mathbb{P}^2)^*$ com $\mathcal{R}(\mathbb{P}^2) = \{\text{conjunto de todas as rectas projectivas de } \mathbb{P}^2\}$, através de:

$$[\alpha] \longleftrightarrow [\ker \alpha]$$

Comecemos com um ponto $A \in \mathbb{P}^2$. Associemos-lhe a recta dual $a \in \mathcal{R}((\mathbb{P}^2)^*)$. Cada ponto desta recta é representado por uma forma linear α que, com a identificação anterior, corresponde a uma recta em \mathbb{P}^2 . Ao ponto A corresponde então uma família de rectas $\mathcal{F}(A)$, em \mathbb{P}^2 , todas elas passando pelo ponto A :

$$A = [\mathbf{a}] \longleftrightarrow a = [\mathbf{a}^\perp] = [\{\alpha : \alpha(\mathbf{a}) = 0\}] \longleftrightarrow \mathcal{F}(A) = \{[\ker \alpha] : \alpha(\mathbf{a}) = 0\}$$

a que se dá o nome de **feixe de rectas**, em \mathbb{P}^2 , de **suporte** A .

Assim, por exemplo, ao ponto $A = [1, -3, 2] \in \mathbb{P}^2$, corresponde a recta a em $(\mathbb{P}^2)^*$, de equação $U - 3V + 2W = 0$. A cada ponto $[\alpha] = [U, V, W]$ desta recta de $(\mathbb{P}^2)^*$, está associada uma recta em \mathbb{P}^2 , de equação $UX + VY + WZ = 0$. A equação:

$$U - 3V + 2W = 0 \quad (6.2)$$

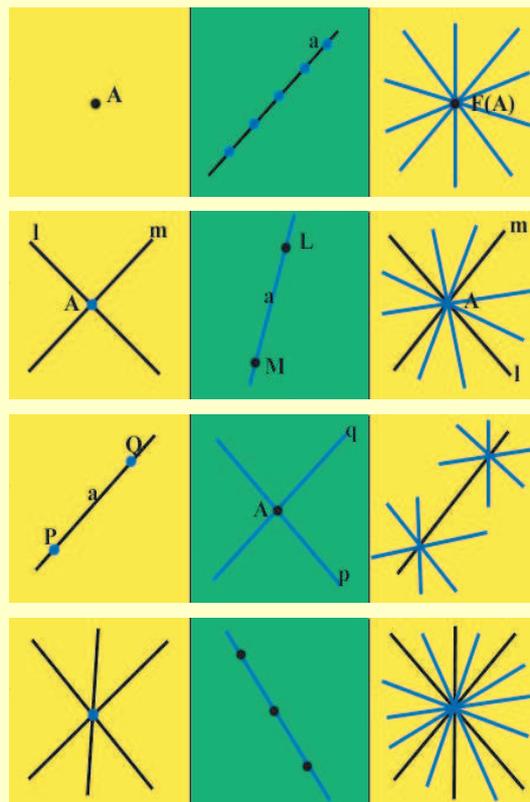
diz que estas rectas, obtidas fazendo variar $[\alpha] = [U, V, W]$, passam todas pelo ponto $A = [1, -3, 2]$.

A equação (6.2) diz-se por isso, a **equação do feixe $\mathcal{F}(A)$** ou, por vezes, a **equação tangencial** do ponto A .

► **6.3 Princípio de dualidade projectiva ...** “Se num enunciado relativo a relações de inclusão de pontos e rectas no plano projectivo \mathbb{P}^2 , substituirmos ponto por recta e todas as inclusões forem invertidas, obtemos um enunciado válido em \mathbb{P}^2)* sse o primeiro o fôr em \mathbb{P}^2 ”.

Dualidade Projectiva no plano

Plano \mathbb{P}^2		Plano dual \mathbb{P}^2)*		Plano \mathbb{P}^2
Ponto A	\leftrightarrow	Recta a	\leftrightarrow	Feixe de rectas $\mathcal{F}(A)$
Recta ℓ	\leftrightarrow	Ponto L	\leftrightarrow	Recta ℓ
Ponto A intersecção de duas rectas ℓ, m	\leftrightarrow	Recta a que une dois pontos L, M	\leftrightarrow	Feixe $\mathcal{F}(A)$ gerado por duas rectas ℓ, m
Recta a que une dois pontos P, Q	\leftrightarrow	Ponto A intersecção das duas rectas p, q	\leftrightarrow	Recta a comum aos dois feixes $\mathcal{F}(P)$ e $\mathcal{F}(Q)$
Três rectas a, b, c intersectam-se num ponto P	\leftrightarrow	Três pontos A, B, C estão alinhados na recta p	\leftrightarrow	Três rectas a, b, c pertencem ao feixe $\mathcal{F}(P)$



► **6.4 Razão anarmónica de quatro rectas concorrentes ...** O dual do conceito de razão anarmónica de quatro pontos colineares é o conceito de razão anarmónica de quatro rectas concorrentes. Se $p = [\mathbf{p}]$, $q = [\mathbf{q}]$, $r = [\mathbf{r}]$ e $s = [\mathbf{s}]$ são quatro rectas concorrentes, com coordenadas de linhas homogêneas $\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s} \in (\mathbb{k}^3)^*$, pômos:

$$\mathbf{r} = \lambda_1 \mathbf{p} + \lambda_2 \mathbf{q}, \quad \mathbf{s} = \mu_1 \mathbf{p} + \mu_2 \mathbf{q}$$

e definimos a razão anarmónica das quatro rectas concorrentes p, q, r, s através de:

$$(pqrs) \stackrel{\text{def}}{=} \frac{\lambda_2}{\lambda_1} : \frac{\mu_2}{\mu_1} \quad (6.3)$$

► **6.5** Se $A = [\mathbf{a}]$ e $B = [\mathbf{b}]$ são dois pontos em \mathbb{P}^2 , a equação da recta AB que os une é:

$$\begin{vmatrix} X & Y & Z \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = 0 \quad (6.4)$$

isto é:

$$(\mathbf{a} \wedge \mathbf{b}) \cdot \mathbf{x} = 0 \quad (6.5)$$

Portanto as coordenadas da recta AB são $\mathbf{a} \wedge \mathbf{b}$, onde \wedge representa o produto vectorial usual em \mathbb{R}^3 . Dualmente, se $p = [\mathbf{p}]$, $q = [\mathbf{q}]$ são duas rectas, as coordenadas do seu ponto de intersecção são $\mathbf{p} \wedge \mathbf{q}$.

► **6.6** Sejam $A = [\mathbf{a}]$, $B = [\mathbf{b}]$, $C = [\mathbf{c}]$ e $D = [\mathbf{d}]$ quatro pontos colineares em \mathbb{P}^2 , e P um outro ponto não pertencente à recta AB . Se $\mathbf{c} = \lambda_1 \mathbf{a} + \lambda_2 \mathbf{b}$ e $\mathbf{d} = \mu_1 \mathbf{a} + \mu_2 \mathbf{b}$, então:

$$(ABCD) = \frac{\lambda_2}{\lambda_1} : \frac{\mu_2}{\mu_1}$$

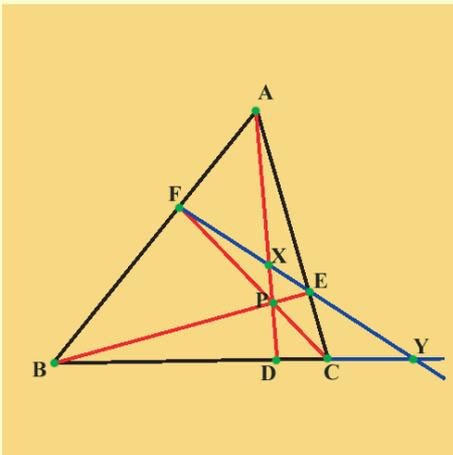
As coordenadas das rectas PA, PB, PC e PD são, respectivamente, $\mathbf{p} \wedge \mathbf{a}$, $\mathbf{p} \wedge \mathbf{b}$, $\mathbf{p} \wedge \mathbf{c}$ e $\mathbf{p} \wedge \mathbf{d}$. Mas:

$$\begin{aligned} \mathbf{p} \wedge \mathbf{c} &= \mathbf{p} \wedge (\lambda_1 \mathbf{a} + \lambda_2 \mathbf{b}) = \lambda_1 (\mathbf{p} \wedge \mathbf{a}) + \lambda_2 (\mathbf{p} \wedge \mathbf{b}) \\ \mathbf{p} \wedge \mathbf{d} &= \mathbf{p} \wedge (\mu_1 \mathbf{a} + \mu_2 \mathbf{b}) = \mu_1 (\mathbf{p} \wedge \mathbf{a}) + \mu_2 (\mathbf{p} \wedge \mathbf{b}) \end{aligned} \quad (6.6)$$

e portanto:

$$(pqrs) = \frac{\lambda_2}{\lambda_1} : \frac{\mu_2}{\mu_1} = (ABCD)$$

► **6.7 Exemplo ...**



Considere um triângulo $\triangle(ABC)$ e os pontos $D \in BC, E \in CA$ e $F \in AB$, de tal forma que as rectas AD, BE e CF se intersectam num ponto P . Sejam ainda $X = EF \cap AD$ e $Y = EF \cap BC$. Mostrar que $(BCDY) = -1$.

Usando o triângulo $\triangle(ABC)$ como triângulo de referência, e P como ponto unidade, então, $A = [1, 0, 0]$, $B = [0, 1, 0]$, $C = [0, 0, 1]$ e $P = [1, 1, 1]$. Calculando temos que:

- as coordenadas da recta AP são $(1, 0, 0) \wedge (1, 1, 1) = (0, -1, 1)$ e portanto é a recta de equação $-Y + Z = 0$.

- as coordenadas da recta BC são $(0, 1, 0) \wedge (0, 0, 1) = (1, 0, 0)$ e portanto é a recta de equação $X = 0$.

- as rectas AP e BC intersectam-se em D que portanto tem coordenadas $(0, -1, 1) \wedge (1, 0, 0) = (0, 1, 1)$.

Analogamente se calcula que as coordenadas de Y são $[0, 1, -1]$. Como $(0, 1, 1) = (0, 1, 0) + (0, 0, 1)$ e $(0, -1, 1) = (0, 1, 0) - (0, 0, 1)$ vem que:

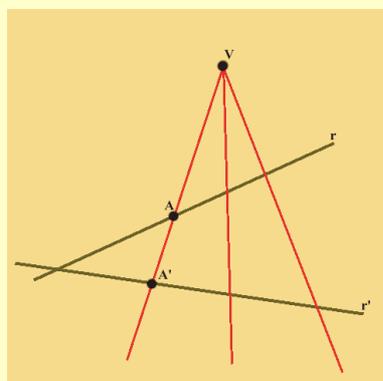
$$(BCDY) = 1/1 : 1/ -1 = -1$$

como se pretendia.

Tópico 7

Teoremas de Desargues e Pappus

► 7.1 Projectões de rectas ...

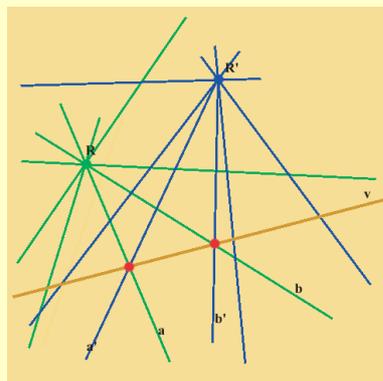


Sejam r e r' duas rectas distintas em \mathbb{P}^2 e V um ponto não pertencente a qualquer delas. A aplicação:

$$\begin{aligned} \pi : r &\longrightarrow r' \\ A &\longmapsto A' = VA \cap r' \end{aligned} \quad (7.1)$$

chama-se uma projectão de r sobre r' de centro V . Diz-se ainda que as pontuais r e r' estão em perspectiva de centro (ou ponto de vista) V .

► 7.2 Projectões de feixes ...



Sejam $\mathcal{F}(R)$ e $\mathcal{F}(R')$ dois feixes distintos, com suportes $R \neq R'$, em \mathbb{P}^2 , e v uma recta não pertencente a qualquer deles: $v \neq RR'$. A aplicação:

$$\begin{aligned} \pi : \mathcal{F}(R) &\longrightarrow \mathcal{F}(R') \\ a &\longmapsto a' = av \vee R' \end{aligned} \quad (7.2)$$

onde $av = a \cap v$, chama-se uma projectão de $\mathcal{F}(R)$ sobre $\mathcal{F}(R')$ de eixo v . Diz-se ainda que os dois feixes $\mathcal{F}(R)$ e $\mathcal{F}(R')$ estão em perspectiva de eixo v .

► **7.3 Teorema ...** *Uma homografia entre duas rectas distintas do plano é uma projectão se e só se o ponto de intersecção dessas duas rectas é transformado em si próprio.*

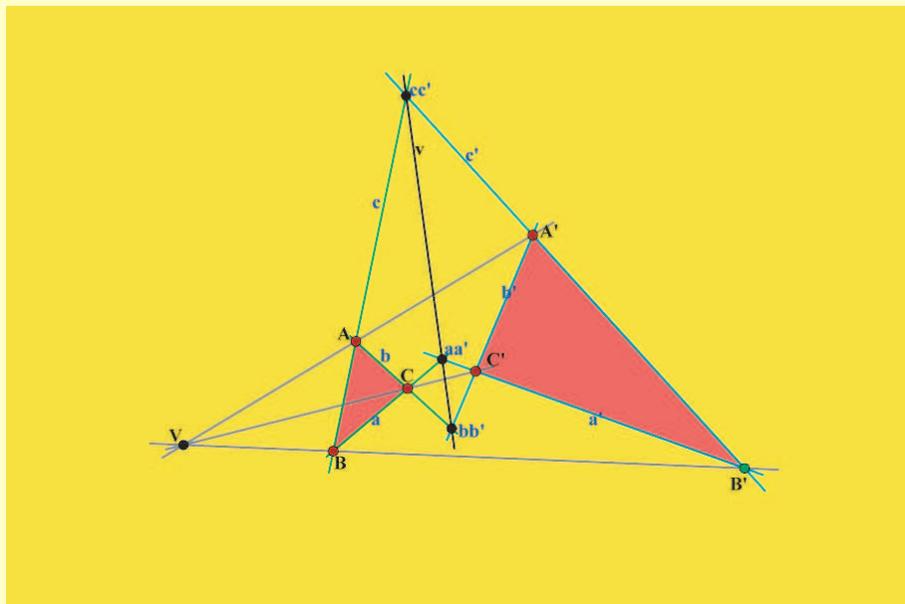
Dem.: Se $h : r \rightarrow r'$ é uma projectão, e $I = r \cap r'$, é claro que $h(I) = I$.

Reciprocamente, seja $h : r \rightarrow r'$ uma homografia tal que $h(I) = I$. Consideremos dois pontos distintos quaisquer $A, B \in r$, diferentes de I , as suas imagens $A' = h(A), B' = h(B) \in r'$ e a projectão $\pi : r \rightarrow r'$ de centro $V = AA' \cap BB'$. Como $\pi(A) = A', \pi(B) = B'$ e $\pi(I) = I$, deduzimos que $\pi \equiv h$.

► **7.4 Teorema dual ...** *Uma homografia entre dois feixes distintos $\mathcal{F}(R)$ e $\mathcal{F}(R')$ do plano é uma projectão se e só se a recta RR' é transformada em si própria.*

► **7.5 Triângulos em perspectiva** ... Dois triângulos no plano, ABC e $A'B'C'$, tendo os vértices e lados distintos, dizem-se que estão em perspectiva de centro V , se as rectas AA' , BB' e CC' , que unem os vértices homólogos, concorrem todas num ponto V .

Dualmente, dois triângulos no plano, abc e $a'b'c'$, tendo os vértices e lados distintos, dizem-se que estão em perspectiva de eixo v , se os pontos aa' , bb' e cc' , de intersecção dos lados homólogos, pertencem todos à recta v .



► **7.6 Teorema de Desargues** ... *Dois triângulos no plano, tendo os vértices e lados distintos, estão em perspectiva de centro V , se e só se estão em perspectiva de eixo v .*

Dem.: No triângulo ABC , os pontos A, B e C são os vértices e $a = BC$, $b = AC$, $c = AB$ os lados. O mesmo para o triângulo $A'B'C'$. aa' representa o ponto de intersecção dos lados a e a' , respectivamente dos triângulos ABC e $A'B'C'$, e analogamente para bb' e cc' .

Suponhamos então que as rectas AA' , BB' e CC' são concorrentes num ponto V . A homografia:

$$h : AA' \longrightarrow CC'$$

é a composta de duas projecções - a projecção $\pi_1 : AA' \rightarrow BB'$, de centro cc' com a projecção $\pi_2 : BB' \rightarrow CC'$, de centro aa' . Estas duas projecções enviam V em si próprio e, portanto, o mesmo acontece com h . Logo, pelo teorema anterior, h é também uma projecção. Como $h(A) = C$ e $h(A') = C'$, concluímos que o centro da projecção h é o ponto $bb' = AC \cap A'C'$.

Resta mostrar que bb' pertence à recta definida por cc' e aa' . Para isso, consideremos a recta $v = bb' \vee cc'$ e os pontos $Q = v \cap AA'$ e $Q' = v \cap CC'$. É claro que $h(Q) = Q'$, e, portanto, $v = QQ'$ passa também por cc' que é o centro da projecção h . Logo aa', bb' e cc' pertencem todos à recta v , como se pretendia mostrar.

O recíproco do teorema obtém-se por dualização - o teorema de Desargues é auto-dual!

► **7.7 Outra demonstração do Teorema de Desargues** ...

Seja V o ponto comum de intersecção das 3 rectas AA', BB' e CC' . Como V, A e A' são colineares e são distintos, podemos encontrar vectores representativos \mathbf{v}, \mathbf{a} e \mathbf{a}' , coplanares em \mathbb{K}^3 , tais que:

$$\mathbf{v} = \mathbf{a} + \mathbf{a}'$$

Analogamente, podemos encontrar vectores representativos \mathbf{b}, \mathbf{b}' , de B, B' , e \mathbf{c}, \mathbf{c}' , de C, C' , tais que:

$$\mathbf{v} = \mathbf{b} + \mathbf{b}', \quad \text{e} \quad \mathbf{v} = \mathbf{c} + \mathbf{c}'$$

Daqui se conclui que:

$$\mathbf{a} + \mathbf{a}' = \mathbf{b} + \mathbf{b}', \quad \mathbf{b} + \mathbf{b}' = \mathbf{c} + \mathbf{c}', \quad \mathbf{a} + \mathbf{a}' = \mathbf{c} + \mathbf{c}'$$

e ainda:

$$\begin{aligned} \mathbf{a} - \mathbf{b} &= \mathbf{b}' - \mathbf{a}' = \mathbf{p} && \text{é um vector representativo de } P = AB \cap A'B' \\ \mathbf{b} - \mathbf{c} &= \mathbf{c}' - \mathbf{b}' = \mathbf{q} && \text{é um vector representativo de } Q = BC \cap B'C' \\ \mathbf{a} - \mathbf{c} &= \mathbf{c}' - \mathbf{a}' = \mathbf{r} && \text{é um vector representativo de } R = CA \cap C'A' \end{aligned}$$

Finalmente:

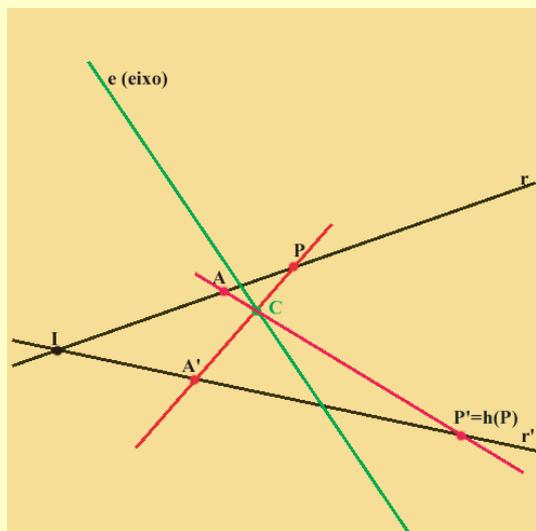
$$\mathbf{p} + \mathbf{q} + \mathbf{r} = \mathbf{a} - \mathbf{b} + \mathbf{b} - \mathbf{c} + \mathbf{c} - \mathbf{a} = \mathbf{0}$$

e os vectores $\mathbf{p}, \mathbf{q}, \mathbf{r}$ são coplanares o que significa que os pontos P, Q e R são colineares.

□.

Dois triângulos dizem-se **perspectivos** quando as rectas que unem os vértices homólogos concorrem todas num mesmo ponto (o centro da perspectiva). O teorema de Desargues pode enunciar-se na forma “os pontos de intersecção dos lados homólogos de dois triângulos perspectivos estão sobre uma mesma recta (recta arguesiana)”.

► 7.8 Homografias entre duas rectas no plano ...



Sejam r e r' duas rectas distintas em \mathbb{P}^2 e $I = r \cap r'$ o seu ponto de intersecção.

Consideremos dois pontos, $A \in r$ e $A' \in r'$, ambos distintos de I , e ainda um outra recta e que não passe por I .

A cada ponto $P \in r$, associemos o ponto $P' = h(P) \in r'$, construído pelo processo seguinte:

- unimos P com A'
- determinamos a intersecção C da recta PA' com o eixo e
- unimos A com C e determinamos P' como sendo a intersecção da recta AC com r' .

Por outras palavras, primeiro projectamos a recta r sobre o eixo e , a partir do centro A' , e depois projectamos o eixo e sobre a recta r' , a partir do centro A . Sendo a composta de duas perspectivas, a aplicação h é uma homografia (preserva a razão anarmónica).

► **7.9 Teorema** ... (i). Toda a homografia $h : r \rightarrow r'$ pode ser obtida pelo processo acima indicado, a partir de um par de pontos homólogos (A, A') , ambos diferentes de $I = r \cap r'$, e de uma recta e que não passa nem por A nem por A' .

(ii). A recta e depende apenas de h e não do par (A, A') . Em particular se (A, A') e (B, B') são dois pares de pontos homólogos as rectas AB' e $A'B$ intersectam-se sobre e .

A recta e diz-se o **eixo** da homografia h .

Dem.: 1. Suponhamos que $h(I) \neq I$. Seja $E = h^{-1}I \in r, I' = h(I) \in r'$ e consideremos a recta $e = EI'$. Escolhamos um ponto A qualquer em r , distinto de E e I , e ponhamos $A' = h(A)$.

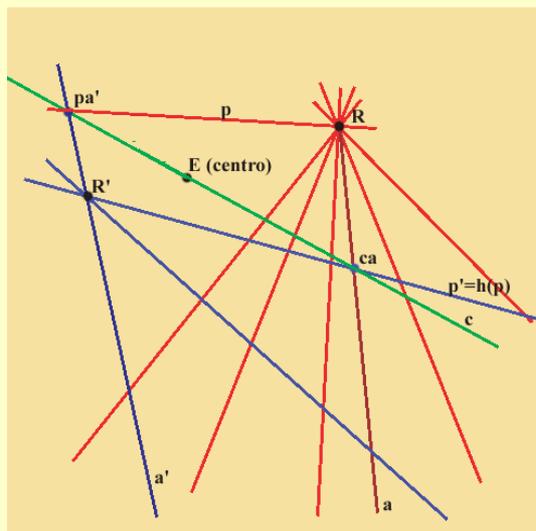
A homografia $h_o : r \rightarrow r'$, construída pelo processo exposto no número anterior, usando o par (A, A') e a recta $e = EI'$, satisfaz $h(A) = A', h(E) = I$ e $H(I) = I'$. O mesmo acontece com h , por construção. Logo $h \equiv h_o$.

2. Se $h(I) = I$ então h é uma projecção. Escolhamos dois pontos distintos $A, B \in r$, diferentes de I , e ponhamos $A' = h(A)$ e $B' = h(B)$. Então $V = AA' \cap BB'$ é o centro da projecção.

Consideremos a recta e que une I com o ponto $C = AB' \cap A'B$. A homografia $h_o : r \rightarrow r'$, construída pelo processo exposto no número anterior, usando o par (A, A') e a recta $e = IC$, satisfaz $h(A) = A', h(B) = B'$ e $H(I) = I$. O mesmo acontece com h , por construção. Logo $h \equiv h_o$.

Em ambos os casos a recta e está univocamente determinada. □.

► 7.10 Homografias entre dois feixes no plano ...



Sejam $\mathcal{F}(R)$ e $\mathcal{F}(R')$ dois feixes distintos de rectas em \mathbb{P}^2 e $i = RR'$ a recta comum.

Consideremos duas rectas, $a \in \mathcal{F}(R)$ e $a' \in \mathcal{F}(R')$, ambas distintas de i , e ainda ponto E não pertencente a i .

A cada recta $p \in \mathcal{F}(R)$, associamos uma recta $p' = h(p) \in \mathcal{F}(R')$, construída pelo processo seguinte:

- intersectamos p com a'
- determinamos a recta c que une o ponto $p \cap a'$ com o ponto E
- intersectamos a recta a com a recta c e determinamos p' - a recta que une o ponto $a \cap c$ com o ponto R' .

► **7.11 Teorema dual de 7.9 ...** (i). Toda a homografia $h : \mathcal{F}(R) \rightarrow \mathcal{F}(R')$ pode ser obtida pelo processo acima indicado, a partir de um par de rectas homólogas (a, a') , ambas distintas de $i = RR'$, e de um ponto E não pertencente nem a a nem a a' .

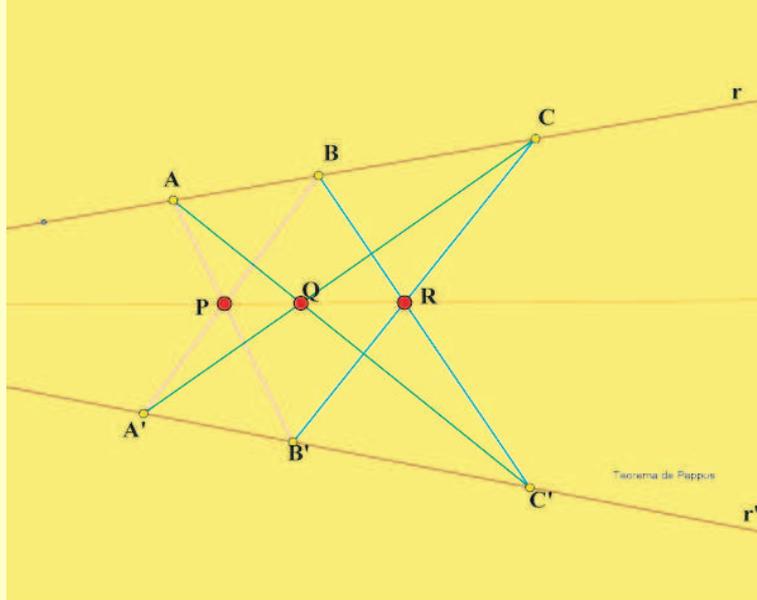
(ii). O ponto E depende apenas de h e não do par (a, a') . Em particular se (a, a'') e (b, b') são dois pares de rectas homólogas os pontos $a \cap b'$ e $a' \cap b$ definem uma recta que contém E .

O ponto E diz-se o **centro** da homografia h .

► **7.12 Teorema de Pappus ...** Dadas duas rectas distintas r e r' em \mathbb{P}^2 , três pontos distintos A, B, C em r e três pontos distintos A', B', C' em r' , então os três pontos:

$$P = AB' \cap A'B, \quad Q = AC' \cap A'C, \quad R = BC' \cap B'C$$

são colineares.



Dem.: Seja $h : r \rightarrow r'$ a única homografia transforma A, B e C , respectivamente em A', B' e C' . O eixo desta homografia é a recta $e = PQ$. Mas R também pertence a esta recta.

□

► **7.13 Outra demonstração do Teorema de Pappus ...** Sem perda de generalidade podemos supôr que A, B, C' e B' formam um referencial projectivo, em que o triângulo de referência é $\Delta(ABC')$ e o ponto unidade é B' :

$$A = [1, 0, 0], \quad B = [0, 1, 0], \quad C' = [0, 0, 1], \quad B' = [1, 1, 1]$$

A recta AB tem coordenadas $(1, 0, 0) \wedge (0, 1, 0) = (0, 0, 1)$ e portanto tem equação $Z = 0$. Como $C \in AB$, $C = [1, c, 0]$ com $c \neq 0$ uma vez que $A \neq C$. Analogamente, a recta $B'C'$ tem equação $X = Y$ e portanto $A' = [1, 1, a]$, com $a \neq 1$.

Calculemos agora as coordenadas dos pontos de intersecção:

$$P = AB' \cap A'B, \quad Q = AC' \cap A'C, \quad R = BC' \cap B'C$$

A recta AB' tem coordenadas $(1, 0, 0) \wedge (1, 1, 1) = (0, -1, 1)$, enquanto que a recta $A'B$ tem coordenadas $(1, 1, a) \wedge (0, 1, 0) = (-a, 0, 1)$. Portanto, $P = AB' \cap A'B$ tem coordenadas $(0, -1, 1) \wedge (-a, 0, 1) = (1, a, a)$.

Analogamente, $Q = AC' \cap A'C$ tem coordenadas $[1 - c, 0, -ca]$ e $R = BC' \cap B'C$ tem coordenadas $[0, 1 - c, 1]$. Mas:

$$(c - 1)(1, a, a) + (1 - c, 0, -ca) + a(0, 1 - c, 1) = 0$$

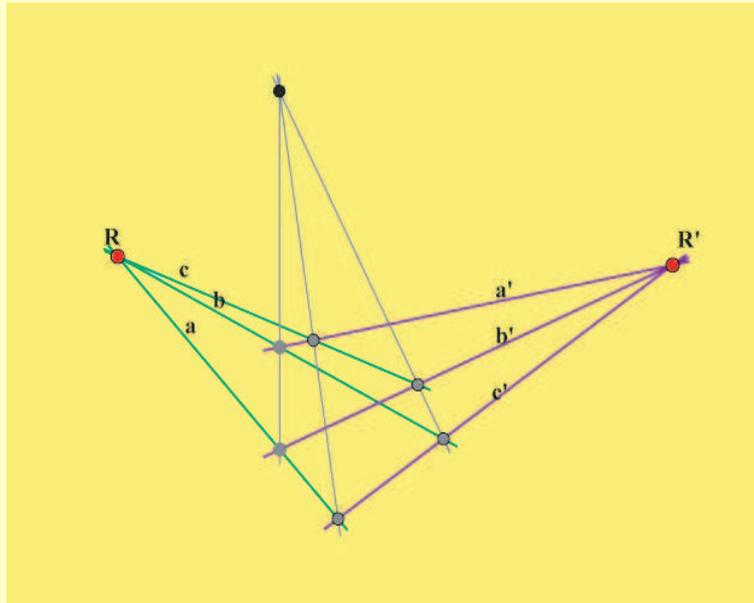
donde se conclui que os três pontos P, Q e R são colineares.

□

► **7.14 Teorema de Pappus dual ...** Dados dois feixes distintos $\mathcal{F}(R)$ e $\mathcal{F}(R')$ em \mathbb{P}^2 , três rectas distintas a, b, c em $\mathcal{F}(R)$ e três rectas distintas a', b', c' em $\mathcal{F}(R')$, então as três rectas:

$$p = ab' \vee a'b, \quad q = ac' \vee a'c, \quad r = bc' \vee b'c$$

são concorrentes num único ponto.



Tópico 8

Cônicas. Polaridade

► **8.1 Formas bilineares simétricas** ... Seja β uma forma bilinear simétrica em \mathbb{k}^3 , isto é:

$$\begin{aligned} \beta : \mathbb{k}^3 \times \mathbb{k}^3 &\longrightarrow \mathbb{k} \\ (\mathbf{a}, \mathbf{b}) &\longmapsto \beta(\mathbf{a}, \mathbf{b}) \end{aligned} \quad (8.1)$$

é linear em cada uma das variáveis e $\beta(\mathbf{a}, \mathbf{b}) = \beta(\mathbf{b}, \mathbf{a})$, $\forall \mathbf{a}, \mathbf{b} \in \mathbb{k}^3$. A **forma quadrática** Q , associada a β , é definida por:

$$Q(\mathbf{a}) = \beta(\mathbf{a}, \mathbf{a}), \quad \mathbf{a} \in \mathbb{k}^3 \quad (8.2)$$

► **8.2 Identidade de polarização** ... A forma bilinear β pode ser recuperada a partir de Q através da identidade de polarização seguinte:

$$\beta(\mathbf{a}, \mathbf{b}) = \frac{1}{2} (Q(\mathbf{a} + \mathbf{b}) - Q(\mathbf{a}) - Q(\mathbf{b})) \quad (8.3)$$

É fácil ver que β também pode ser obtida através de:

$$\beta(\mathbf{a}, \mathbf{b}) = \frac{1}{2} \mathbf{b} \cdot \nabla Q(\mathbf{a}) = \frac{1}{2} \mathbf{a} \cdot \nabla Q(\mathbf{b}) \quad (8.4)$$

► **8.3 Cônica não degenerada** ... Definamos uma aplicação linear $\Phi : \mathbb{k}^3 \rightarrow (\mathbb{k}^3)^*$, através de:

$$\begin{aligned} \Phi : \mathbb{k}^3 &\longrightarrow (\mathbb{k}^3)^* \\ \mathbf{a} &\longmapsto \left(\begin{array}{l} \varphi_{\mathbf{a}} : \mathbb{k}^3 \longrightarrow \mathbb{k} \\ \mathbf{b} \longmapsto \varphi_{\mathbf{a}}(\mathbf{b}) = \beta(\mathbf{a}, \mathbf{b}) \end{array} \right) \end{aligned} \quad (8.5)$$

ou mais simplesmente:

$$\Phi : \mathbf{a} \mapsto \beta(\mathbf{a}, \cdot) \quad (8.6)$$

Quando esta aplicação é um isomorfismo, diz-se que β (ou Q) é **não degenerada**. A curva:

$$Q(\mathbf{x}) = 0 \quad (8.7)$$

diz-se então uma **cônica própria** ou **não degenerada**. Neste caso, o isomorfismo linear Φ induz uma homografia:

$$\begin{aligned} \phi : \mathbb{P}^2 &\longrightarrow (\mathbb{P}^2)^* \\ [\mathbf{a}] &\longmapsto [\beta(\mathbf{a}, \cdot)] \end{aligned} \quad (8.8)$$

► **8.4 Polaridade relativamente a uma cónica não degenerada** ... Recordemos agora que no tópico 6, identificamos $(\mathbb{P}^2)^*$ com $\mathcal{R}(\mathbb{P}^2)$, o conjunto de todas as rectas (projectivas) em \mathbb{P}^2 . Portanto fica definido um isomorfismo:

$$\begin{aligned} \phi : \quad \mathbb{P}^2 &\longrightarrow \mathcal{R}(\mathbb{P}^2) \\ A = [\mathbf{a}] &\longmapsto \phi(A) = [\ker \beta(\mathbf{a}, \cdot)] \end{aligned} \quad (8.9)$$

que se diz a **polaridade** relativamente à cónica (própria ou não degenerada) $\mathcal{C} = [Q^{-1}(0)] \subset \mathbb{P}^2$.

► **8.5 Pólo e recta polar** ... Se $A = [\mathbf{a}] \in \mathbb{P}^2$ é um ponto, à recta $a = \phi(A) = [\ker \beta(\mathbf{a}, \cdot)]$ chama-se a **recta polar** do ponto A , e ao ponto A chama-se **pólo** da recta $a = \phi(A)$.

Como a forma é simétrica tem-se que:

$$B \in \phi(A) \Leftrightarrow A \in \phi(B) \quad (8.10)$$

► **8.6 Pontos conjugados** ... Dois pontos $A = [\mathbf{a}], B = [\mathbf{b}] \in \mathbb{P}^2$ dizem-se **conjugados** relativamente a \mathcal{C} , se $\beta(\mathbf{a}, \mathbf{b}) = 0$.

A recta polar do ponto A é pois constituída por todos os pontos B conjugados a A .

Dois pontos distintos $A, B \in \mathcal{C}$ nunca podem ser conjugados. Caso contrário, ter-se-ia $\phi(A) = AB = \phi(B)$, o que contraria a injectividade da polaridade ϕ .

Em particular, para $A \in \mathcal{C}$, a polar de A tem apenas o ponto A em comum com \mathcal{C} . Por isso, $\phi(A)$ é a **recta tangente** a \mathcal{C} em A .

► **8.7 Exemplo** ... Em \mathbb{P}^2 consideremos a cónica $\mathcal{C} : X^2 + Y^2 + Z^2 = 0$, cuja forma polar é:

$$\beta((X, Y, Z), (X', Y', Z')) = XX' + YY' + ZZ'$$

A polaridade relativamente à cónica \mathcal{C} é a dualidade tratada no tópico 6.

► **8.8 Exemplo** ... Em \mathbb{P}^2 consideremos a cónica $\mathcal{C} : X^2 + Y^2 - Z^2 = 0$ (circunferência de centro 0 e raio 1), cuja forma polar é $\beta((X, Y, Z), (X', Y', Z')) = XX' + YY' - ZZ'$. A recta polar a , de um ponto $A = [X_o, Y_o, Z_o] \in \mathbb{P}^2$, é definida por:

$$a = \{B = [X, Y, Z] \in \mathbb{P}^2 : X_o X + Y_o Y - Z_o Z = 0\}$$

Em coordenadas afins $x = X/Z, y = Y/Z$, a cónica \mathcal{C} tem por equação $x^2 + y^2 = 1$, e, supondo que o ponto A está a “distância finita”, i.e., que $Z_o \neq 0$, então as coordenadas afins de A são $(x_o = X_o/Z_o, y_o = Y_o/Z_o)$. A recta polar a é a recta afim dada por:

$$x_o x + y_o y = 1$$

► **8.9 Recta tangente a uma cónica** ... Quando o ponto $A = [\mathbf{a}]$ pertence à cónica \mathcal{C} , isto é, quando $Q(\mathbf{a}) = 0$, a recta polar de A é definida pela equação

$$X \frac{\partial Q}{\partial X}(\mathbf{a}) + Y \frac{\partial Q}{\partial Y}(\mathbf{a}) + Z \frac{\partial Q}{\partial Z}(\mathbf{a}) = \mathbf{x} \cdot \nabla Q(\mathbf{a}) = 0$$

que é exactamente a equação do **recta tangente à cónica \mathcal{C} em A**

► **8.10 Intersecção de \mathcal{C} com uma recta ...** Sejam $A = [\mathbf{a}]$, $B = [\mathbf{b}]$ dois pontos distintos em \mathbb{P}^2 . Cada ponto da recta AB , distinto de A , pode ser escrito na forma $[t\mathbf{a} + \mathbf{b}]$, com $t \in \mathbb{k}$. Um tal ponto estará em \mathcal{C} se:

$$\begin{aligned} 0 &= Q(t\mathbf{a} + \mathbf{b}) \\ &= \beta(t\mathbf{a} + \mathbf{b}, t\mathbf{a} + \mathbf{b}) \\ &= Q(\mathbf{b}) + 2t\beta(\mathbf{a}, \mathbf{b}) + t^2Q(\mathbf{a}) \end{aligned} \quad (8.11)$$

Daqui se deduzem os factos seguintes:

- \mathcal{C} não contém 3 pontos colineares. De facto, se $A = [\mathbf{a}]$, $B = [\mathbf{b}]$ e $[t\mathbf{a} + \mathbf{b}]$ estivessem em \mathcal{C} , então $Q(\mathbf{a}) = 0$, $Q(\mathbf{b}) = 0$ e $Q(t\mathbf{a} + \mathbf{b}) = 0$. Portanto, ter-se-ia também que $\beta(\mathbf{a}, \mathbf{b}) = 0$, isto é, os pontos A e B seriam conjugados. Mas, como já vimos antes, não é possível ter dois pontos conjugados em \mathcal{C} que sejam colineares.
- Uma recta de \mathbb{P}^2 intersecta \mathcal{C} quando muito em dois pontos.
- Uma recta tem um único ponto comum com \mathcal{C} sse é a tangente a \mathcal{C} nesse ponto. De facto, seja AB essa recta com $B \in \mathcal{C}$ e $A \notin \mathcal{C}$. Então B é o único ponto comum a \mathcal{C} e à recta AB sse $t = 0$ é raiz dupla de (8.11). Como $Q(\mathbf{b}) = 0$ esta condição equivale a $\beta(\mathbf{a}, \mathbf{b}) = 0$, isto é, $\phi(B) = AB$.

► **8.11 Cálculos em coordenadas homogéneas ...** Consideremos uma base fixa $\mathcal{B} = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ para \mathbb{k}^3 e coordenadas homogéneas $[X, Y, Z]$ relativas a essa base.

Seja

$$S = \beta(\mathbf{e}_i, \mathbf{e}_j) = \begin{pmatrix} a & e & f \\ e & b & g \\ f & g & c \end{pmatrix} \quad (8.12)$$

a matriz da forma bilinear β relativamente à base \mathcal{B} . Para vectores $\mathbf{a} = (X, Y, Z)$, $\mathbf{a}' = (X', Y', Z')$ de \mathbb{k}^3 põe-se:

$$\begin{aligned} \beta(\mathbf{a}, \mathbf{b}) &= \mathbf{a}^t S \mathbf{b} \\ &= (X \ Y \ Z) \begin{pmatrix} a & e & f \\ e & b & g \\ f & g & c \end{pmatrix} \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} \\ &= aXX' + bYY' + cZZ' + e(XY' + X'Y) + f(XZ' + X'Z) + g(YZ' + Y'Z) \end{aligned}$$

Pômos ainda:

$$Q(X, Y, Z) = \mathbf{a}^t S \mathbf{a} = aX^2 + bY^2 + cZ^2 + 2eXY + 2fXZ + 2gYZ \quad (8.13)$$

Um cálculo simples mostra que:

$$2\beta(\mathbf{a}, \mathbf{a}') = X'Q_X(\mathbf{a}) + Y'Q_Y(\mathbf{a}) + Z'Q_Z(\mathbf{a}) \quad (8.14)$$

onde $Q_X = \partial Q / \partial X$, etc...

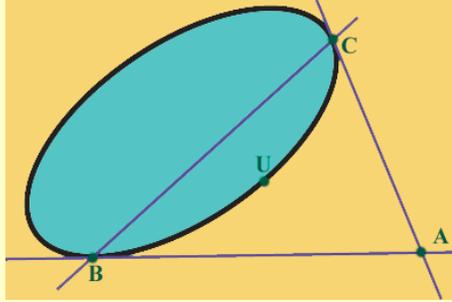
A equação da polar de um ponto $A = \pi(\mathbf{a})$ é pois:

$$XQ_X(\mathbf{a}) + YQ_Y(\mathbf{a}) + ZQ_Z(\mathbf{a}) = 0 \quad (8.15)$$

► **8.12** Vamos ver a forma que a equação da cónica tem, quando escolhemos convenientemente o referencial.

Consideremos uma base fixa $\mathcal{B} = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ para \mathbb{k}^3 , e sejam $A = [\mathbf{a}]$, $B = [\mathbf{b}]$, $C = [\mathbf{c}]$ os vértices do triângulo de referência, de tal forma que $A = [1, 0, 0]$, $B = [0, 1, 0]$, $C = [0, 0, 1]$.

- B e C estão sobre \mathcal{C} e as rectas BA e CA são tangentes a \mathcal{C} em B e C , respectivamente.



Neste caso, como $B = [0, 1, 0] \in \mathcal{C}$ e $C = [0, 0, 1] \in \mathcal{C}$, vem que $Q(0, 1, 0) = 0 = Q(0, 0, 1)$ e portanto a equação de \mathcal{C} tem a forma:

$$Q(X, Y, Z) = aX^2 + 2eXY + 2fXZ + 2gYZ$$

As rectas tangentes em B e C têm por equações respectivamente

$$\begin{aligned} (X, Y, Z) \cdot \nabla Q(0, 1, 0) &= eX + gZ = 0 \\ (X, Y, Z) \cdot \nabla Q(0, 0, 1) &= fX + gY = 0 \end{aligned} \quad (8.16)$$

Como estas tangentes são distintas, podemos supôr que $A = [1, 0, 0]$ é o seu ponto comum. Como as rectas AB e AC têm por equação $Z = 0$ e $Y = 0$, respectivamente, deduzimos então que $e = f = 0$, $g \neq 0$ e a equação de \mathcal{C} é pois:

$$aX^2 + 2gYZ = 0$$

Podemos ainda exigir que o ponto unidade $U = [1, 1, 1]$ esteja sobre \mathcal{C} e obtemos finalmente a equação para \mathcal{C} :

$$X^2 - YZ = 0 \quad (8.17)$$

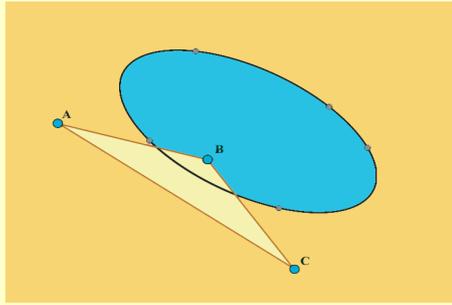
- A, B e C estão todos sobre \mathcal{C} .

Como \mathcal{C} não contém 3 pontos colineares, podemos supôr que $A, B, C \in \mathcal{C}$. Neste caso a equação de \mathcal{C} é:

$$2eXY + 2fXZ + 2gYZ = 0 \quad (8.18)$$

- *Caso em que A, B e C formam um triângulo auto-polar.*

Podemos supôr que a base $\mathcal{B} = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ é ortogonal relativamente a β . Esta condição equivale a $0 = \beta(\mathbf{a}, \mathbf{b}) = \beta(\mathbf{a}, \mathbf{c}) = \beta(\mathbf{b}, \mathbf{c})$, o que significa que os 3 pontos A, B e C formam um **triângulo auto-polar**, isto é, um triângulo em que cada um dos vértices é o pólo do lado oposto.



Neste caso a equação de \mathcal{C} é:

$$aX^2 + bY^2 + cZ^2 = 0 \quad (8.19)$$

A partir de um ponto qualquer A e de um dos seus conjugados $B \neq A$, por exemplo, obtemos um triângulo auto-polar A, B, C tomando C como o pólo do lado AB .

► **8.13 Construção das polares** ... Faz-se a partir das propriedades seguintes:

- Se A, B são dois pontos distintos de \mathcal{C} , então a recta AB é a polar do ponto de encontro das tangentes a \mathcal{C} em A e B .

Com efeito, a polar deste ponto passa por A e por B .

- Sejam M, N, A, B quatro pontos alinhados distintos, com $A, B \in \mathcal{C}$. Então a polar de M contém N (e vice-versa) sse $(ABMN) = -1$.

Por outras palavras, a polaridade correspondente a β induz uma involução sobre cada secante à cónica \mathcal{C} .

Para mostrar isto, seja $A = [\mathbf{a}], B = [\mathbf{b}] \in \mathcal{C}$ e escrevamos $M = [\mathbf{a} + s\mathbf{b}], N = [\mathbf{a} + t\mathbf{b}]$, com $s, t \in \mathbb{k} - \{0\}$. Tem-se então que:

$$\begin{aligned} \beta(\mathbf{a} + s\mathbf{b}, \mathbf{a} + t\mathbf{b}) &= Q(\mathbf{a}) + (s+t)\beta(\mathbf{a}, \mathbf{b}) + stQ(\mathbf{b}) \\ &= (s+t)\beta(\mathbf{a}, \mathbf{b}) \\ (ABMN) &= \frac{s}{t} \end{aligned} \quad (8.20)$$

Como, $\beta(\mathbf{a}, \mathbf{b}) \neq 0$, vemos que a polar de M contém N sse $s+t=0$, isto é, sse $s/t = -1$.

Quando $\mathbb{k} = \mathbb{C}$, toda a recta não tangente a \mathcal{C} intersecta \mathcal{C} em exactamente dois pontos. A polar de M é pois o conjunto dos pontos N tais que $(ABMN) = -1$, onde A e B são os pontos comuns a \mathcal{C} e a MN .

Tópico 9

Equações tangenciais das cónicas. Assíntotas e focos

► **9.1 Curva dual** ... Dada uma curva algébrica em \mathbb{P}^2 :

$$\mathcal{C} = \{P = [X, Y, Z] : F(P) = F(X, Y, Z) = 0\} \quad (9.1)$$

define-se a respectiva **curva dual** \mathcal{C}^* , em $(\mathbb{P}^2)^*$, através de:

$$\mathcal{C}^* = \{\alpha = [U, V, W] : \text{a recta } \ker \alpha \text{ é tangente a } \mathcal{C}, \text{ em algum ponto de } \mathcal{C}\} \quad (9.2)$$

Suponhamos que \mathcal{C} é não singular, isto é, todos os pontos P de \mathcal{C} são regulares (pelo menos uma das derivadas parciais $F_X(P), F_Y(P), F_Z(P)$ é não nula).

A equação da recta $\ker \alpha$ é:

$$UX + VY + WZ = 0 \quad (9.3)$$

Por outro lado, a equação da recta tangente a \mathcal{C} em $P = [X, Y, Z]$ é:

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0 \quad (9.4)$$

Portanto $\alpha = [U, V, W]$ deverá satisfazer o sistema de equações seguinte:

$$\begin{cases} U & = \lambda F_X(X, Y, Z) \\ V & = \lambda F_Y(X, Y, Z) \\ W & = \lambda F_Z(X, Y, Z) \\ F_X(X, Y, Z) & = 0 \end{cases} \quad (9.5)$$

que, após eliminação de X, Y, Z e λ conduzem a uma equação do tipo:

$$F^*(U, V, W) = 0 \quad (9.6)$$

que se diz a **equação tangencial** da curva \mathcal{C} . O grau de F^* diz-se a **classe da curva** \mathcal{C} .

► **9.2 Equação tangencial de uma cónica não singular** ... Consideremos uma cónica \mathcal{C} não singular, dada por:

$$Q(\mathbf{x}) = \mathbf{x}^t S \mathbf{x} = 0$$

onde pusemos $\mathbf{x} = (X, Y, Z)$. S é a matriz simétrica inversível que representa a forma polar de Q , relativamente a uma base fixa de \mathbb{k}^3 . A equação da recta tangente num ponto $A = [\mathbf{a}]$ é:

$$\mathbf{x}^t S \mathbf{a} = 0$$

ou, de forma equivalente:

$$\mathbf{x} \cdot \nabla Q(\mathbf{a}) = Q_X(\mathbf{a})X + Q_Y(\mathbf{a})Y + Q_Z(\mathbf{a})Z = 0$$

uma vez que $\nabla F(\mathbf{a}) = 2S\mathbf{a}$.

A recta $\ker \alpha$, onde $\alpha = [\mathbf{u}] = [U, V, W]$, tem por equação:

$$\mathbf{u}\mathbf{x} = 0$$

(\mathbf{u} é vector-linha), e será tangente a \mathcal{C} , num ponto $A = [\mathbf{a}] \in \mathcal{C}$, sse:

$$\mathbf{u} = \lambda(S\mathbf{a})^t = \lambda\mathbf{a}^t S^t$$

Para encontrar a equação tangencial da cónica \mathcal{C} devemos pois eliminar λ e \mathbf{a} no sistema de equações (recorde que $S^t = S$):

$$\begin{cases} \mathbf{u} &= \lambda\mathbf{a}^t S \\ \mathbf{a}^t S\mathbf{a} &= 0 \end{cases} \quad (9.7)$$

Da primeira tiramos que:

$$\mathbf{a}^t = \mathbf{u}S^{-1}/\lambda$$

que substituída na segunda dá:

$$0 = \mathbf{a}^t S\mathbf{a} = \mathbf{u}S^{-1}/\lambda S S^{-1}\mathbf{u}^t/\lambda \Rightarrow \mathbf{u}S^{-1}\mathbf{u}^t = 0$$

isto é, a equação tangencial de \mathcal{C} é:

$$\mathbf{u}S^{-1}\mathbf{u}^t = 0$$

► **9.3 Exemplo** ... *Calcular a equação tangencial das cónicas:*

$$\begin{aligned} \text{(i.)} \quad aX^2 + bY^2 + cZ^2 &= 0 \\ \text{(ii.)} \quad aYZ + bXZ + cXY &= 0 \\ \text{(iii.)} \quad XY + Z^2 &= 0 \end{aligned}$$

Resolução

(i.) $U^2/a + V^2/b + W^2/c = 0$

(ii.) $aU^2 + bV^2 + cW^2 - abUV - acUW - bcVW = 0$.

► **9.4 Assíntotas** ... Seja \mathcal{C} uma curva afim em \mathbb{A}^2 e $\widehat{\mathcal{C}}$ o seu fecho projectivo em \mathbb{P}^2 . Uma assíntota de \mathcal{C} , em \mathbb{A}^2 , é uma recta afim ℓ , cujo fecho projectivo $\widehat{\ell}$, é tangente num ponto $A \in \mathcal{C}_\infty = \widehat{\mathcal{C}} \cap \{Z = 0\}$.

Para calcular as assíntotas de \mathcal{C} , procede-se da seguinte forma

1. Calculamos os pontos $A \in \mathcal{C}_\infty = \widehat{\mathcal{C}} \cap \{Z = 0\}$
2. Calculamos as tangentes a $\widehat{\mathcal{C}}$ nesses pontos A .
3. As assíntotas são as tangentes que são diferentes de $Z = 0$.

► **9.5 Exemplo** ... Calculemos as assíntotas da hipérbole $x^2 - y^2 - 1 = 0$, em $\mathbb{A}_{\mathbb{R}}^2$. O fecho projectivo é $\widehat{X}^2 - \widehat{Y}^2 - \widehat{Z}^2 = 0$ e os pontos no infinito são $A = [1, 1, 0]$ e $B = [1, -1, 0]$. Ambos são suaves (simples) com tangentes $X + Y = 0$ e $X - Y = 0$, respectivamente. As assíntotas são pois as rectas $y = \pm x$.

► **9.6 Exercício** ... Mostrar que as assíntotas do círculo $x^2 + y^2 = 1$ são as linhas isotrópicas que passam no seu centro.

► **9.7 Exercício** ... Mostrar que as assíntotas da elipse $b^2x^2 + a^2y^2 = a^2b^2$ são $y = \pm i(b/a)x$

► **9.8 Exercício** ... Mostrar que a assíntota da parábola $y^2 = 4px$ é a recta do infinito contada duas vezes.

► **9.9 Rectas isotrópicas** ... Recordemos que os **pontos cíclicos** em $\mathbb{P}^2(\mathbb{C})$ são os pontos:

$$I = [1, i, 0] \quad \text{e} \quad J = [1, -i, 0]$$

Dado um ponto $P \in \mathbb{P}^2(\mathbb{C})$, distinto de I e de J , às rectas PI e PJ chamam-se as **rectas isotrópicas** que passam em P .

Quando P é real as rectas isotrópicas são complexas conjugadas.

► **9.10 Focos** ... Suponhamos agora que é dada uma cónica afim real $\mathcal{C} : Q(\mathbf{x}) = 0$, em \mathbb{R}^2 , não degenerada e seja $(a, b) \in \mathbb{R}^2$ um ponto real. Seja $P = [a, b, 1]$ e consideremos as rectas isotrópicas que passam em P . As suas coordenadas tangenciais são:

$$\begin{aligned} PI & : (a, b, 1) \wedge (1, i, 0) = (-i, 1, ai - b) \\ PJ & : (a, b, 1) \wedge (1, -i, 0) = (i, 1, -ai - b) \end{aligned} \tag{9.8}$$

O ponto $(a, b) \in \mathbb{R}^2$ diz-se um **foco** da cónica \mathcal{C} , quando as rectas isotrópicas que passam em $P = [a, b, 1]$ são tangentes a $\widehat{\mathcal{C}}$.

Note que estas rectas isotrópicas serão tangentes a $\widehat{\mathcal{C}}$ quando as respectivas coordenadas (9.8) verificarem a equação tangencial da cónica.

► **9.11 Exemplo** ... Calculemos os focos da parábola $y^2 - 4x = 0$. O seu fecho projectivo é:

$$Q(X, Y, Z) = Y^2 - 4XZ = 0$$

ou ainda:

$$Q(\mathbf{x}) = \mathbf{x}^t S \mathbf{x} = \mathbf{x}^t \begin{pmatrix} 0 & 0 & -2 \\ 0 & 1 & 0 \\ -2 & 0 & 0 \end{pmatrix} \mathbf{x}$$

A equação tangencial é $\mathbf{u}S^{-1}\mathbf{u}^t = 0$, isto é:

$$Q(\mathbf{u}) = \mathbf{u}S\mathbf{u}^t = \mathbf{u} \begin{pmatrix} 0 & 0 & -1/2 \\ 0 & 1 & 0 \\ 0 & 0 & -1/2 \end{pmatrix} \mathbf{u}^t$$

ou ainda:

$$Q^*(\mathbf{u}) = V^2 - UW = 0$$

Um ponto $(a, b) \in \mathbb{R}^2$ é um foco da parábola quando as rectas isotrópicas que passam em $P = [a, b, 1]$ são tangentes a $\widehat{\mathcal{C}}$. As coordenadas tangenciais destas rectas são dadas por (9.8), $PI = [-i, 1, ai - b]$ e $PJ = [i, 1, -ai - b]$. Elas serão tangente à parábola quando essas coordenadas verificarem a equação tangencial da cónica $V^2 - UW = 0$, portanto, quando:

$$1 - a - ib = 0 \quad \text{e} \quad 1 - a - ib = 0$$

Isto acontece apenas quando $a = 1$ e $b = 0$, o que significa que $(1, 0)$ é o único foco da parábola.

► **9.12 Exemplo** ... Calculemos os focos da elipse $x^2 + 4y^2 - 4 = 0$. O seu fecho projectivo é:

$$Q(X, Y, Z) = X^2 + 4Y^2 - 4Z^2 = 0$$

ou ainda:

$$Q(\mathbf{x}) = \mathbf{x}^t S \mathbf{x} = \mathbf{x}^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -4 \end{pmatrix} \mathbf{x}$$

A equação tangencial é $\mathbf{u} S^{-1} \mathbf{u}^t = 0$, isto é:

$$Q(\mathbf{u}) = \mathbf{u} S \mathbf{u}^t = \mathbf{u} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/4 & 0 \\ 0 & 0 & -1/4 \end{pmatrix} \mathbf{u}^t$$

ou ainda:

$$Q^*(\mathbf{u}) = 4U^2 + V^2 - W^2 = 0$$

Um ponto $(a, b) \in \mathbb{R}^2$ é um foco da elipse quando as rectas isotrópicas que passam em $P = [a, b, 1]$ são tangentes a $\widehat{\mathcal{C}}$. As coordenadas tangenciais destas rectas são dadas por (9.8), $PI = [-i, 1, ai - b]$ e $PJ = [i, 1, -ai - b]$. Elas serão tangente à elipse quando essas coordenadas verificarem a equação tangencial da cónica $4U^2 + V^2 - W^2 = 0$, portanto, quando:

$$-4 + 1 - (ai - b)^2 = 0 \quad \text{e} \quad -4 + 1 - (-ai - b)^2 = 0$$

Isto acontece apenas quando $a = \pm\sqrt{3}$ e $b = 0$, o que significa que $(\pm\sqrt{3}, 0)$ são os dois focos da elipse.

► **9.13 Focos** ... Mais geralmente, seja \mathcal{C} uma curva algébrica de classe n em $\mathbb{P}^2(\mathbb{R})$. Os focos de \mathcal{C} , em $\mathbb{P}^2(\mathbb{C})$ são os pontos de intersecção das tangente a \mathcal{C} que partem dos pontos cíclicos I e J . A curva tem portanto n^2 focos.

► **9.14 Exemplo** ... Os focos da elipse $4x^2 + 9y^2 = 36$ são $(\pm\sqrt{5}, 0)$ e $(0, \pm i\sqrt{5})$.

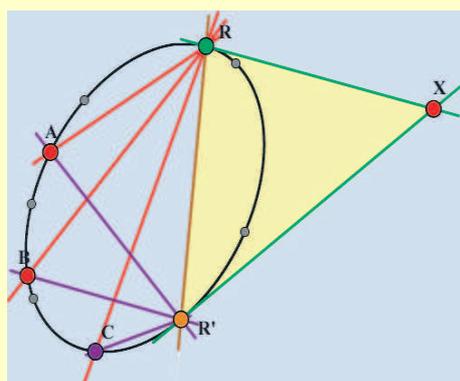
► **9.15 Exemplo** ... O foco da parábola $y^2 = 4px$ é $(p, 0)$.

► **9.16 Exemplo** ... Os focos da hipérbole $b^2x^2 - a^2y^2 = a^2b^2$ são $(\pm\sqrt{a^2 + b^2}, 0)$ e $(0, \pm i\sqrt{a^2 + b^2})$.

Tópico 10

Homografias e Cónicas. Teoremas de Pascal e Brianchon

► 10.1 Homografias numa cónica ...



Teorema de Chasles ... Sejam R e R' dois pontos de uma cónica não degenerada \mathcal{C} , e r, r' as tangentes a \mathcal{C} em R e R' , respectivamente.

Definimos uma aplicação $h : \mathcal{F}(R) \rightarrow \mathcal{F}(R')$ da seguinte forma:

Cada recta que passa por R , distinta de r , intersecta \mathcal{C} num outro ponto A . Pômos então:

$$h(RA) = R'A$$

e ainda $h(r) = RR'$ e $h(RR') = r'$.

h é uma homografia de feixes. Em particular, para quatro pontos distintos $A, B, C, D \in \mathcal{C}$ tem-se que:

$$(RA, RB, RC, RD) = (R'A, R'B, R'C, R'D) \quad (10.1)$$

Dem.: Seja X o ponto comum às tangentes r e r' . Fazamos os cálculos em coordenadas homogéneas relativas ao referencial formado pelo triângulo de referência $X = [1, 0, 0], R = [0, 1, 0], R' = [0, 0, 1]$ e ponto unidade $U = [1, 1, 1] \in \mathcal{C}$. Como vimos, a equação de \mathcal{C} é então:

$$X^2 - YZ = 0$$

Podemos gerar o feixe $\mathcal{F}(R)$ pela tangente $r = RX$, cuja equação é $Z = 0$ (com coordenadas $[0, 0, 1]$), e a recta RR' de equação $X = 0$ (com coordenadas $[1, 0, 0]$). As rectas do feixe $\mathcal{F}(R)$ têm pois equações do tipo $aX + bZ = 0$, ou ainda, $X + tZ = 0$, $t = b/a$ onde a $t = \infty$ corresponde a recta r .

Analogamente, podemos gerar o feixe $\mathcal{F}(R')$ pela tangente $r' = R'X$, cuja equação é $Y = 0$ (com coordenadas $[0, 1, 0]$), e a recta RR' de equação $X = 0$ (com coordenadas $[1, 0, 0]$). As rectas do feixe $\mathcal{F}(R')$ têm pois equações do tipo $cX + dY = 0$, ou ainda, $X + t'Y = 0$, $t' = d/c$ onde a $t' = \infty$ corresponde a recta r' .

Para t e t' em $\mathbb{k} - \{0\}$, as rectas $X + tZ = 0$ e $X + t'Y = 0$ intersectam-se sobre \mathcal{C} sse $(tt' - 1)X^2 = 0$. Neste caso, $X \neq 0$ e portanto $tt' = 1$ define uma homografia h entre t e t' .

Para $t = 0$ esta homografia dá $t' = \infty$, o que corresponde a $h(RR') = r'$. Para $t = \infty$, esta homografia dá $t' = 0$, o que corresponde a $h(r) = RR'$.

□.

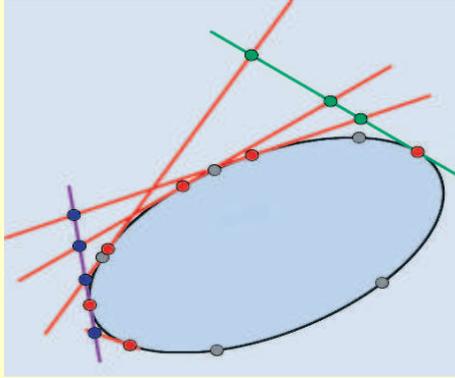
► **10.2 Nota** ... a homografia definida no teorema, entre os feixes $\mathcal{F}(R)$ e $\mathcal{F}(R')$ (ou, de forma equivalente, entre rectas de $(\mathbb{P}^2)^*$), está univocamente definida pelas imagens de 3 rectas distintas do feixe $\mathcal{F}(R)$ (que são 3 rectas distintas do feixe $\mathcal{F}(R')$).

Por outras palavras, 3 rectas distintas e as respectivas imagens distintas determinam univocamente a cónica \mathcal{C} .

Em particular, a cónica \mathcal{C} fica univocamente determinada por:

- 3 dos seus pontos distintos R, R', S e das tangentes em R e R' .
- dando 4 pontos distintos R, R', S, S' e da tangente em R .
- dando 5 pontos distintos.

► **10.3 Teorema dual** ...



Teorema dual ... Quatro tangentes distintas em \mathcal{C} determinam sobre duas outras tangentes duas pontuais em correspondência projectiva.

Dem.: Com efeito a polaridade relativa a \mathcal{C} transforma cada ponto A de \mathcal{C} na recta a , tangente a \mathcal{C} em A , e a recta que une dois pontos A e B , em \mathcal{C} , no ponto de intersecção das tangentes a e b .

► **10.4 Teorema de Steiner** ... Consideremos dois feixes $\mathcal{F}(R)$ e $\mathcal{F}(R')$ de suportes $R \neq R'$ em \mathbb{P}^2 . Podemos supôr que $R = [1, 0, 0]$ e que $R' = [0, 1, 0]$. Qualquer recta do primeiro feixe é então da forma $Y + \lambda Z = 0$ (porquê?) e, analogamente, qualquer recta do segundo feixe é da forma $X + \mu Z = 0$ (porquê?), com $\lambda, \mu \in \mathbb{R} \cup \{\infty\} = \mathbb{P}^1$.

Suponhamos que existe uma projectividade entre os dois feixes, do tipo:

$$\mu = \frac{a\lambda + b}{c\lambda + d}, \quad c \neq 0, \quad ad - bc \neq 0 \quad (10.2)$$

Eliminando λ e μ nas três equações:

$$Y + \lambda Z = 0, \quad X + \mu Z = 0 \quad \mu = \frac{a\lambda + b}{c\lambda + d}$$

obtemos uma cónica pontual \mathcal{C} de equação:

$$aYZ - bZ^2 + cXY - dXZ = 0 \quad (10.3)$$

Observe que R e R' pertencem a \mathcal{C} . A recta RR' , quando considerada como pertencente ao feixe $\mathcal{F}(R)$, corresponde pela projectividade referida, à recta $T_{R'}\mathcal{C}$, enquanto que, quando considerada como pertencente ao feixe $\mathcal{F}(R')$, corresponde à recta $T_R\mathcal{C}$ (verificar). Fica assim demonstrado o seguinte:

Teorema de Steiner ... O lugar geométrico dos pontos de intersecção dos pares de rectas de dois feixes $\mathcal{F}(R)$ e $\mathcal{F}(R')$, em correspondência projectiva, constitui uma cónica pontual.

► **10.5 Teorema de Steiner dual** ... Dulizando o enunciado anterior, obtemos:

Teorema de Steiner dual ... A envolvente das rectas que unem os pares de pontos duas pontuais r e r' , em correspondência projectiva, é uma cónica tangencial.

Podemos supôr que $r = [1, 0, 0]$ e que $r' = [0, 1, 0]$. Qualquer ponto de r tem equação tangencial $V + \lambda W = 0$ (porquê?) e, analogamente, ponto de r' tem equação tangencial $U + \mu W = 0$ (porquê?), com $\lambda, \mu \in \mathbb{R} \cup \{\infty\} = \mathbb{P}^1$.

Suponhamos que existe uma projectividade entre as duas pontuais, do tipo:

$$\mu = \frac{a\lambda + b}{c\lambda + d}, \quad c \neq 0, \quad ad - bc \neq 0 \quad (10.4)$$

Eliminando λ e μ nas três equações:

$$V + \lambda W = 0, \quad U + \mu W = 0 \quad \mu = \frac{a\lambda + b}{c\lambda + d}$$

obtemos uma cónica tangencial \mathcal{C}^* de equação:

$$aVW - bW^2 + cUV - dUW = 0 \quad (10.5)$$

Observe que r e r' são tangente a \mathcal{C} (a cónica pontual correspondente a \mathcal{C}^*). O ponto de intersecção rr' , das duas rectas, quando considerado como pertencente à recta r , corresponde pela projectividade referida, ao ponto de contacto de r' com \mathcal{C} , enquanto que, quando considerado como pertencente à recta r' , corresponde ao ponto de contacto de r com \mathcal{C} (verificar).

► **10.6 Exercício** ... Considere as rectas $y = 0$ e $y = 1$ no plano afim \mathbb{R}^2 , e suponha que existe uma projectividade, entre as duas rectas, do tipo:

$$\mu = \frac{2\lambda + 1}{\lambda}$$

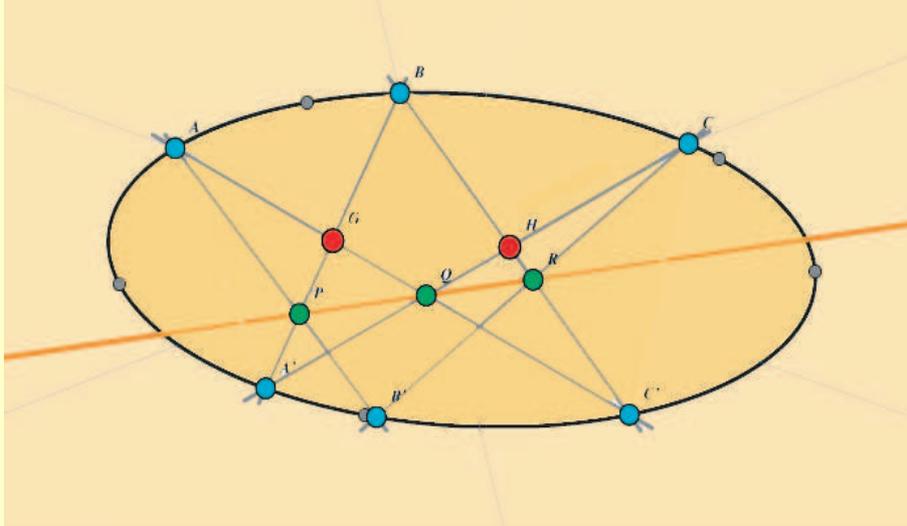
onde a recta $y = 0$ é parametrizada por $\lambda \rightarrow (\lambda, 0)$ e a recta $y = 1$ por $\mu \rightarrow (\mu, 1)$. Calcular a equação da cónica pontual envolvente desta família de rectas.

$$\text{Solução: } x^2 - 4xy + 8y^2 - 4y = 0.$$

► **10.7 Teorema de Pascal** ... *Sejam A, B, C, A', B', C' seis pontos distintos numa cónica \mathcal{C} . Então:*

$$P = AB' \cap A'B, \quad Q = AC' \cap A'C, \quad R = BC' \cap B'C$$

são colineares.



Dem.: Seja $G = AC' \cap A'B$ e $H = BC' \cap CA'$, como na figura. Temos então que:

$$A[B'A'BC'] = C[B'A'BC']$$

e portanto:

$$[PA'BG] = [RHBC']$$

Seja $R' = PQ \cap BC'$. Pela perspectiva de centro Q deduzimos que:

$$[PA'BG] = [R'HBC']$$

Daí que:

$$[RHBC'] = [R'HBC'] \Rightarrow R = R'$$

uma vez que H, B, C' são distintos.

□.

► **10.8 Outra demonstração do teorema de Pascal** ... Suponhamos que $A = [1, 0, 0]$, $B' = [0, 1, 0]$, que o triângulo de referência é $\triangle(AB'P)$, onde $P = [0, 0, 1] = T_A\mathcal{C} \cap T_{B'}\mathcal{C}$, e que o ponto unidade é $C = [1, 1, 1]$. A cónica tem então por equação:

$$Z^2 = XY \tag{10.6}$$

Os pontos A', B e C' têm coordenadas que podemos supôr da forma:

$$\begin{aligned} A' &= [1, \alpha^2, \alpha] \\ B &= [1, \beta^2, \beta] \\ C' &= [1, \gamma^2, \gamma] \end{aligned} \tag{10.7}$$

Calculamos agora sucessivamente as coordenadas dos pontos e rectas seguintes:

$$\begin{aligned} AB' &= [0, 0, 1] \\ A'B &= [1, \alpha^2, \alpha] \wedge [1, \beta^2, \beta] = [\alpha\beta, 1, -\alpha - \beta] \\ P &= AB' \cap A'B = [0, 0, 1] \wedge [\alpha\beta, 1, -\alpha - \beta] = [-1, \alpha\beta, 0] \\ B'C &= [0, 1, 0] \wedge [1, 1, 1] = [1, 0, -1] \\ BC' &= [1, \beta^2, \beta] \wedge [1, \gamma^2, \gamma] = [\beta\gamma, 1, -\beta - \gamma] \\ Q &= B'C \cap BC' = [1, 0, -1] \wedge [\beta\gamma, 1, -\beta - \gamma] = [1, \beta + \gamma - \beta\gamma, 1] \\ CA' &= [1, 1, 1] \wedge [1, \alpha^2, \alpha] = [\alpha, 1, -1 - \alpha] \\ AC' &= [1, 0, 0] \wedge [1, \gamma^2, \gamma] = [0, 1, -\gamma] \\ R &= CA' \cap AC' = [\alpha, 1, -1 - \alpha] \wedge [0, 1, -\gamma] = [\alpha + 1 - \gamma, \alpha\gamma, \alpha] \end{aligned} \tag{10.8}$$

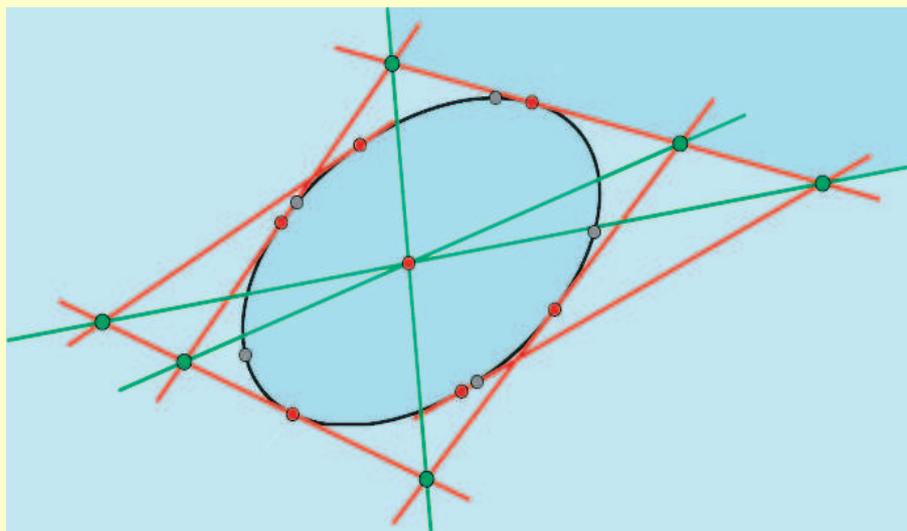
Finalmente tem-se que:

$$\det \begin{pmatrix} -1 & \alpha\beta & 0 \\ 1 & \beta + \gamma - \beta\gamma & 1 \\ \alpha + 1 - \gamma & \alpha\gamma & \alpha \end{pmatrix} = 0$$

► **10.9 Teorema Dual de Brianchon** ... Sejam dadas seis tangentes distintas a, b, c, a', b', c' à cónica \mathcal{C} . As rectas que unem os pares de vértices opostos:

$$p = ab' \cup a'b, \quad q = ac' \cup a'c, \quad r = bc' \cup b'c$$

são concorrentes.



Tópico 11

Pontos racionais em cónicas

► **11.1 Pontos e rectas racionais ...** Um ponto (x, y) no plano diz-se **racional** quando $x, y \in \mathbb{Q}$. Um recta $ax + by + c = 0$ diz-se **racional** quando $a, b, c \in \mathbb{Q}$. É fácil mostrar que:

- a recta que une dois pontos racionais é racional.
- o ponto de intersecção de duas rectas racionais é racional.

► **11.2 Cónicas racionais ...** Uma cónica:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

diz-se **racional** quando $a, b, c, d, e, f \in \mathbb{Q}$.

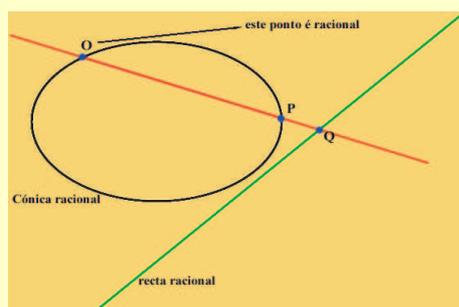
Será verdade que os pontos de intersecção de uma recta racional com uma cónica racional são também racionais?

Em geral não! De facto ao calcular esses pontos sômos conduzidos a uma equação quadrática com coeficientes racionais e só quando esta equação tem soluções racionais é que a resposta é afirmativa. No entanto:

- se um dos pontos de intersecção for racional o outro também o é.

Basta atender ao facto de que numa equação quadrática a soma das raízes é igual ao segundo coeficiente da equação.

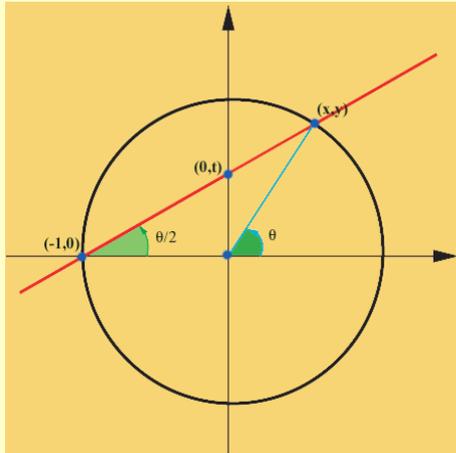
► **11.3 Pontos racionais numa cónica ...** Este facto simples, permite descrever completamente os pontos racionais de uma cónica. No entanto resta ainda a questão de saber quando uma certa cónica tem pelo menos um ponto racional, o que pode ser falso, como veremos em breve!



Suponhamos então que temos uma cónica racional que contem pelo menos um ponto racional O . Podemos então obter todos os outros pontos racionais da seguinte forma - escolhemos uma qualquer recta racional que não passe por O e projectamos a cónica sobre esta recta a partir de O . Obtemos assim uma correspondência bijectiva entre os pontos da cónica (com excepção do ponto O) e os pontos da recta escolhida.

Os factos acima mencionado permitem concluir que, se Q fôr racional, também o será a recta OQ (porque O é racional, por hipótese) e portanto também o será o ponto P . Basta pois fazer com que Q percorra os pontos racionais da recta escolhida para obter todo os pontos racionais P da cónica dada.

► **11.4** Círculo $x^2 + y^2 = 1$...



Consideremos o círculo \mathcal{C} :

$$x^2 + y^2 = 1$$

e apliquemos o processo anterior escolhendo, por exemplo, $O = (-1, 0)$ e a recta sobre a qual se projecta o eixo dos yy , isto é, a recta (racional) $x = 0$. Designando por $(0, t)$ a projecção de $(x, y) \in \mathcal{C}$ sobre $x = 0$, um cálculo simples mostra que:

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2} \quad (11.1)$$

Obtemos assim uma parametrização racional de \mathcal{C} que é uma bijecção de \mathbb{R} sobre $\mathcal{C} - \{(-1, 0)\}$. Podemos até prolongá-la a uma bijecção ϕ de $\mathbb{R} \cup \{\infty\}$ sobre \mathcal{C} , pondo $\phi(\infty) = (-1, 0)$.

As fórmulas (11.1) permitem pois obter todos os pontos racionais do círculo \mathcal{C} (recordando que projectamos a partir do ponto racional $(-1, 0) \in \mathcal{C}$). De facto, se x e y são racionais também o será t . Reciprocamente, se $t \in \mathbb{Q}$ é óbvio, pelas mesmas fórmulas, que (x, y) será um ponto racional de \mathcal{C} .

► **11.5** As fórmulas (11.1) têm várias aplicações. Da figura vê-se facilmente que:

$$x = \cos \theta, \quad y = \sin \theta, \quad \text{e ainda que} \quad t = \tan \frac{\theta}{2} = \frac{\sin \theta}{1 + \cos \theta} \quad (11.2)$$

fórmulas que permitem escrever $\sin \theta$ e $\cos \theta$ como expressões racionais de $\tan \frac{\theta}{2}$:

$$x = \cos \theta = \frac{1 - t^2}{1 + t^2}, \quad y = \sin \theta = \frac{2t}{1 + t^2} \quad (11.3)$$

Se quisermos testar a validade de uma expressão complicada com senos e cossenos, podemos substituir nessa expressão $\sin \theta$ e $\cos \theta$ pelas suas expressões racionais (11.3), em termos de t , e verificar se se obtem uma identidade.

► **11.6** Uma outra aplicação resulta da observação de que as fórmulas (11.1) permitem escrever todas as funções trigonométricas de um ângulo θ como expressões racionais em $t = \tan \theta/2$. Note que:

$$\theta = 2 \arctan(t), \quad d\theta = \frac{2 dt}{1 + t^2} \quad (11.4)$$

Portanto se quisermos calcular a primitiva de uma função que envolve $\sin \theta$ e $\cos \theta$, faz-se as substituições transformando essa primitiva numa primitiva de uma função racional em t , que pode ser feita como habitualmente.

► **11.7 Triângulos Pitagóricos** ... O fecho projectivo do círculo $x^2 + y^2 - 1 = 0$, em $\mathbb{P}_{\mathbb{k}}^2$, é a curva \mathcal{C} :

$$X^2 + Y^2 - Z^2 = 0 \quad (11.5)$$

Tomemos o ponto $O = [-1, 0, 1] \in \mathcal{C}$ e a recta que une este ponto ao ponto $Q = [0, t, 1]$. Pontos desta recta $\neq O$ são da forma:

$$\lambda \mapsto \lambda O + Q = [-\lambda, t, \lambda + 1]$$

e os que estão em \mathcal{C} correspondem aos valores de λ tais que:

$$\lambda^2 + t^2 - (\lambda + 1)^2 = 0$$

isto é:

$$\lambda = (t^2 - 1)/2$$

Obtemos assim a parametrização (polinomial) do círculo:

$$\phi(t) = [(1 - t^2)/2, t, (t^2 + 1)/2] = [1 - t^2, 2t, t^2 + 1]$$

Quando $\mathbb{k} = \mathbb{Q}$ é o corpo dos racionais, este resultado tem uma aplicação muito interessante que passamos a descrever.

Suponhamos que se pretende calcular todos os triângulos rectângulos cujos lados têm comprimento inteiro. Por outras palavras, pelo teorema de Pitágoras, pretende-se calcular as soluções inteiras positivas de:

$$X^2 + Y^2 = Z^2$$

Uma tal solução $[X, Y, Z]$ (se existir) é um ponto do círculo \mathcal{C} , com coordenadas inteiras. Reciprocamente, se $[X, Y, Z] \in \mathcal{C}$, em $\mathbb{P}_{\mathbb{Q}}^2$ então, multiplicando pelo mmc dos denominadores dos números racionais X, Y, Z obtemos números inteiros tais que $[X, Y, Z] \in \mathcal{C}$, e portanto uma solução para o problema - um **triângulo Pitagórico**.

Mas vimos antes que qualquer ponto da círculo \mathcal{C} é, ou $O = [-1, 0, 1]$, ou é da forma:

$$[X, Y, Z] = [1 - t^2, 2t, t^2 + 1]$$

para algum número racional $t = p/q \in \mathbb{Q}$. Obtemos pois todas as soluções inteiras pondo:

$$X = q^2 - p^2, \quad Y = 2pq, \quad Z = p^2 + q^2$$

Por exemplo, para $p = 1, q = 2$, obtem-se $3^2 + 4^2 = 5^2$, enquanto que, para $p = 2, q = 3$, vem $5^2 + 12^2 = 13^2$.

► **11.8 Problema de Fermat** ... Um problema célebre em teoria de números consiste em calcular todos os inteiros positivos X, Y, Z tais que:

$$X^n + Y^n = Z^n, \quad n \geq 3 \quad (11.6)$$

De forma equivalente, procuram-se pontos racionais positivos $x = X/Z, y = Y/Z$ na curva de Fermat $x^n + y^n = 1$ de grau n .

Fermat (1601-1665) escreveu na margem de um dos seus livros que tinha encontrado uma prova de que, para $n \geq 3$, a equação **não tem** soluções inteiras positivas.

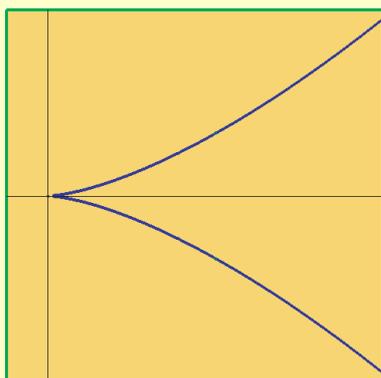
A técnica anterior não funciona uma vez que é possível demonstrar que, para $n \geq 3$, a curva de Fermat não admite uma parametrização racional. O problema foi resolvido por Wiles em 1996, que demonstrou que a conjectura de Fermat está de facto correcta!

► **11.9 Círculo $x^2 + y^2 = 3$** ... Este círculo não tem pontos racionais! Por outras palavras, não é possível que a soma dos quadrados de dois números racionais dê 3!

Tópico 12

Curvas algébricas planas afins. Mais exemplos

► 12.1 Cúspide ou Parábola semi-cúbica ...



É a curva:

$$\mathcal{C} = \{(x, y) \in \mathbb{K}^2 : x^3 - y^2 = 0\}$$

parametrizada por:

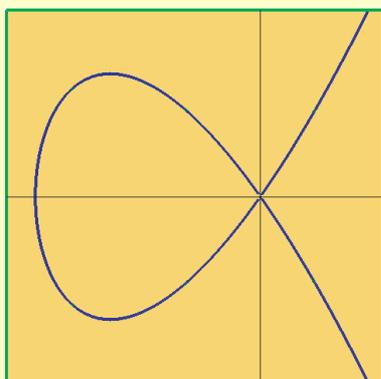
$$\varphi(t) = (t^2, t^3)$$

Para calcular esta parametrização polinomial, consideramos a intersecção da curva com as rectas $y = tx$, para cada t fixo. Obtemos:

$$0 = x^3 - t^2x^2 = x^2(x - t^2) \Rightarrow x = 0 \text{ ou } x = t^2$$

e portanto para $t = 0$ obtemos $(0, 0)$ e para $t \in \mathbb{K}$, o ponto $(x = t^2, y = tx = t^3)$.

► 12.2 Cúbica crunodal de Newton ...



É a curva:

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : y^2 - x^2(x + 1) = 0\}$$

parametrizada por:

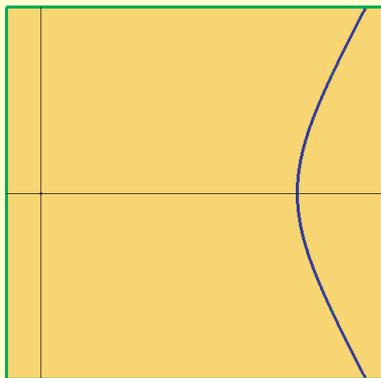
$$\varphi(t) = (t^2 - 1, t^3 - t)$$

Para calcular esta parametrização polinomial, consideramos a intersecção da curva com as rectas $y = tx$, para cada t fixo. Obtemos:

$$0 = x^2(x + 1 - t^2) \Rightarrow x = 0 \text{ ou } x = t^2 - 1$$

e portanto para $t = 0$ obtemos $(0, 0)$ e para $t \in \mathbb{k}$, o ponto $(x = t^2 - 1, y = tx = t^3 - t)$. Para traçar a curva, podemos determinar os pontos de intersecção com as rectas $x = \lambda$. Para $\lambda < -1$ não existem intersecções, para $\lambda = -1$ e $\lambda = 0$ existe um ponto de intersecção, e para todos os outros λ existem dois pontos de intersecção.

► **12.3 Cúbica acnodal ...**



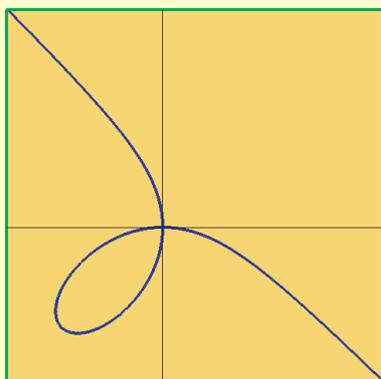
É a curva:

$$y^2 - x^2(x - 1) = 0$$

Uma parametrização polinomial é dada por:

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

► **12.4 Folium de Descartes ...**



É a curva

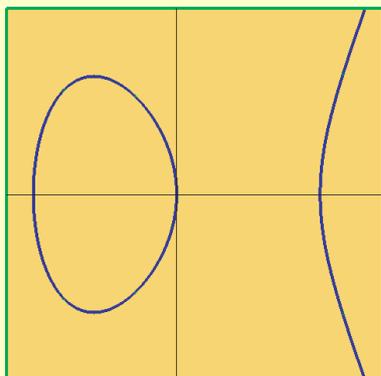
$$y^3 + x^3 + 3xy = 0$$

Uma parametrização racional é dada por:

$$x(t) = \frac{-3t}{1 + t^3}, \quad y(t) = tx(t) = \frac{-3t^2}{1 + t^3}$$

que pode ser obtida pelo mesmo processo.

► **12.5 Cúbica elíptica $y^2 - x(x^2 - 1) = 0$...**



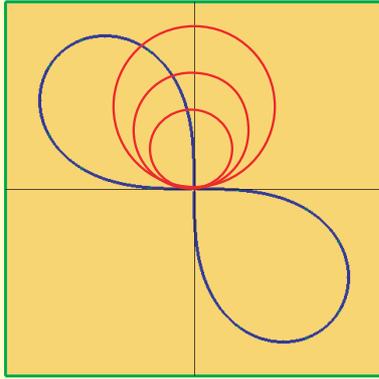
Consideremos a curva:

$$y^2 - x(x^2 - 1) = 0$$

Intersectando a curva com as rectas $x = t$, para cada valor fixo de t , obtemos a parametrização:

$$x = t, \quad y = \pm \sqrt{t(t^2 - 1)}$$

► **12.6 Quártica $xy + (x^2 + y^2)^2 = 0$...**



Consideremos a curva:

$$xy + (x^2 + y^2)^2 = 0$$

Uma parametrização racional é dada por:

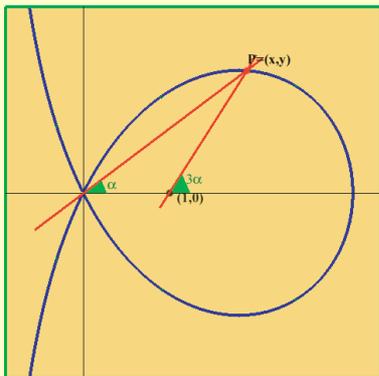
$$x(t) = \frac{-8t^3}{1 + 16t^4}, \quad y(t) = -\frac{x}{4t^2} = \frac{2t}{1 + 16t^4}$$

Esta parametrização pode ser obtida intersectando a curva com o feixe de círculos:

$$x^2 + (y - t)^2 - t^2 = x^2 + y^2 - 2ty = 0$$

Para cada t , este é o círculo centrado em $(0, t)$ e de raio t . Eliminando $x^2 + y^2$ entre a equação da curva e a equação do círculo, obtém-se $y(x + 4t^2y) = 0$. A solução $y = 0$ corresponde à intersecção na origem. A outra solução $y = -x/4t^2$, substituída na equação do círculo conduz à parametrização racional referida.

► 12.7 Trissectriz de MacLaurin ...



Consideremos a curva:

$$x^3 + xy^2 + y^2 - 3x^2 = 0$$

Na figura desenhamos duas rectas. A primeira passa no ponto $(1, 0)$, com declive $\tan 3\alpha$, e intersecta a curva no ponto P . Para trissectar o ângulo 3α , unimos P à origem, obtendo a segunda recta que tem declive $\tan \alpha$.

Tópico 13

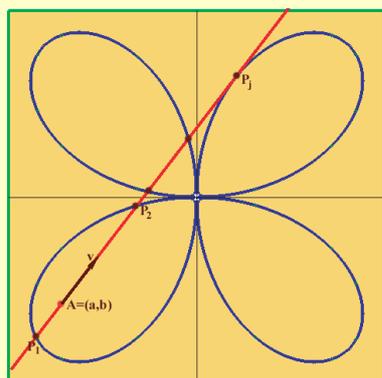
Curvas algébricas planas afins. Pontos simples e múltiplos

► **13.1 Intersecções com uma recta, pontos simples e múltiplos ...** Consideremos uma curva afim \mathcal{C} , em \mathbb{A}^2 , de equação $f(x, y) = 0$.

f é um polinómio de grau n , que escrevemos na forma:

$$f(x, y) = f_0 + f_1(x, y) + f_2(x, y) + \cdots + f_n(x, y) \quad (13.1)$$

onde f_j é homogéneo de grau j , e $f_n \neq 0$.



Seja ℓ a recta afim que passa no ponto $A = (a, b)$ e tem a direcção do vector $\mathbf{v} = (u, v)$, parametricamente definida por:

$$x = x(t) = a + ut, \quad y = y(t) = b + vt \quad (13.2)$$

Os valores do parâmetro t , correspondentes aos pontos de intersecção da recta ℓ com a curva \mathcal{C} , são as raízes da equação:

$$\phi(t) = f(a + ut, b + vt) = 0 \quad (13.3)$$

O polinómio $\phi \in \mathbb{k}[t]$, diz-se o **polinómio de intersecção** da recta ℓ com a curva \mathcal{C} . Será identicamente nulo se \mathcal{C} contem ℓ , caso que excluimos.

Caso contrário, ϕ tem grau $\leq n$ e portanto ℓ terá quando muito n pontos distintos de intersecção com \mathcal{C} .

Sejam P_1, P_2, \dots, P_r os pontos distintos de intersecção e t_1, t_2, \dots, t_r os respectivos parâmetros. A multiplicidade m_j da raiz t_j da equação (13.3), diz-se o **número de intersecção**, em P_j , da recta ℓ com a curva \mathcal{C} , e representa-se por $I_{P_j}(\ell \cap \mathcal{C})$.

$$I_{P_j}(\ell \cap \mathcal{C}) = \text{multiplicidade da raiz } t_j \text{ da equação (13.3)}$$

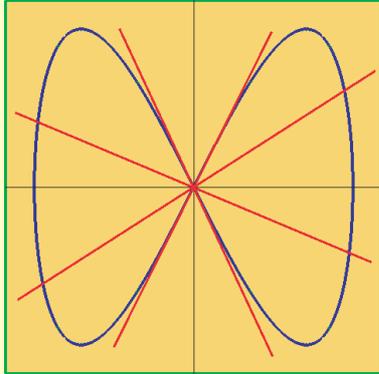
É fácil ver que $I_{P_j}(\ell \cap \mathcal{C})$ depende apenas do ponto P_j , sendo invariante por mudança do referencial afim e da parametrização afim para ℓ .

O **número (total) de intersecção** da recta ℓ com a curva \mathcal{C} , é, por definição:

$$I(\ell \cap \mathcal{C}) \stackrel{\text{def}}{=} \sum_j I_{P_j}(\ell \cap \mathcal{C})$$

Pelo exposto é $\leq n$.

► **13.2 Exemplo ...**



Consideremos a quártica afim (figura oito) \mathcal{C} , em $\mathbb{A}_{\mathbb{R}}^2$, de equação:

$$f(x, y) = y^2 - x^2 + x^4 = 0$$

e, para cada $\lambda \in \mathbb{R}$, a recta ℓ_λ , de equação $y = \lambda x$, parametrizada por $x = t, y = \lambda t$. O polinómio de intersecção da recta ℓ com a curva \mathcal{C} , é:

$$\phi_\lambda(t) = f(t, \lambda t) = \lambda^2 t^2 - t^2 + t^4$$

e as suas raízes, calculadas pela equação:

$$\lambda^2 t^2 - t^2 + t^4 = t^2(\lambda^2 - 1 + t^2) = 0$$

são:

- se $\lambda = \pm 1$, $t_1 = 0$, com multiplicidade 4, a que corresponde o ponto $P_1 = O = (0, 0)$.
Portanto:

$$I_O(\ell_{\pm 1} \cap \mathcal{C}) = 4$$

- se $\lambda \neq \pm 1$, $t_1 = 0$, com multiplicidade 2, a que corresponde o ponto $P_1 = O = (0, 0)$.
Portanto:

$$I_O(\ell_\lambda \cap \mathcal{C}) = 2, \quad \lambda \neq \pm 1$$

Se $-1 < \lambda < +1$, temos mais duas raízes reais $t_{2,3} = \pm\sqrt{1 - \lambda^2}$ a correspondem dois pontos simples, P_2, P_3 com número de intersecção 1. Por exemplo, para $\lambda = 0$, a recta ℓ_0 é o eixo dos xx que intersecta \mathcal{C} nos pontos $(-1, 0), (0, 0)$ e $(1, 0)$ com números de intersecção 1, 2, 1, respectivamente:

$$I_{(-1,0)}(\ell_0 \cap \mathcal{C}) = 1, \quad I_{(0,0)}(\ell_0 \cap \mathcal{C}) = 2, \quad I_{(+1,0)}(\ell_0 \cap \mathcal{C}) = 1$$

► **13.3 Multiplicidade de um ponto numa curva ...** Consideremos mais uma vez uma curva afim \mathcal{C} , em \mathbb{A}^2 , de equação $f(x, y) = 0$.

Fixemos um ponto $A = (a, b)$ em \mathcal{C} , de tal forma que $f(a, b) = 0$, e consideremos o feixe de rectas $\mathcal{F}(A)$ baseado em A .

Como A pertence a \mathcal{C} , temos automaticamente que $t = 0$ é raíz do polinómio de intersecção, isto é, $\phi(t) = t^{m_o}(\dots)$ e portanto:

$$I_A(\ell \cap \mathcal{C}) \geq 1, \quad \forall \ell \in \mathcal{F}(A)$$

A multiplicidade de A em \mathcal{C} define-se através de:

$$m(A) = m_{\mathcal{C}}(A) \stackrel{\text{def}}{=} \min \{I_A(\ell \cap \mathcal{C}), \ell \in \mathcal{F}(A)\} \quad (13.4)$$

Portanto $m(A) = m$, se $I_A(\ell \cap \mathcal{C}) \geq m, \forall \ell \in \mathcal{F}(A)$, e se existem rectas que passam por A , para as quais o respectivo número de intersecção satisfaz $I_A(\ell \cap \mathcal{C}) = m$.

Pontos de multiplicidade 1, 2, 3, 4, ... dizem-se pontos **simples**, **duplos**, **triplos**, **quádruplos**, ... de \mathcal{C} . Um ponto de multiplicidade m é, grosso modo, um ponto de \mathcal{C} onde m ramos da curva se auto-intersectam.

Por exemplo, na figura oito do número anterior, a multiplicidade da origem $O \in \mathcal{C}$ é 2: $m(O) = 2$. Portanto O é um ponto duplo da figura oito (verifique). Note, no entanto, que existem duas rectas, nomeadamente as rectas $y = \pm x$, cujo número de intersecção é 4.

► **13.4 Cálculo da multiplicidade de um ponto numa curva ...** Seja $\mathbf{v} = (u, v) \in \mathbb{K}^2$ um vector não nulo e consideremos a recta $\ell_{\mathbf{v}}$ do feixe $\mathcal{F}(A)$, que une os pontos $A = (a, b)$ e $A + \mathbf{v} = (a + u, b + v)$, parametrizada por:

$$x = a + tu, \quad y = b + tv$$

Como o ponto $A = (a, b)$ pertence a \mathcal{C} , então $\phi(0) = f(a, b) = 0$ e portanto $t = 0$ é raiz do polinómio de intersecção. Será uma raiz simples se o coeficiente de ϕ em t for não nulo. De acordo com a fórmula de Taylor:

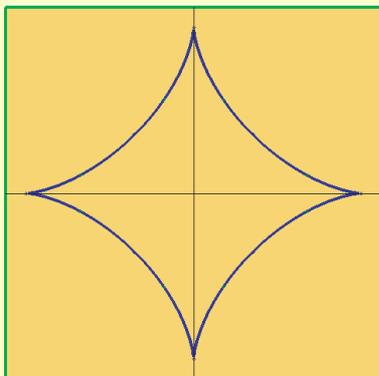
$$\begin{aligned} \phi(t) &= f(a + tu, b + tv) \\ &= \phi(0) + \phi'(0)t + \phi''(0)\frac{t^2}{2!} + \phi'''(0)\frac{t^3}{3!} + \dots \\ &= f(a, b) + t \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right) f(a, b) + \frac{t^2}{2!} \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right)^2 f(a, b) + \dots \\ &= f(A) + t(\mathbf{v} \cdot \nabla)f(A) + \frac{t^2}{2}(\mathbf{v} \cdot \nabla)^2 f(A) + \dots \\ &= t^m \Phi_m(u, v) + t^{m+1} \Phi_{m+1}(u, v) + \dots \end{aligned} \tag{13.5}$$

onde Φ_j é uma forma homogénea de grau j .

Claramente que t^m é um factor para todas as escolhas de u e v . Se existirem escolhas de u e v , isto é, de rectas $\ell_{\mathbf{v}}$ do feixe, para as quais $\Phi_m(u, v) \neq 0$, isto significa que, para essas escolhas, t^{m+1} não é factor de ϕ e, portanto, m será a multiplicidade de A em \mathcal{C} .

A fórmula (13.5) mostra ainda que a multiplicidade de $A \in \mathcal{C}$ é m se e só se todas as derivadas parciais de f de ordem $< m$ forem nulas, em A , e pelo menos uma derivada parcial de ordem m for não nula em A .

► **13.5 Exemplo ...**



Considere o astróide $(1 - x^2 - y^2)^3 - 27x^2y^2 = 0$. Vamos calcular a multiplicidade de $A = (a, b) = (1, 0)$, por exemplo. Procedendo como no número anterior, vem que:

$$\begin{aligned} \phi(t) &= f(1 + tu, tv) \\ &= (1 - (1 + tu)^2 - (tv)^2)^3 - 27(1 + tu)^2(tv)^2 \\ &= t^2(-27v^2) + t^3\Phi_3(u, v) + \dots \end{aligned} \tag{13.6}$$

donde se conclui que a multiplicidade de $A = (a, b) = (1, 0)$ é 2, isto é, A é ponto duplo de \mathcal{C} .

Note que para $v = 0$ obtemos a recta $(x, y) = (1, 0) + t(1, 0) = (1 + t, 0)$, isto é, o eixo dos xx , cujo número de intersecção, em A , com \mathcal{C} , é 3.

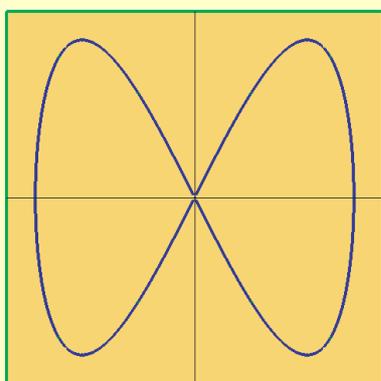
► **13.6 Pontos singulares** ... Um ponto $A \in \mathcal{C}$ diz-se **singular** se a sua multiplicidade for ≥ 2 .

A fórmula (13.5) mostra que $A = (a, b)$ é singular sse:

$$\begin{cases} f(a, b) = 0 \\ f_x(a, b) = 0 \\ f_y(a, b) = 0 \end{cases} \quad (13.7)$$

onde pusemos $f_x = \frac{\partial f}{\partial x}$ e $f_y = \frac{\partial f}{\partial y}$. Estas são as equações que permitem calcular os pontos singulares de \mathcal{C} .

► **13.7 Exemplo** ...



Calculemos os pontos singulares da figura oito \mathcal{C} , de equação:

$$f(x, y) = y^2 - x^2 + x^4 = 0$$

O sistema (13.7) é, pondo $a = x, b = y$:

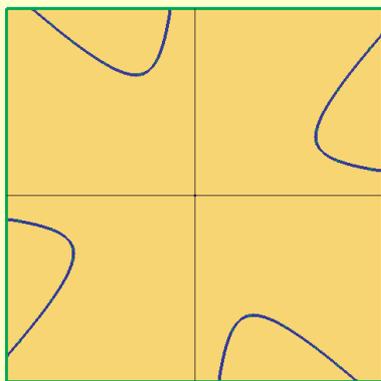
$$\begin{cases} y^2 - x^2 + x^4 = 0 \\ -2x + 4x^3 = 0 \\ 2y = 0 \end{cases}$$

donde se deduz que o único ponto singular é $(0, 0)$, cuja multiplicidade é 2. De facto:

$$f(tu, tv) = t^2(v^2 - u^2) + t^4u^4$$

Note que este ponto duplo é exactamente o ponto onde a curva se auto-intersecta.

► **13.8 Exemplo** ...



A cruz de Maltese é a quártica definida pela equação:

$$xy(x^2 - y^2) - (x^2 + y^2) = 0$$

Calculemos os seus pontos singulares. O sistema (13.7) é, pondo $a = x, b = y$:

$$\begin{cases} xy(x^2 - y^2) - (x^2 + y^2) = 0 \\ 3x^2 - y^3 - 2x = 0 \\ x^3 - 3xy^2 - 2y = 0 \end{cases}$$

Para resolver isto, notemos que $f = 0 \Rightarrow xf_x + yf_y = 0$, isto é:

$$0 = 4xy(x^2 - y^2) - 2(x^2 + y^2) = 2xy(x^2 - y^2)$$

donde $x = 0, y = 0$ ou $x = \pm y$. Em qualquer dos casos, $(0, 0)$ é o único ponto singular.

► **13.9 Exemplo** ... Qualquer curva em $\mathbb{A}_{\mathbb{R}}^2$ pode ser considerada como uma curva em $\mathbb{A}_{\mathbb{C}}^2$. Podem existir pontos singulares complexos não reais.

Por exemplo, para a curva:

$$f(x, y) = (1 + x^2)^2 - xy^2 = 0$$

o sistema (13.7) é:

$$\begin{cases} (1 + x^2)^2 - xy^2 & = & 0 \\ 4x(1 + x^2) - y^2 & = & 0 \\ -2xy & = & 0 \end{cases}$$

cujas soluções são $(0, 0)$ e $(\pm i, 0)$.

Tópico 14

Tangentes afins

► **14.1 Tangentes afins** ... Seja $A \in \mathcal{C}$ um ponto de multiplicidade m numa curva algébrica $\mathcal{C} : f(x, y) = 0$, em \mathbb{A}^2 .

Recorde que isto significa que m é o valor mínimo para o número de intersecção $I_A(\ell \cap \mathcal{C})$, quando ℓ varia no feixe de rectas $\mathcal{F}(A)$, que passam por A . Portanto:

$$I_A(\ell \cap \mathcal{C}) \geq m, \quad \forall \ell \in \mathcal{F}(A)$$

(e existem rectas deste feixe para as quais $I_A(\ell \cap \mathcal{C}) = m$). Uma recta ℓ que passa em A , diz-se uma **tangente** a \mathcal{C} em A se:

$$I_A(\ell \cap \mathcal{C}) \geq m + 1 \tag{14.1}$$

Diz-se que duas curvas \mathcal{C} e \mathcal{D} são tangentes num ponto comum A , se existe uma recta ℓ que seja simultâneamente tangente a \mathcal{C} e a \mathcal{D} em A .

► **14.2 Cálculo das tangentes num ponto simples** ... Suponhamos que $A = (a, b)$ é um ponto simples de \mathcal{C} , isto é, que $m = 1$. Uma recta ℓ que passa em A , é uma tangente a \mathcal{C} em A se:

$$I_A(\ell \cap \mathcal{C}) \geq 2$$

Suponhamos que a recta é definida por $\mathbf{v} = [u, v]$, isto é, que é parametrizada por:

$$x = a + tu, \quad y = b + tv$$

A equação cartesiana desta recta é:

$$-v(x - a) + u(y - b) = 0 \tag{14.2}$$

Como já se viu em (13.5), o polinómio de intersecção ϕ de \mathcal{C} com ℓ , em A , é:

$$\begin{aligned} \phi(t) &= f(a + tu, b + tv) \\ &= t \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right) f(a, b) + \frac{t^2}{2!} \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right)^2 f(a, b) + \dots \\ &= t\Phi_1(u, v) + t^2\Phi_2(u, v) + \dots \end{aligned}$$

Como, por hipótese, $m = 1$, sabemos que existem vectores (u, v) , tais que $\Phi_1(u, v) \neq 0$. Por outras palavras, existem rectas $\ell = \ell_{\mathbf{v}}$ cujo número de intersecção $I_A(\ell \cap \mathcal{C}) = 1$. Uma tangente em A é pois uma recta definida por uma direcção $\mathbf{v} = [u, v]$ para a qual:

$$\Phi_1(u, v) = u f_x(a, b) + v f_y(a, b) = 0$$

Daqui se deduz que:

$$[u, v] = [-f_y(a, b), f_x(a, b)]$$

e portanto, por (14.2), a equação da tangente é:

$$f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0 \quad (14.3)$$

► **14.3 Cálculo das tangentes num ponto duplo ...** Suponhamos que $A = (a, b)$ é um ponto duplo de \mathcal{C} , isto é, que $m = 2$. Uma recta ℓ que passa em A , é uma tangente a \mathcal{C} em A se:

$$I_A(\ell \cap \mathcal{C}) \geq 3$$

Suponhamos que a recta é definida por $\mathbf{v} = [u, v]$, isto é, que é parametrizada por:

$$x = a + tu, \quad y = b + tv$$

A equação cartesiana desta recta é:

$$-v(x - a) + u(y - b) = 0 \quad (14.4)$$

Como já se viu em (13.5), o polinómio de intersecção ϕ de \mathcal{C} com ℓ , em A , é:

$$\begin{aligned} \phi(t) &= f(a + tu, b + tv) \\ &= t \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right) f(a, b) + \frac{t^2}{2!} \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right)^2 f(a, b) + \dots \\ &= \frac{t^2}{2!} \Phi_2(u, v) + \dots \end{aligned}$$

Como, por hipótese, $m = 2$, sabemos que existem vectores (u, v) , tais que:

$$\Phi_2(u, v) = \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right)^2 f(a, b) \neq 0$$

Por outras palavras, existem rectas $\ell = \ell_{\mathbf{v}}$ cujo número de intersecção $I_A(\ell \cap \mathcal{C}) = 2$.

Uma tangente em A é uma recta tal que $I_A(\ell \cap \mathcal{C}) \geq 3$, e é pois definida por uma direcção $[u, v]$ para a qual:

$$\Phi_2(u, v) = u^2 f_{xx}(a, b) + 2uv f_{xy}(a, b) + v^2 f_{yy}(a, b) = 0$$

Este é um polinómio homogéneo de grau 2, nas variáveis u e v que, em \mathbb{C}^2 , se factoriza no produto de dois factores lineares, eventualmente iguais, digamos:

$$\Phi_2(u, v) = (\alpha u + \beta v)(\gamma u + \delta v)$$

forneendo por isso duas soluções $[u, v] = [-\beta, \alpha]$ e $[u, v] = [-\delta, \gamma]$. Quando substituídas em (14.4) conduzem às duas tangentes (eventualmente coincidentes):

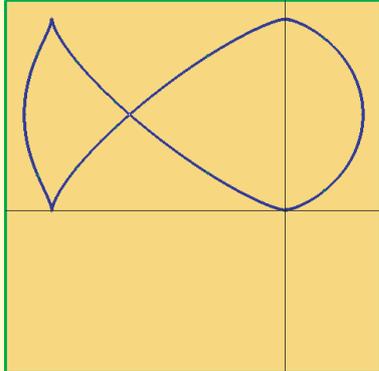
$$\alpha(x - a) + \beta(y - b) = 0, \quad \gamma(x - a) + \delta(y - b) = 0$$

Existem várias hipóteses:

- existem duas tangentes distintas. Neste caso, A diz-se um **nodo**. Se as tangentes forem ambas reais A diz-se um **crunodo**. Se forem complexas conjugadas, A diz-se um **acnodo**.

- As tangentes coincidem. Neste caso, A diz-se um **cúspide**.

► 14.4 Exemplo ...



Consideremos a curva de grau 6:

$$f(x, y) = y^3(4 - y)^3 - 4x^4(x + 3)^2 = 0$$

O ponto $A = (-2, 2)$ é um ponto duplo. O polinómio de intersecção é:

$$\phi(t) = f(-2 + tu, 2 + tv) = -24t^2(u^2 + 2v^2) + \dots$$

Como:

$$u^2 + 2v^2 = (u + i\sqrt{2}v)(u - i\sqrt{2}v)$$

obtemos as duas tangentes distintas:

$$(x + 2) \pm i\sqrt{2}(y - 2) = 0$$

Portanto A é um **acnodo**.

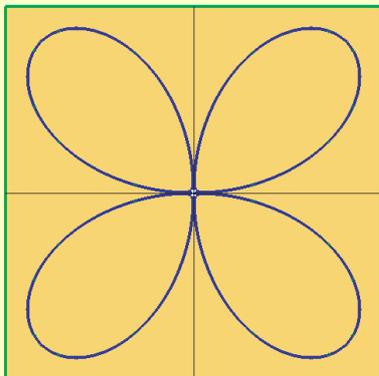
► 14.5 Cálculo das tangentes em pontos triplos, quádruplos, etc. ... Se $A = (a, b)$ é um ponto de multiplicidade m , um raciocínio semelhante mostra que as tangentes em A são obtidas a partir da factorização em factores lineares do polinómio homogéneo de grau m :

$$\begin{aligned} \Phi_m(u, v) &= \left(u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} \right)^m f(a, b) \\ &= (\alpha_1 u + \beta_1 v)^{m_1} \cdot (\alpha_2 u + \beta_2 v)^{m_2} \cdots (\alpha_k u + \beta_k v)^{m_k} \end{aligned}$$

onde os $[\alpha_j, \beta_j]$ são todos distintos e $m_1 + \dots + m_k = m$. As tangentes em A são pois:

$$\alpha_j(x - a) + \beta_j(y - b), \quad \text{com multiplicidade } m_j, \quad j = 1, 2, \dots, k$$

► 14.6 Exemplo ...



O trevo de quatro folhas é a curva de grau 6:

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

que tem um ponto quádruplo em $A = O = (0, 0)$ com as duas tangentes $x = 0$ e $y = 0$ ambas com multiplicidade 2 (verifique).

Tópico 15

Curvas planas projectivas. Tangentes

► **15.1 Forma de intersecção** ... Consideremos uma curva projectiva de grau n :

$$\mathcal{C} : F(X, Y, Z) = 0$$

em \mathbb{P}^2 , onde F é um polinómio homogéneo de grau n . A recta $\ell = AB$, determinada pelos pontos $A = [a_1, a_2, a_3]$ e $B = [b_1, b_2, b_3]$, pode ser parametrizada por:

$$(s, t) \longmapsto sA + tB \quad (15.1)$$

isto é:

$$X = sa_1 + tb_1, \quad Y = sa_2 + tb_2, \quad Z = sa_3 + tb_3 \quad (15.2)$$

e as intersecções de ℓ com \mathcal{C} são dadas pelas raízes do **polinómio de intersecção**:

$$\begin{aligned} \Phi(s, t) &= F(sA + tB) \\ &= F(sa_1 + tb_1, sa_2 + tb_2, sa_3 + tb_3) = 0 \end{aligned} \quad (15.3)$$

Como F é um polinómio homogéneo de grau n , tem-se que:

$$\Phi(\lambda s, \lambda t) = \lambda^n \Phi(s, t) \quad (15.4)$$

e portanto, a chamada **forma de intersecção** Φ , é uma forma binária de grau n , que admite, sobre \mathbb{C} , uma factorização em factores lineares do tipo:

$$\Phi(s, t) = (s_1 t - t_1 s)^{m_1} \cdot (s_2 t - t_2 s)^{m_2} \cdots (s_k t - t_k s)^{m_k} \quad (15.5)$$

onde os $[s_i, t_i]$ são distintos e $m_1 + \cdots + m_k = n$.

Portanto, sobre \mathbb{C} , a recta ℓ intersecta a curva \mathcal{C} em exactamente n pontos, contados com multiplicidades.

► **15.2 Números de intersecção** ... Como antes, se $[s_i, t_i]$ é uma raiz da forma de intersecção Φ , com multiplicidade m_i , a que corresponde o ponto $A_i = s_i A + t_i B \in \ell \cap \mathcal{C}$, pômos:

$$I_{A_i}(\ell \cap \mathcal{C}) = m_i \quad (15.6)$$

para o **número de intersecção** em A_i da recta ℓ com a curva \mathcal{C} .

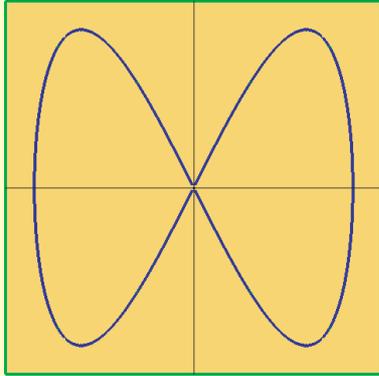
O número de intersecção é invariante por mudança projectiva de parâmetro, do tipo $U(s, t) = (u, v)$ com:

$$\begin{cases} u &= \alpha s + \gamma t \\ v &= \beta s + \delta t \end{cases}, \quad \alpha\delta - \beta\gamma \neq 0$$

O **número total de intersecção** de \mathcal{C} com ℓ é a soma dos números de intersecção $I_A(\ell \cap \mathcal{C})$, quando A percorre \mathcal{C} . Como vimos, quando a curva \mathcal{C} está em $\mathbb{P}^2(\mathbb{C})$ o número total de intersecção é igual a n , desde que ℓ não seja uma componente de \mathcal{C} .

► **15.3 Exemplo ...**

O fecho projectivo da figura oito \mathcal{C} : $f = y^2 - x^2 + x^4 = 0$, é a quártica $\widehat{\mathcal{C}}$:



$$F = Y^2Z^2 - X^2Z^2 + X^4 = 0$$

em \mathbb{P}^2 . Consideremos a recta $\ell : X = 0$, definida pelos pontos $A = [0, 0, 1]$ e $B = [0, 1, 0]$, ambos em $\widehat{\mathcal{C}}$, o último dos quais em \mathcal{C}_∞ . É parametrizada por:

$$X = 0, \quad Y = t, \quad Z = s$$

A forma de intersecção é $\Phi(s, t) = s^2t^2$ que tem grau 4. As suas raízes são $[0, 1]$ e $[1, 0]$, ambas com multiplicidade 2, correspondentes a A e B , respectivamente. Logo:

$$I_A(\ell \cap \mathcal{C}) = I_B(\ell \cap \mathcal{C}) = 2$$

► **15.4 Multiplicidade de um ponto numa curva ...** Seja A um ponto numa curva $\mathcal{C} : \{F = 0\}$ em \mathbb{P}^2 , e consideremos o feixe de rectas $\mathcal{F}(A)$ que passam em A .

A **multiplicidade de A** (em \mathcal{C}) é, por definição, o valor mínimo $m(A) = m_{\mathcal{C}}(A)$ dos números de intersecção $I_A(\ell \cap \mathcal{C})$, quando ℓ varia em $\mathcal{F}(A)$. Portanto:

$$m(A) = m$$

sse $I_A(\ell \cap \mathcal{C}) \geq m, \forall \ell \in \mathcal{F}(A)$ e se existe pelo menos uma recta do feixe $\mathcal{F}(A)$ para a qual $I_A(\ell \cap \mathcal{C}) = m$. Intuitivamente, uma recta genérica de $\mathcal{F}(A)$ intersecta a curva m vezes em A .

Pontos de multiplicidade 1, 2, 3, 4, ... dizem-se **simples, duplos, triplos, quádruplos**, etc...

Um ponto $A \in \mathcal{C}$ diz-se **singular** quando a sua multiplicidade é ≥ 2 . A curva diz-se **singular** quando tem um ponto singular. Caso contrário diz-se **não singular** ou **suave**.

► **15.5 Teorema ...** Um ponto $A \in \mathcal{C}$ é um ponto singular da curva $\mathcal{C} : F = 0$ se e só se:

$$F(A) = 0, \quad F_X(A) = 0, \quad F_Y(A) = 0, \quad F_Z(A) = 0 \tag{15.7}$$

Dem.: Seja $A = [a_1, a_2, a_3] \in \mathcal{C}$ e $B = [b_1, b_2, b_3]$ um outro ponto qualquer diferente de A . A forma de intersecção da recta AB com a curva \mathcal{C} é dada por:

$$\begin{aligned} \Phi(s, t) &= F(sA + tB) \\ &= s^n F_0(A, B) + s^{n-1}t F_1(A, B) + s^{n-2}t^2 F_2(A, B) + \dots + t^n F_n(A, B) \end{aligned} \tag{15.8}$$

onde cada $F_k(A, B)$ é um polinómio nas componentes de A e B (isto é, nas variáveis a_i e b_i).

O ponto A corresponde a $[s, t] = [1, 0]$ e o ponto B corresponde a $[s, t] = [0, 1]$. Como A pertence a \mathcal{C} a forma de intersecção anula-se em $[s, t] = [1, 0]$ e A será singular quando esta

solução tiver multiplicidade ≥ 2 , isto é, quando t^2 for factor de $\Phi(s, t)$. Mas isto acontece quando $F_0(A, B) = 0$ e também $F_1(A, B) = 0$. A condição $F_0(A, B) = 0$ é automática já que $A \in \mathcal{C}$. Resta interpretar a outra condição $F_1(A, B) = 0$. Seja:

$$\begin{aligned} \phi(t) &= \Phi(1, t) = F(A + tB) \\ &= F(A) + t(B \cdot \nabla)F(A) + \frac{t^2}{2!}(B \cdot \nabla)^2F(A) + \dots + \frac{t^k}{k!}(B \cdot \nabla)^kF(A) + \dots \end{aligned} \quad (15.9)$$

Daqui se deduz que:

$$\begin{aligned} F_0(A, B) &= F(A) \\ F_1(A, B) &= (B \cdot \nabla)F(A) \\ &= (b_1\partial_X + b_2\partial_Y + b_3\partial_Z)F(A) \\ F_2(A, B) &= (B \cdot \nabla)^2F(A) \\ &= (b_1\partial_X + b_2\partial_Y + b_3\partial_Z)^2F(A), \dots \end{aligned} \quad (15.10)$$

Como $F(A)=0$, A será ponto singular sse $(b_1\partial_X + b_2\partial_Y + b_3\partial_Z)F(A) = 0$, $\forall b_1, b_2, b_3$, isto é, sse $F_X(A) = 0$, $F_Y(A) = 0$, $F_Z(A) = 0$, como se pretendia.

► **15.6 Exemplo** ... O fecho projectivo da figura oito $f = y^2 - x^2 + x^4$ é a quártica:

$$F = Y^2Z^2 - X^2(Z^2 - X^2) = 0$$

em \mathbb{P}^2 , que intersecta a recta do infinito $Z = 0$, nos pontos que satisfazem:

$$Y^2Z^2 - X^2(Z^2 - X^2) = 0, \quad Z = 0$$

isto é, no ponto $A = [0, 1, 0]$.

Qual a multiplicidade $m(A)$, de A em \mathcal{C} ?

Consideremos a recta definida por este ponto e por um outro $B = [u, v, w]$, digamos, dada parametricamente por:

$$X = tu, \quad Y = s + tv, \quad Z = tw$$

Como já sabemos $[1, 0]$ é raiz da forma de intersecção $\Phi(s, t)$. Basta pois analisar a forma:

$$\begin{aligned} \phi(t) = \Phi(1, t) &= F(tu, 1 + tv, tw) \\ &= (1 + tv)^2(tw)^2 - (tu)^2((tw)^2 - (tu)^2) \\ &= t^2w^2 + t^3vw^2 + t^4(u^4 + u^2w^2) \end{aligned}$$

donde se deduz que $A = [0, 1, 0]$ é um ponto duplo - tem multiplicidade dois.

► **15.7 Exemplo: Cúbicas de Steiner** ... Considere a família de cúbicas de Steiner $\mathcal{C} = \mathcal{C}(\lambda, \mu)$, em $\mathbb{P}^2(\mathbb{C})$, dadas por:

$$F(X, Y, Z) = \mu(X^3 + Y^3 + Z^3) + 3\lambda XYZ \quad (15.11)$$

onde $\lambda, \mu \in \mathbb{C}$.

A curva $\mathcal{C}(\lambda, \mu)$ é singular se e só se $\mu = 0$ e $\lambda^3 = -1$, e, em cada um destes quatro casos, a curva reduz-se a um triângulo (reunião de 3 rectas não concorrentes).

Quando $\mu = 0$, a curva é dada por $XYZ = 0$ que é de facto um triângulo com pontos singulares nos vértices $[1, 0, 0]$, $[0, 1, 0]$ e $[0, 0, 1]$.

Suponhamos agora que $\mu \neq 0$. Podemos supôr que $\mu = 1$, é claro! Como sabemos, os pontos singulares são dados por $F = 0, F_X = 0, F_Y = 0$ e $F_Z = 0$, isto é:

$$X^2 = -\lambda YZ, \quad Y^2 = -\lambda ZX, \quad Z^2 = -\lambda XY \quad (15.12)$$

Se um dos X, Y ou Z é nulo então todos o são. Podemos pois supôr que todos são não nulos. Igualando o produto dos membros esquerdos das 3 igualdades anteriores, com os produtos dos três membros direitos, obtemos:

$$(1 + \lambda^3)X^2Y^2Z^2 = 0$$

Quando $\lambda^3 \neq -1$, um dos X, Y ou Z é nulo, o que é absurdo. Portanto, quando $\lambda^3 \neq -1$ a curva é não singular.

Suponhamos agora que $\lambda^3 = -1$. Multiplicando as 3 igualdades (15.12), respectivamente por X, Y e Z , obtemos:

$$X^3 = Y^3 = Z^3 = -\lambda XYZ$$

Sejam $1, \omega, \omega^2$ as raízes cúbicas da unidade. Então λ é igual a um dos números $-1, -\omega$ ou $-\omega^2$. Além disso, podemos supôr ainda que $X = 1$, de tal forma que Y e Z são iguais a um dos números $1, \omega$ ou ω^2 . Obtemos desta forma os seguintes pontos singulares:

$$\begin{cases} \lambda = -1 & [1, 1, 1] & [1, \omega, \omega^2] & [1, \omega^2, \omega] \\ \lambda = -\omega & [1, 1, \omega^2] & [1, \omega, \omega] & [1, \omega^2, 1] \\ \lambda = -\omega^2 & [1, 1, \omega] & [1, \omega, 1] & [1, \omega^2, \omega^2] \end{cases}$$

Em cada caso, temos 3 pontos não colineares; as rectas que unem cada par desses pontos intersectam \mathcal{C} em ≥ 4 pontos, e portanto têm que ser componentes de \mathcal{C} . Como \mathcal{C} tem grau 3, ela reduz-se, nestes casos, a um triângulo cujos vértices são os pontos singulares referidos.

► **15.8 Tangentes a uma curva ...** Seja $\mathcal{C} \{F = 0\}$ uma curva em \mathbb{P}^2 , e A um ponto de multiplicidade m em \mathcal{C} , de tal forma que $I_A(\ell \cap \mathcal{C}) \geq m$, para toda a recta $\ell \in \mathcal{F}(A)$ (e existem rectas deste feixe para as quais $I_A(\ell \cap \mathcal{C}) = m$).

Uma recta $\ell \in \mathcal{F}(A)$ diz-se tangente a \mathcal{C} em A , se:

$$I_A(\ell \cap \mathcal{C}) \geq m + 1 \quad (15.13)$$

► **15.9 Tangentes a uma curva num ponto simples ...** Seja A um ponto simples numa curva $\mathcal{C} : F = 0$ em \mathbb{P}^2 . De (15.9) ou (15.10) deduz-se imediatamente que única tangente a \mathcal{C} em A é dada pela equação:

$$XF_X(A) + YF_Y(A) + ZF_Z(A) = 0 \quad (15.14)$$

(apenas mudamos as notações: $(u, v, w) \rightarrow (X, Y, Z)$).

► **15.10 Tangentes a uma curva num ponto duplo ...** Seja A um ponto duplo numa curva $\mathcal{C} : F = 0$ em \mathbb{P}^2 . De (15.9) ou (15.10) deduz-se imediatamente que as tangentes a \mathcal{C} em A são dadas pela equação:

$$(XF_X + YF_Y + ZF_Z)^2(A) = 0 \quad (15.15)$$

(mudamos mais uma vez as notações: $(u, v, w) \rightarrow (X, Y, Z)$). Esta é uma forma quadrática que se factoriza em \mathbb{C} em dois factores lineares, digamos:

$$(XF_X + YF_Y + ZF_Z)^2(A) = (\alpha_1X + \alpha_2Y + \alpha_3Z)(\beta_1X + \beta_2Y + \beta_3Z) = 0$$

que fornecem as duas tangentes (eventualmente coincidentes).

O cálculo das tangentes em pontos de maior multiplicidade faz-se de forma análoga.

► **15.11 Exemplo** ... A curva $Y^2Z^2 - X^2(Z^2 - X^2) = 0$ tem dois pontos singulares em $A = [0, 0, 1]$ e $B = [0, 1, 0]$.

Em A a forma de intersecção é:

$$\begin{aligned}\phi(t) &= F(tX, tY, 1 + tZ) \\ &= (tY)^2(1 + tZ)^2 - (tX)^2(1 + tZ)^2 + (tX)^4 \\ &= t^2(Y^2 - X^2) + t^3(\dots)\end{aligned}\tag{15.16}$$

e as tangentes em A são dadas por $Y \pm X = 0$.

Em B a forma de intersecção é:

$$\begin{aligned}\phi(t) &= F(tX, 1 + tY, tZ) \\ &= (1 + tY)^2(tZ)^2 - (tX)^2(tZ)^2 + (tX)^4 \\ &= t^2Z^2 + t^3(\dots)\end{aligned}\tag{15.17}$$

e as tangentes em B são dadas por $Z = 0$ (contada duas vezes).

► **15.12 Exercício** ... A curva $(X^2 - Y^2)^2 + (2X^2 - 6Y^2)Z^2 = 0$ tem três pontos singulares em $A = [1, 1, 0]$, $B = [1, -1, 0]$ e $C = [0, 0, 1]$ todos duplos. Calcular as tangentes nesses pontos.

► **15.13 Assíntotas** ... Seja \mathcal{C} uma curva afim em \mathbb{A}^2 e $\widehat{\mathcal{C}}$ o seu fecho projectivo em \mathbb{P}^2 . Uma assíntota de \mathcal{C} , em \mathbb{A}^2 , é uma recta afim ℓ , cujo fecho projectivo $\widehat{\ell}$, é tangente num ponto $A \in \mathcal{C}_\infty = \widehat{\mathcal{C}} \cap \{Z = 0\}$.

Para calcular as assíntotas de \mathcal{C} , procede-se da seguinte forma

1. Calculamos os pontos $A \in \mathcal{C}_\infty = \widehat{\mathcal{C}} \cap \{Z = 0\}$
2. Calculamos as tangentes a $\widehat{\mathcal{C}}$ nesses pontos A .
3. As assíntotas são as tangentes que são diferentes de $Z = 0$.

► **15.14 Focos** ... Seja $\mathcal{C} : F = 0$ uma curva em \mathbb{P}^2 . Os focos de \mathcal{C} são os pontos de intersecção das tangentes a \mathcal{C} tiradas a partir dos pontos cíclicos $I, J = [1, \pm i, 0]$.

Tópico 16

Inflexões

► **16.1 Inflexões** ... Seja A um ponto simples ou suave de uma curva algébrica projectiva \mathcal{C} , em \mathbb{P}^2 . Como sabemos, o número de intersecção da única tangente $T_A\mathcal{C}$, a \mathcal{C} em A , é ≥ 2 :

$$I_A(T_A\mathcal{C} \cap \mathcal{C}) \geq 2$$

Em geral, este número de intersecção é exactamente igual a 2, mas poderá haver pontos exceptionais na curva onde seja superior a 2.

$A \in \mathcal{C}$ diz-se uma **inflexão** de \mathcal{C} se esse número é ≥ 3 :

$$I_A(T_A\mathcal{C} \cap \mathcal{C}) \geq 3 \quad (16.1)$$

Neste caso, a tangente $T_A\mathcal{C}$ diz-se uma **tangente inflexional** à curva \mathcal{C} .

A diz-se uma **inflexão ordinária** quando esse número é exactamente igual a 3 e uma **ondulação** quando é ≥ 4 .

Por exemplo, a origem é uma inflexão da curva $YZ^2 - X^3 = 0$, e o eixo dos X 's é a tangente inflexional nesse ponto.

► **16.2** Quando a curva é irredutível e de grau n , a ordem de contacto de qualquer tangente inflexional é ≥ 3 mas $\leq n$. Caso contrário a ordem de contacto torna-se infinita e a recta será uma componente de \mathcal{C} . Em particular, a ordem de contacto de uma tangente inflexional com uma cúbica irredutível é exactamente igual a 3 e todas as inflexões são por isso ordinárias ou simples.

► **16.3 Como determinar as inflexões? A Hessiana** ... Seja $\mathcal{C} : \{F(X, Y, Z) = 0\}$ uma curva em \mathbb{P}^2 . Uma aplicação sucessiva da identidade de Euler, a F e às suas derivadas parciais, permite obter as igualdades seguinte:

$$\begin{aligned} nF &= XF_X + YF_Y + ZF_Z, & \text{identidade de Euler} \\ (n-1)F_X &= XF_{X^2} + YF_{XY} + ZF_{XZ} \\ (n-1)F_Y &= XF_{YX^2} + YF_Y^2 + ZF_{YZ^2} \\ (n-1)F_Z &= XF_{ZX} + YF_{ZY} + ZF_Z^2 \\ n(n-1)F &= (n-1)(XF_X + YF_Y + ZF_Z) \\ &= (X^2F_{X^2} + XYF_{XY} + XZF_{XZ}) + (\dots) + (\dots) + \dots \\ &= X^2F_{X^2} + Y^2F_{Y^2} + Z^2F_{Z^2} + 2(XYF_{XY} + YZF_{YZ} + XZF_{XZ}) \\ &= \begin{pmatrix} X & Y & Z \end{pmatrix} \begin{pmatrix} F_{X^2} & F_{XY} & F_{XZ} \\ F_{YX} & F_{Y^2} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{Z^2} \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \end{aligned} \quad (16.2)$$

A forma homogénea de grau $3(n-2)$ definida por:

$$H_F = \det \begin{pmatrix} F_{X^2} & F_{XY} & F_{XZ} \\ F_{YX} & F_{Y^2} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{Z^2} \end{pmatrix} \quad (16.3)$$

diz-se o **determinante Hessiano** de F . A curva associada $\mathcal{H} = \mathcal{H}_\mathcal{C} : \{H_F = 0\}$ diz-se a **Hessiana** de \mathcal{C} .

► **16.4 Teorema [Critério para inflexões]** ... Um ponto não singular $A \in \mathcal{C}$ é uma inflexão de \mathcal{C} se e só se $A \in \mathcal{H}_\mathcal{C}$, isto é, sse:

$$H_F(A) = 0$$

Em particular, uma curva \mathcal{C} , de grau n , pode ter quando muito $3n(n-2)$ inflexões.

Dem.: Seja $A \in \mathcal{C}$ um ponto suave de \mathcal{C} e $T_A\mathcal{C} : XF_X(A) + YF_Y(A) + ZF_Z(A) = 0$ a única tangente a \mathcal{C} em A . Seja B um ponto variável nessa tangente, de tal forma que:

$$B \cdot \nabla F(A) = 0$$

Recorde que:

$$\begin{aligned} F(sA + tB) &= s^n F(A) + s^{n-1}t(B \cdot \nabla F)(A) + s^{n-2}t^2/2(B \cdot \nabla F)^2(A) + t^3(\dots) \\ &= \frac{1}{2}s^{n-2}t^2(B \cdot \nabla F)^2(A) + t^3(\dots) \end{aligned} \quad (16.4)$$

uma vez que $A \in \mathcal{C} \Rightarrow F(A) = 0$ e $B \in T_A\mathcal{C} \Rightarrow B \cdot \nabla F(A) = 0$.

A ordem de contacto da tangente $T_A\mathcal{C}$ com \mathcal{C} , em A , é a potência mínima de t que surge como factor em $F(sA + tB)$, no desenvolvimento (16.4). Mas esta potência mínima será ≥ 3 sse:

$$(B \cdot \nabla F)^2(A) = 0, \quad \forall B \in T_A\mathcal{C}$$

Mas isto implica que a cónica:

$$\begin{pmatrix} X & Y & Z \end{pmatrix} \begin{pmatrix} F_{X^2}(A) & F_{XY}(A) & F_{XZ}(A) \\ F_{YX}(A) & F_{Y^2}(A) & F_{YZ}(A) \\ F_{ZX}(A) & F_{ZY}(A) & F_{Z^2}(A) \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = 0 \quad (16.5)$$

é redutível, uma vez que os pontos $B \in T_P\mathcal{C}$ lhe pertencem. Em particular, tem-se que:

$$H_F(A) = \det \begin{pmatrix} F_{X^2}(A) & F_{XY}(A) & F_{XZ}(A) \\ F_{YX}(A) & F_{Y^2}(A) & F_{YZ}(A) \\ F_{ZX}(A) & F_{ZY}(A) & F_{Z^2}(A) \end{pmatrix} = 0$$

isto é, A pertence à Hessiana: $A \in \mathcal{H}_\mathcal{C}$.

► **16.5 Corolário** ... A Hessiana de uma cúbica é também uma cúbica. Portanto uma cúbica irredutível tem quando muito 9 inflexões.

► **16.6** As inflexões de \mathcal{C} são pois os pontos de intersecção de \mathcal{C} com a respectiva Hessiana $\mathcal{H}_\mathcal{C}$, que são regulares em \mathcal{C} . Na prática, calculamos as intersecções resolvendo os sistema:

$$\begin{cases} F(X, Y, Z) = 0 \\ H_F(X, Y, Z) = 0 \end{cases}$$

e eliminamos as que são singulares em \mathcal{C} .

► **16.7 Exemplo** ... Seja $\mathcal{C} : \{F = X^3 + Y^3 + Z^3 = 0\}$ a cúbica de Fermat. \mathcal{C} é suave e a Hessiana \mathcal{H} é dada por:

$$H_F = \det \begin{pmatrix} F_{X^2} & F_{XY} & F_{XZ} \\ F_{YX} & F_{Y^2} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{Z^2} \end{pmatrix} = 6^3 XYZ = 0$$

que é uma cúbica redutível, reunião das 3 rectas $X = 0, Y = 0$ e $Z = 0$. Os pontos de inflexão são os pontos de intersecção destas rectas com \mathcal{C} . A recta $Z = 0$ tem 3 pontos de inflexão:

$$[1, -1, 0], \quad [\omega, -1, 0], \quad [\omega^2, -1, 0]$$

onde ω é uma raiz cúbica da unidade.

Existem também 3 pontos de inflexão em cada uma das rectas $X = 0$ e $Y = 0$ e, portanto, existem ao todo 9 pontos de inflexão.

Três desses pontos são reais: $[1, -1, 0], [0, -1, 1]$ e $[-1, 0, 1]$.

Esta é uma situação típica. De facto, é possível provar que *toda a cúbica suave tem sempre exactamente três pontos de inflexão reais que são colineares*.

► **16.8 Exemplo** ... Consideremos a cúbica cuspidal:

$$F = Y^2Z - X^3 = 0$$

em \mathbb{P}^2 . O único ponto singular é $A = [0, 0, 1]$. A Hessiana é:

$$H = \det \begin{pmatrix} -6X & 0 & 0 \\ 0 & 2Z & 2Y \\ 0 & 2Y & 0 \end{pmatrix} = 24XY^2 = 0$$

que é a reunião das rectas $X = 0$ e $Y = 0$. A cúbica intersecta a recta $X = 0$ quando $Y^2Z = 0$, isto é, quando $Y = 0$ ou $Z = 0$, o que dá o ponto suave $A = [0, 1, 0]$ e o ponto singular $B = [0, 0, 1]$. O ponto A é pois o único ponto da intersecção de \mathcal{C} com \mathcal{H} que é suave em \mathcal{C} e é pois a única inflexão de \mathcal{C} .

► **16.9 Exemplo** ... Consideremos a cúbica irredutível (folium de Descartes):

$$F = X^3 + Y^3 - XYZ = 0$$

em \mathbb{P}^2 . O único ponto singular é $A = [0, 0, 1]$, que é um nodo com tangentes $X = 0$ e $Y = 0$. A Hessiana é:

$$H = \det \begin{pmatrix} 6X & -Z & -Y \\ -Z & 6Y & -X \\ -Y & -X & 0 \end{pmatrix} = -2\{3(X^3 + Y^3) + XYZ\} = 0$$

As intersecções de \mathcal{C} com \mathcal{H} são dadas por $X^3 + Y^3 = 0, XYZ = 0$. A última equação dá $X = 0, Y = 0$ ou $Z = 0$. Claramente que $X = 0, Y = 0$ conduz apenas ao ponto singular A . No entanto, $Z = 0$ produz os 3 pontos colineares $B = [1, -1, 0], C = [1, -\omega, 0]$ e $D = [1, -\omega^2, 0]$, onde ω é uma raiz cúbica complexa da unidade. Os pontos B, C, D são suaves em \mathcal{C} , por serem distintos de A , e são pois as 3 inflexões de \mathcal{C} .

► **16.10 Cúbicas de Steiner** ... No número (15.7) consideramos a família de cúbicas de Steiner $\mathcal{C} = \mathcal{C}(\lambda, \mu)$, em $\mathbb{P}^2(\mathbb{C})$, dadas por:

$$F(X, Y, Z) = \mu(X^3 + Y^3 + Z^3) + 3\lambda XYZ \quad (16.6)$$

onde $\lambda, \mu \in \mathbb{C}$.

Mostramos aí que a curva $\mathcal{C}(\lambda, \mu)$ é singular se e só se $\mu = 0$ e $\lambda^3 = -1$, e, em cada um destes quatro casos, a curva reduz-se a um triângulo (reunião de 3 rectas não concorrentes).

Vamos agora determinar as inflexões das cúbicas de Steiner. Supômos que \mathcal{C} é não singular, de tal forma que $\mu = 1$ e $\lambda^3 \neq -1$. O Hessiano é:

$$H_F = \det \begin{pmatrix} 6X & 3\lambda Z & 3\lambda Y \\ 3\lambda Z & 6Y & 3\lambda X \\ 3\lambda Y & 3\lambda X & 6Z \end{pmatrix} = 27(-2\lambda^2(X^3 + Y^3 + Z^3) + 2(4 + \lambda^3)XYZ)$$

Para calcular as inflexões temso que resolver asa equações:

$$\begin{cases} (X^3 + Y^3 + Z^3) + 3\lambda XYZ & = 0 \\ -2\lambda^2(X^3 + Y^3 + Z^3) + 2(4 + \lambda^3)XYZ & = 0 \end{cases}$$

Note que quer F quer H_F são combinações lineares das cúbicas $X^3 + Y^3 + Z^3$ e XYZ . O determinante da matriz dos coeficientes do sistema anterior é:

$$\det \begin{pmatrix} 1 & 3\lambda \\ -2\lambda^2 & 2(4 + \lambda^3) \end{pmatrix} = 2(4 + \lambda^3) + 6\lambda^3 = 8 + 8\lambda^3$$

Portanto é não nulo uma vez que estamos a supôr que $\lambda^3 \neq -1$. As intersecções de \mathcal{C} com \mathcal{H} são dadas portanto por

$$\begin{cases} X^3 + Y^3 + Z^3 & = 0 \\ XYZ & = 0 \end{cases}$$

Se $X = 0$, então $Y^3 + Z^3 = 0$ e tomando $Z = 1$, vem que $Y^3 = -1$, isto é, $Y = -1$, $Y = -\omega$ ou $Y = -\omega^2$, onde ω é uma raiz da unidade. Procedendo de forma análoga para os casos $Y = 0$ e $Z = 0$, obtemos as nove inflexões seguintes:

$$\begin{array}{lll} I_{11} = [0, -1, 1] & I_{12} = [0, -\omega, 1] & I_{13} = [0, -\omega^2, 1] \quad \text{na recta } X = 0 \\ I_{21} = [1, 0, -1] & I_{22} = [1, 0, -\omega] & I_{23} = [1, 0, -\omega^2] \quad \text{na recta } Y = 0 \\ I_{31} = [-1, 1, 0] & I_{32} = [-\omega, 1, 0] & I_{33} = [-\omega^2, 1, 0] \quad \text{na recta } Z = 0 \end{array}$$

Note que estas nove inflexões não dependem de λ . Apenas três (as da primeira coluna) são reais e apenas I_{11} e I_{21} são visíveis na vista afim $Z = 1$.

Note ainda que:

- os pontos das primeira, segunda e terceira linha pertencem, respectivamente, às rectas $X = 0, Y = 0$ e $Z = 0$.
- os pontos das primeira, segunda e terceira coluna pertencem, respectivamente, às rectas $X + Y + Z, \omega X + \omega^2 Y + Z = 0$ e $\omega^2 X + \omega Y + Z = 0$.
- os pontos das duas diagonais principais pertencem, respectivamente, às rectas $\omega X + Y + Z = 0$ e $\omega X + \omega Y + Z = 0$.

É possível mostrar até que *a recta que passa em duas quaisquer das nove inflexões, passa exactamente por uma outra.*

As nove inflexões das cúbicas de Steiner são pois um exemplo da chamada **configuração de nove pontos**, isto é, de uma configuração constituída por nove pontos distintos de $\mathbb{P}^2(\mathbb{C})$ que tem a propriedade de que a recta que passa em dois quaisquer desses pontos passa exactamente por um outro.

Tópico 17

Teorema de Bézout. Aplicações

► **17.1 Lema** ... Consideremos dois polinómios $f, g \in \mathbb{D}[t]$, com coeficientes num anel de factorização única \mathbb{D} . Então f e g têm um factor comum não constante se e só se existem polinómios não nulos α e β , com $\deg \alpha < \deg f$ e $\deg \beta < \deg g$, tais que:

$$f\beta = g\alpha \quad (17.1)$$

Dem.: suponhamos que f e g têm um factor comum h não constante, de tal forma que existem polinómios não nulos α e β , com $\deg \alpha < \deg f$ e $\deg \beta < \deg g$

$$f = h\alpha \quad \text{e} \quad g = h\beta$$

Então $f\beta = h\alpha\beta = h\beta\alpha = g\alpha$.

Reciprocamente, suponhamos que existem α e β tais que $f\beta = g\alpha$. Todos estes polinómios têm factorizações únicas em irredutíveis. Os factores de g têm que aparecer nos factores de $f\beta$, mas não podem estar todos nos factores de β uma vez que $\deg \beta < \deg g$. Portanto, pelo menos um factor de g deve aparecer entre os factores de f , i.e., f e g têm um factor comum.

► **17.2** Para manter a discussão o mais concretamente possível, suponhamos que:

$$\begin{aligned} f(t) &= A_0t^3 + A_1t^2 + A_2t + A_3 \\ g(t) &= B_0t^2 + B_1t + B_2 \end{aligned} \quad (17.2)$$

A condição:

$$f\beta = g\alpha$$

com $\deg \alpha < \deg f$ e $\deg \beta < \deg g$, digamos:

$$\begin{aligned} \alpha(t) &= \alpha_0t^2 + \alpha_1t + \alpha_2 \\ \beta(t) &= \beta_0t + \beta_1 \end{aligned} \quad (17.3)$$

traduz-se na condição:

$$(A_0t^3 + A_1t^2 + A_2t + A_3)(\beta_0t + \beta_1) = (B_0t^2 + B_1t + B_2)(\alpha_0t^2 + \alpha_1t + \alpha_2)$$

ou ainda, igualando coeficientes, no sistema:

$$\begin{cases} A_3\beta_1 & - & B_2\alpha_2 & & & = & 0 \\ A_2\beta_1 + A_3\beta_0 & - & B_1\alpha_2 - B_2\alpha_1 & & & = & 0 \\ A_1\beta_1 + A_2\beta_0 & - & B_0\alpha_2 - B_1\alpha_1 - B_2\alpha_0 & & & = & 0 \\ A_0\beta_1 + A_1\beta_0 & & & - & B_0\alpha_1 - B_1\alpha_0 & = & 0 \\ & & A_0\beta_0 & & & - & B_0\alpha_0 = 0 \end{cases} \quad (17.4)$$

urualmente por $R(X, Y)$:

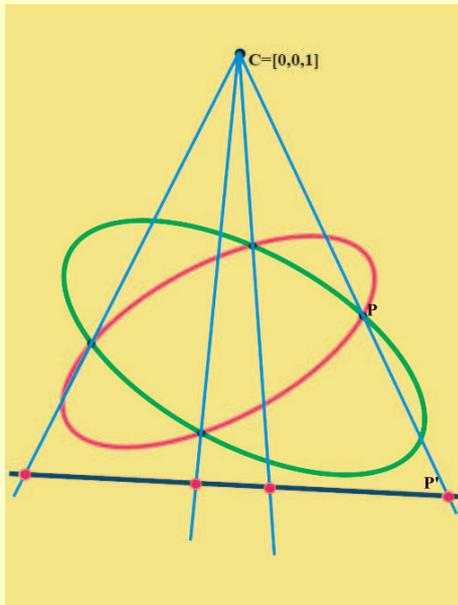
$$\begin{aligned}
 R(\lambda X, \lambda Y) &= \det \begin{pmatrix} \lambda^3 A_3 & & \lambda^2 B_2 & & \\ \lambda^2 A_2 & \lambda^3 A_3 & \lambda B_1 & \lambda^2 B_2 & \\ \lambda A_1 & \lambda^2 A_2 & B_0 & \lambda B_1 & \lambda^2 B_2 \\ A_0 & \lambda A_1 & & B_0 & \lambda B_1 \\ & A_0 & & & B_0 \end{pmatrix} \\
 &= \lambda^{-2} \lambda^{-1} \lambda^{-3} \lambda^{-2} \lambda^{-1} \det \begin{pmatrix} \lambda^5 A_3 & & \lambda^5 B_2 & & \\ \lambda^4 A_2 & \lambda^4 A_3 & \lambda^4 B_1 & \lambda^4 B_2 & \\ \lambda^3 A_1 & \lambda^3 A_2 & \lambda^3 B_0 & \lambda^3 B_1 & \lambda^3 B_2 \\ \lambda^2 A_0 & \lambda^2 A_1 & & \lambda^2 B_0 & \lambda^2 B_1 \\ & \lambda A_0 & & & \lambda B_0 \end{pmatrix} \\
 &= \lambda^{-9} \lambda^5 \lambda^4 \lambda^3 \lambda^2 \lambda \det \begin{pmatrix} A_3 & & B_2 & & \\ A_2 & A_3 & B_1 & B_2 & \\ A_1 & A_2 & B_0 & B_1 & B_2 \\ A_0 & A_1 & & B_0 & B_1 \\ & A_0 & & & B_0 \end{pmatrix} \\
 &= \lambda^6 R(X, Y)
 \end{aligned} \tag{17.9}$$

A segunda igualdade foi obtida multiplicando a primeira coluna e a quarta por λ^2 , a segunda e a quinta por λ e a terceira por λ^3 . A segunda igualdade foi obtida observando que a primeira linha aparece multiplicada por λ^5 , a segunda por λ^4 , etc.

A conclusão é pois que R é homogêneo de grau $\deg F \times \deg G = 3 \times 2 = 6$. O mesmo tipo de argumento pode ser usado no caso geral:

► **17.6 Teorema** ... Sejam $F, G \in \mathbb{k}[X, Y, Z] \simeq \mathbb{k}[X, Y][Z]$, dois polinômios homogêneos de graus m e n , respectivamente, vistos como polinômios na indeterminada Z , com coeficientes no anel $\mathbb{D} = \mathbb{k}[X, Y]$. Então a resultante $R(X, Y)$, de F e G , relativamente a Z , ou é nula ou é um polinômio homogêneo de grau mn .

► **17.7 Interpretação geométrica** ...



Consideremos a projecção central Π_C de centro C sobre uma recta ℓ , que não contém C :

$$\begin{aligned}
 \Pi_C : \mathbb{P}^2 - \{C\} &\rightarrow \ell \\
 P &\mapsto P' = CP \cap \ell
 \end{aligned}$$

Podemos supôr que $C = [0, 0, 1]$ e que $\ell : Z = 0$. de tal forma que, se $P = [X, Y, Z]$, então:

$$\Pi_C[X, Y, Z] = [X, Y, 0]$$

Sejam \mathcal{C} e \mathcal{D} duas curvas em $\mathbb{P}^2(\mathbb{C})$, sem componente comum, dadas por:

$$F(X, Y, Z) = 0, \quad G(X, Y, Z) = 0$$

onde F, G são dois polinômios homogêneos de graus m e n , respectivamente:

$$\begin{aligned} F(X, Y, Z) &= A_0(X, Y)Z^m + A_1(X, Y)Z^{m-1} + \dots + A_m(X, Y) \\ G(X, Y, Z) &= B_0(X, Y)Z^n + B_1(X, Y)Z^{n-1} + \dots + B_n(X, Y) \end{aligned} \quad (17.10)$$

Podemos supôr que C não pertence a qualquer das duas curvas, o que significa que $A_0 \neq 0$ e $B_0 \neq 0$. A recta que une o ponto $P' = [X, Y, 0] \in \ell$ ao ponto $C = [0, 0, 1]$ pode ser parametrizada por Z :

$$Z \mapsto [X, Y, 0] + Z[0, 0, 1] = [X, Y, Z]$$

Daí o desenvolvermos os polinómios F e G segundo a variável Z , para cada $P' = [X, Y, 0] \in \ell$ fixo. Para detectarmos se existe um ponto $P \in \mathcal{C} \cap \mathcal{D}$ na recta $P'C$, podemos pois recorrer à resultante (relativamente a Z) dos dois polinómios F e G .

De facto, existe um tal ponto P se e só se os polinómios F e G , vistos como polinómios em Z (para X e Y fixos), tiverem uma raíz comum Z , e isto acontece sse $R(X, Y) = 0$. Por outro lado, para cada $P' = [X, Y, 0] \in \ell$ fixo só pode haver um número finito de pontos $P \in \mathcal{C} \cap \mathcal{D}$. Caso contrário a recta $P'C$ seria uma componente de $\mathcal{C} \cap \mathcal{D}$. Concluindo: $\#(\mathcal{C} \cap \mathcal{D})$ é finito.

Contemos agora os pontos de intersecção das duas curvas. Existe apenas um número finito de rectas que os unem uns aos outros. Escolhendo coordenadas de tal forma que C não pertença a qualquer dessas rectas, podemos supôr que existe quando muito um ponto de intersecção em cada recta $P'C$. Por outras palavras, existem quando muito tantas intersecções quantos os zeros da resultante $R(X, Y)$. Como $\deg R = mn$, deduzimos o seguinte:

► **17.8 Teorema** ... Se \mathcal{C} e \mathcal{D} são duas curvas em $\mathbb{P}^2(\mathbb{C})$, sem componente comum, então:

$$\#(\mathcal{C} \cap \mathcal{D}) \leq \deg \mathcal{C} \cdot \deg \mathcal{D} \quad (17.11)$$

Contemos agora os pontos de intersecção com as respectivas multiplicidades.

► **17.9 Número (ou multiplicidade) de intersecção** $I_A(\mathcal{C} \cap \mathcal{D})$... Sejam \mathcal{C} e \mathcal{D} duas curvas em $\mathbb{P}^2(\mathbb{C})$, sem componente comum, dadas por:

$$F(X, Y, Z) = 0, \quad G(X, Y, Z) = 0$$

onde F, G são dois polinómios homogêneos de graus m e n , respectivamente.

Suponhamos ainda que $C = [0, 0, 1]$ não pertence a qualquer das duas curvas e que em cada recta $P'C$ existe quando muito um ponto de intersecção.

Se $A = [X, Y, Z] \in \mathcal{C} \cap \mathcal{D}$, define-se o **número (ou multiplicidade) de intersecção** $I_A(\mathcal{C} \cap \mathcal{D})$, através de:

$$I_A(\mathcal{C} \cap \mathcal{D}) \stackrel{\text{def}}{=} \text{multiplicidade de } (X, Y) \text{ como raíz de } R(X, Y) \quad (17.12)$$

► **17.10** O número de intersecção $I_A(\mathcal{C} \cap \mathcal{D})$ satisfaz as propriedades seguintes:

- Se $A \notin \mathcal{C} \cap \mathcal{D}$, então $I_A(\mathcal{C} \cap \mathcal{D}) = 0$.
- Se $A \in \mathcal{C} \cap \mathcal{D}$, e se \mathcal{C} e \mathcal{D} se intersectam transversalmente em A , simbolicamente:

$$P \in \mathcal{C}_1 \pitchfork \mathcal{C}_2$$

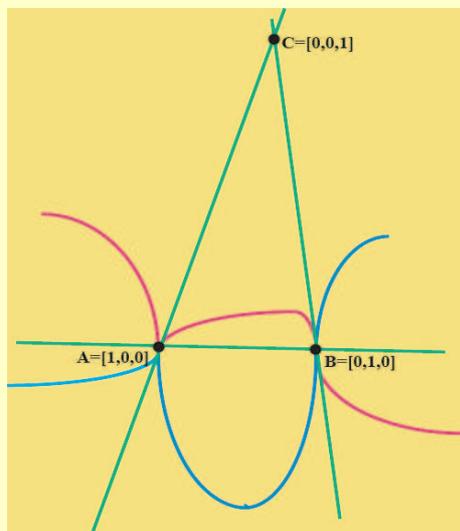
isto é, se A é ponto regular quer de \mathcal{C} , quer de \mathcal{D} , e as rectas tangentes em A , a \mathcal{C} e \mathcal{D} são distintas, então

$$I_A(\mathcal{C} \pitchfork \mathcal{D}) = 1$$

- Se $A \in \mathcal{C} \cap \mathcal{D}$, mas se \mathcal{C} e \mathcal{D} não se intersectam transversalmente em A , então

$$I_A(\mathcal{C} \cap \mathcal{D}) \geq 2$$

► **17.11 Exemplo**



Sejam $\mathcal{C} : F(X, Y, Z) = Z^3 - XY^2$ e $\mathcal{D} : G(X, Y, Z) = Z^3 + XY^2$. Então:

$$R(X, Y) = 8X^3Y^6$$

As duas cúbicas intersectam-se em:

$$\begin{aligned} A &= [1, 0, 0] && \text{com multiplicidade } 6 \\ B &= [0, 1, 0] && \text{com multiplicidade } 3 \end{aligned}$$

O ponto $B = [0, 1, 0]$ é uma inflexão comum a tangente $X = 0$.

► **17.12 Teorema de Bézout ...** Sejam \mathcal{C} e \mathcal{D} duas curvas projectivas sem componente comum. Então:

$$\sum_{A \in \mathcal{C} \cap \mathcal{D}} I_A(\mathcal{C} \cap \mathcal{D}) = (\deg \mathcal{C}) \cdot (\deg \mathcal{D}) \quad (17.13)$$

onde a soma se faz sobre todos os pontos de $\mathcal{C} \cap \mathcal{D}$ que têm coordenadas complexas. Em particular, se \mathcal{C} e \mathcal{D} são curvas regulares com intersecções todas transversais, então:

$$\#(\mathcal{C} \cap \mathcal{D}) = (\deg \mathcal{C}) \cdot (\deg \mathcal{D}) \quad (17.14)$$

Dois curvas intersectam-se em pelo menos um ponto.

► **17.13** Muitas vezes o teorema de Bézout é usado para determinar se duas curvas são de facto a mesma, ou, pelo menos, se têm uma componente comum.

► **17.14 Exemplo ...** Suponhamos que \mathcal{C} e \mathcal{D} são duas cónicas que têm 5 pontos distintos comuns. O teorema de Bézout diz que que elas têm uma componente comum. Como o grau de uma componente tem que ser inferior ao grau da curva de que faz parte, concluímos que

- ou existe uma recta ℓ tal que $\mathcal{C} \cap \mathcal{D} = \ell$, ou
- $\mathcal{C} = \mathcal{D}$.

Portanto:

existe uma única cónica que passa por 5 pontos dados, desde que não haja 3 colineares.

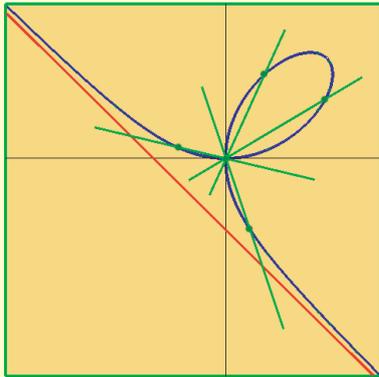
► **17.15** Mais geralmente, se \mathcal{C} e \mathcal{D} são duas curvas irredutíveis, ambas de grau n , que têm $n^2 + 1$ pontos distintos comuns, então $\mathcal{C} = \mathcal{D}$.

Note, no entanto, que para $n \geq 3$ não existe, em geral, nenhuma curva de grau n que passe em $n^2 + 1$ pontos dados. De facto, o número de condições impostas, $n^2 + 1$, é maior do que o número $\frac{1}{2}(n+1)(n+2)$ de coeficientes a determinar num polinómio homogéneo de grau n .

► **17.16 Aplicação ...** Uma cúbica tem quando muito um ponto duplo. De facto, se tivesse 2 pontos duplos a recta que os une intersectaria a curva em 4 pontos, o que é absurdo, uma vez que a curva é irreduzível.

Quando uma cúbica tem exactamente um ponto duplo, uma recta arbitrária que por ele passa, cuja equação contém um certo parâmetro $t \in \mathbb{P}^1$, intersecta a cúbica num outro ponto. Desta forma se exprime parametricamente um ponto arbitrário da curva como função do parâmetro t .

► **17.17 Exemplo ...**



A cúbica:

$$F = X^3 + Y^3 - XYZ = 0$$

tem um ponto duplo em $[0, 0, 1]$. Consideremos o feixe de rectas que passa por esse ponto:

$$Y - tX = 0$$

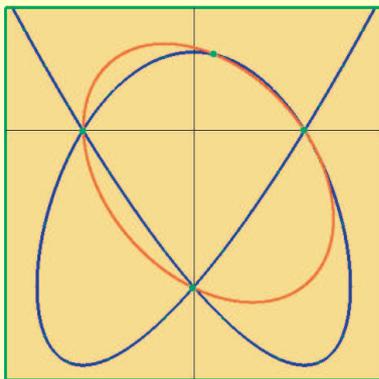
Para cada t , a recta $Y = tX$ intersecta a curva duas vezes em $[0, 0, 1]$ e uma outra vez no ponto

$$X = t, \quad Y = t^2, \quad Z = 1 + t^3$$

► **17.18 Aplicação ...** Uma quártica tem quando muito $\frac{1}{2}(4-1)(4-2) = 3$ pontos duplos. De facto, se tivesse 4 pontos duplos a cónica que passa por eles e por um quinto ponto da curva, intersectá-la-ia 9 pontos, o que é absurdo, uma vez que a curva é irreduzível.

Quando uma quártica tem exactamente 3 pontos duplos, uma cónica arbitrária, cuja equação contém um certo parâmetro $t \in \mathbb{P}^1$, que por eles passa e por um quarto ponto fixo da curva, intersecta-a num outro ponto que pode portanto ser expresso como função do parâmetro t .

► **17.19 Exemplo ...**



A quártica

$$F = Y^2Z(2Y + 3Z) - (X^2 - Z^2)^2 = 0$$

tem 3 pontos duplos em $[1, 0, 1]$, $[-1, 0, 1]$ e $[0, -1, 1]$. Consideremos ainda o ponto $[0, 1, 0]$ o feixe de cónicas que passam por estes quatro pontos. A equação de uma cónica é:

$$aX^2 + bY^2 + cZ^2 + 2fYZ + 2gZX + 2hXY = 0$$

e impondo que ela passe pelos 4 pontos referidos, obtemos $b = 0, g = 0$, e se tomarmos $a = 1$, então $c = 1$ e $2f = -1$. A equação da cónica é então, em coordenadas não homogéneas:

$$x^2 + 2hxy - y - 1 = 0$$

que pode ser escrita na forma:

$$xy + t(x^2 - y - 1) = 0$$

Tópico 18

Teorema dos nove pontos. Aplicações

► **18.1** Uma curva projectiva \mathcal{C} , em $\mathbb{P}^2(\mathbb{C})$, é representada em coordenadas homogéneas por um polinómio homogéneo de grau n :

$$F(X, Y, Z) = a_0 X^n + a_1 X^{n-1} Y + \dots + a_N Y^n$$

onde $N = \frac{1}{2}(n+1)(n+2)$.

Por exemplo, uma cúbica é dada por:

$$aX^3 + bY^3 + cZ^3 + eX^2Y + fXY^2 + gX^2Z + hXZ^2 + kY^2Z + lYZ^2 + mXYZ \quad (18.1)$$

onde figuram ao todo $N = \frac{1}{2}(3+1)(3+2) = 10$ coeficientes a, b, c, \dots . No entanto estes coeficientes estão definidos a menos da multiplicação por um escalar não nulo. Portanto apenas 9 são essenciais e daí que o conjunto \mathfrak{C}_3 de todas as cúbicas de \mathbb{P}^2 pode ser identificado com \mathbb{P}^9 :

$$\mathfrak{C}_3 = \{F(X, Y, Z) = aX^3 + bY^3 + \dots + mXYZ =\} \cong \mathbb{P}^9$$

Quando impomos que uma cúbica passe num certo ponto P , somos conduzidos a uma equação linear homogénea nos coeficientes de F . Portanto, o conjunto das cúbicas que passam em P , é um hiperplano $\mathcal{H}(P)$ de \mathbb{P}^9 .

Analogamente, se fixamos dois pontos distintos P e Q , as cúbicas que passam por eles formam um conjunto definido por duas equações lineares homogéneas independentes, nos coeficientes de F , e portanto definem uma variedade linear de \mathbb{P}^9 de codimensão 2.

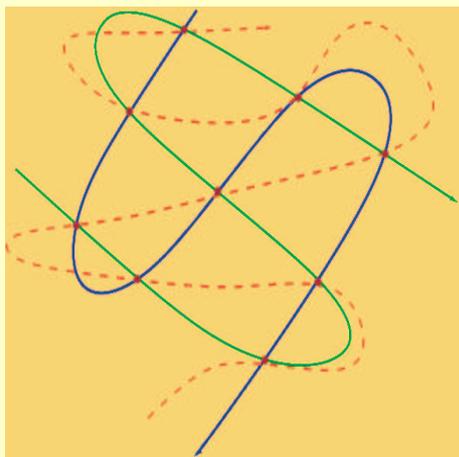
Continuando desta forma vemos que, para uma colecção de 9 pontos dados $P_1, P_2, \dots, P_9 \in \mathbb{P}^2$, distintos, as cónicas que por eles passam são determinadas como soluções de um conjunto de 9 equações lineares homogéneas nos 10 coeficientes de F . Em geral, o conjunto das soluções é dado pelos múltiplos de uma solução dada e, portanto, uma cúbica ficará univocamente determinada por 9 pontos, desde que as equações lineares a que eles conduzem sejam independentes.

Em geral, uma curva de grau n ficará determinada por:

$$\frac{1}{2}(n+1)(n+2) - 1 = \frac{1}{2}(n(n+3))$$

pontos "independentes" no sentido acima referido.

► **18.2 Teorema dos nove pontos ...** Apesar de, em geral, uma cúbica ficar univocamente determinada por 9 pontos, poderá haver configurações especiais dos tais 9 pontos, para as quais haja uma família a um parâmetro de cúbicas que por eles passam. Esta é a situação descrita no teorema seguinte:



Teorema dos nove pontos ... *Suponhamos que \mathcal{C}_1 e \mathcal{C}_2 são duas cúbicas que se intersectam em 9 pontos distintos P_1, P_2, \dots, P_9 .*

Se \mathcal{C} é uma outra cúbica que passa nos oito primeiros P_1, \dots, P_8 , então, \mathcal{C} passa necessariamente pelo nono ponto P_9 .

Dem.: Suponhamos que $\mathcal{C}_1 : F_1(X, Y, Z) = 0$ e $\mathcal{C}_2 : F_2(X, Y, Z) = 0$ são duas cúbicas em \mathbb{P}^2 , que se intersectam nos 9 pontos distintos dados P_1, P_2, \dots, P_9 . Então, em geral, $F_1 = \lambda F_2$ e $\mathcal{C}_1 = \mathcal{C}_2$, isto é, em geral existe uma única cúbica que passa em 9 pontos distintos dados. Mas a situação descrita no teorema é diferente.

De facto, consideremos o conjunto de todas as cúbicas que passam nos primeiros 8 pontos P_1, \dots, P_8 . Este conjunto corresponde às soluções de um sistema de 8 equações lineares homogêneas nas 10 variáveis que representam os coeficientes de F . O conjunto das soluções deste sistema consiste de todas as combinações lineares de 2 soluções linearmente independentes. Mas como as duas cúbicas dadas passam pelos 8 pontos P_1, \dots, P_8 , os coeficientes dos polinómios correspondentes F_1 e F_2 dão-nos duas soluções linearmente independentes (isto porque os 8 pontos são distintos). Portanto \mathcal{C} será dada por:

$$F(X, Y, Z) = \lambda_1 F_1(X, Y, Z) + \lambda_2 F_2(X, Y, Z) = 0$$

para algumas constantes λ_1, λ_2 . Mas o nono ponto P_9 está em \mathcal{C}_1 e \mathcal{C}_2 , isto é, $F_1(P_9) = F_2(P_9) = 0$, e daí que $F(P_9)$ também, como se pretendia.

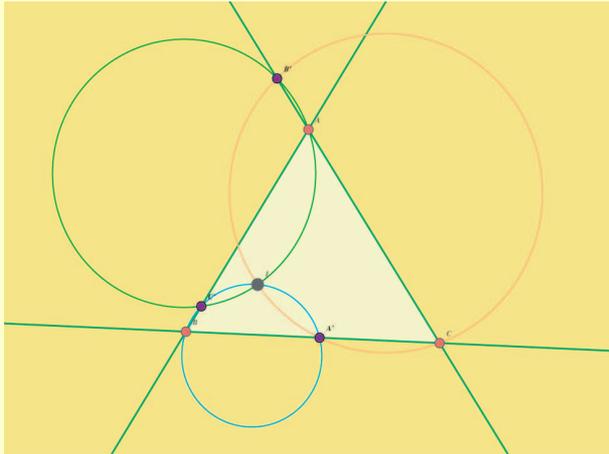
Mais geralmente, tem-se que:

► **18.3 Teorema de Cayley ...** *Sejam \mathcal{C}_1 e \mathcal{C}_2 duas curvas em \mathbb{P}^2 , de graus d_1 e d_2 , respectivamente, sem componente comum, e suponhamos que \mathcal{C}_1 e \mathcal{C}_2 se intersectam em $d_1 \cdot d_2$ pontos. Seja \mathcal{C} uma curva em \mathbb{P}^2 de grau $d_1 + d_2 - 3$. Então, se \mathcal{C} passa por todos excepto um dos pontos de $\mathcal{C}_1 \cap \mathcal{C}_2$, \mathcal{C} deve passar pelo ponto restante.*

Não é necessário que as curvas dadas se interesectem em pontos distintos. Por exemplo, se $P \in \mathcal{C}_1 \cap \mathcal{C}_2$ é um ponto duplo (multiplicidade 2), digamos porque \mathcal{C}_1 e \mathcal{C}_2 têm uma tangente comum em P , temos apenas que exigir que \mathcal{C} tenha a mesma tangente em P .

Vejamos agora algumas aplicações:

► **18.4 Teorema do pivot ...** *Seja ABC um triângulo e A', B', C' pontos nas rectas que contêm respectivamente os lados BC, CA e AB . Então os círculos $BC'A', CA'B'$ e $AB'C'$ intersectam-se num mesmo ponto G .*



Dem.: As cónicas:

$$\mathcal{C}_1 = \text{recta } BC \cup \text{círculo } AB'C'$$

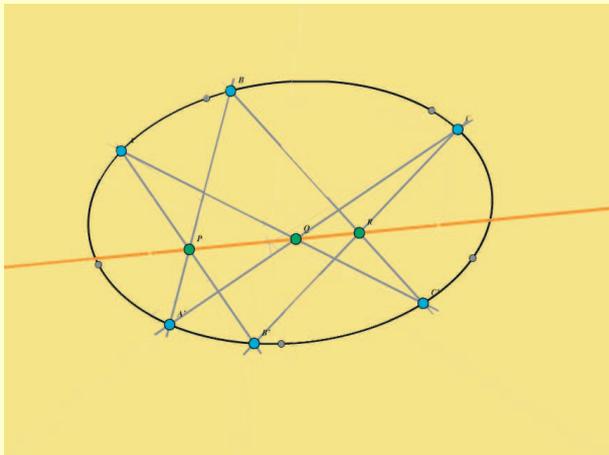
$$\mathcal{C}_2 = \text{recta } CA \cup \text{círculo } BC'A'$$

passam pelos seis pontos A, B, C, A', B', C' , pelos pontos circulares I, J e ainda pelo ponto G ; ao todo nove pontos. A cónica:

$$\mathcal{C} = \text{recta } AB \cup \text{círculo } CA'B'$$

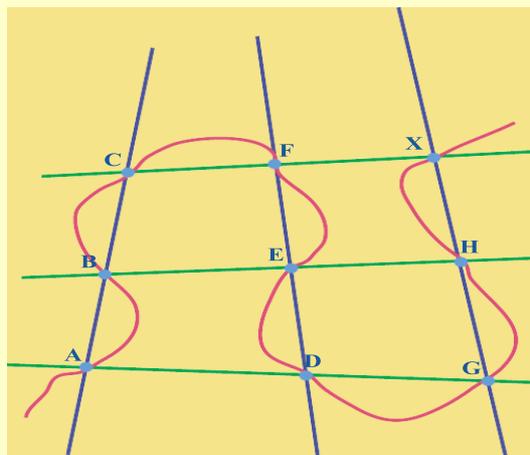
passa pelos oito primeiros, logo passa também em G .

► **18.5 Teorema de Pascal** ...*Sejam A, B, C, A', B', C' seis pontos numa cónica. Então as intersecções $BC' \cap B'C, CA' \cap C'A$ e $AB' \cap A'B$ são colineares.*



Dem.: De facto, as rectas $B'C, C'A, A'B$ formam conjuntamente uma cúbica. O mesmo acontece com as rectas BC', CA', AB' e ainda com a cónica dada conjuntamente com a recta DE . Estas três cúbicas passam todas pelos 8 pontos $A, B, C, A', B', C', D, E$ e portanto também passam pelo nono ponto comum.

► **18.6 Exemplo** ... Considere as rectas AB, DE, GH da figura seguinte:



Estas rectas constituem uma cúbica. O mesmo acontece com as rectas AD, BE e CF . Estas duas cúbicas passam pelos 8 pontos A, B, C, D, E, F, G, H . Portanto qualquer cúbica que passe por estes 8 pontos tem que passar pelo nono ponto $X = CF \cap HG$.

► **18.7** Se na configuração descrita no número anterior, fizermos $B \rightarrow A$, ao longo da curva desenhada, a recta AC converge para a tangente a essa curva em A . Analogamente, se fizermos $E \rightarrow D$, sempre ao longo da curva desenhada, a recta DE converge para a tangente a essa curva em D . Mas então $H \rightarrow G$ e, portanto, se uma recta intersecta uma cúbica nos pontos A, D, G , as tangentes nesses pontos intersectam a cúbica novamente em pontos colineares.

► **18.8** Se B e E são inflexões, e se ambos $A, C \rightarrow B$, e $D, F \rightarrow E$, então $X, G \rightarrow H$. Portanto, a recta que une duas inflexões numa cúbica, passa através de uma terceira inflexão.

Tópico 19

Pontos racionais em cúbicas. Estrutura de grupo numa cúbica

► **19.1 Cúbicas racionais** ... Consideremos uma cúbica afim \mathcal{C} da forma:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + ly + m = 0 \quad (19.1)$$

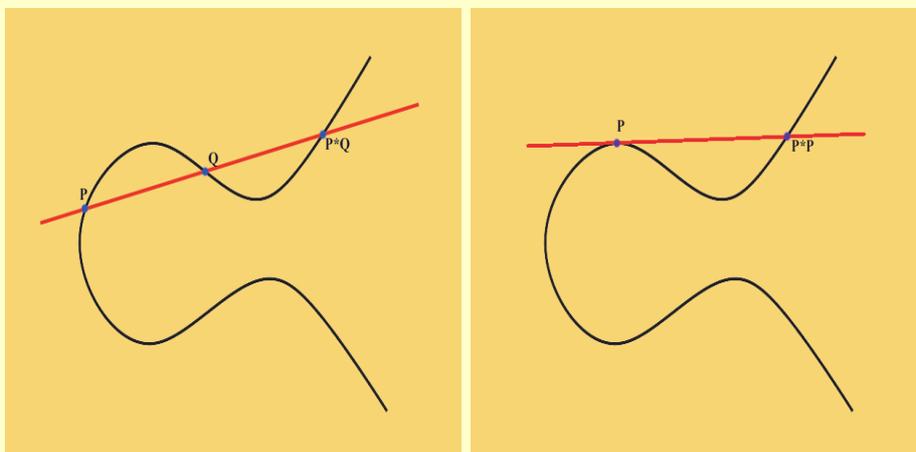
\mathcal{C} diz-se **racional** se todos os coeficientes $a, b, c, \dots \in \mathbb{Q}$.

O problema de encontrar os pontos racionais de \mathcal{C} não pode, em geral, ser resolvido pelo método que usamos para determinar os pontos racionais das cónicas, uma vez que uma recta intersecta uma cúbica em 3 pontos (eventualmente, complexos, no infinito e não necessariamente distintos).

Mas existe um outro processo geométrico que pode ser usado. *Se a cúbica tem dois pontos racionais tem, em geral, um terceiro.* Para o encontrar considera-se a recta que une os dois pontos racionais. Esta recta é pois racional, e intersecta \mathcal{C} num outro ponto. Quando se calcula as intersecções de uma recta com uma cúbica sômos conduzidos a uma equação cúbica com coeficientes racionais. Se duas das raízes são racionais a terceira também o será. Obtemos assim uma espécie de lei de composição em \mathcal{C} :

$$(P, Q) \mapsto P * Q = \mathcal{C} \cap (PQ)$$

Se $P = Q$, a recta PQ será a tangente a \mathcal{C} em P .



Portanto, começando com alguns pontos racionais obtemos em geral outros desenhando rectas e calculando intersecções.

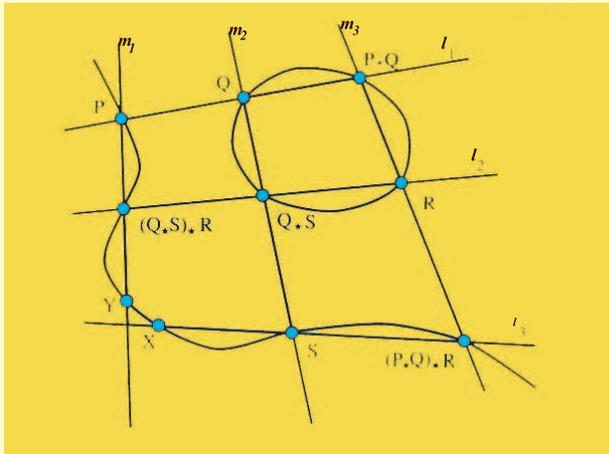
Um dos teoremas mais importantes, conjecturado por Poincaré e demonstrado por Mordell, em 1921, diz-se que:

“se \mathcal{C} é uma cúbica racional não singular, existe um número finito de pontos racionais tais que todo o outro ponto racional pode ser encontrado pelo processo acima descrito”.

Não existe porém qualquer método conhecido para determinar, num número finito de etapas, se uma dada cúbica tem ou não qualquer ponto racional! Este é um problema em aberto.

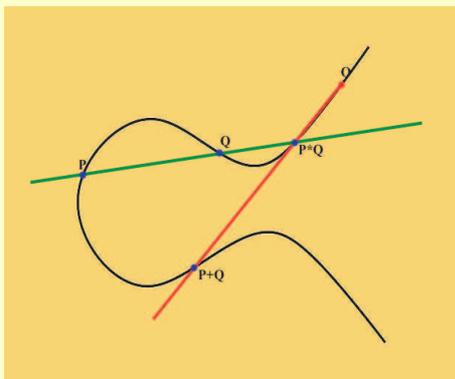
► **19.2 Lema** ... A operação binária $(P, Q) \mapsto P * Q = \mathcal{C} \cap (PQ)$ satisfaz as propriedades seguintes:

- (i). $P * Q = Q * P$
- (ii). $(P * Q) * P = Q$
- (iii). $((P * Q) * R) * S = P * ((Q * S) * R)$



Dem.: As duas primeiras propriedades são imediatas. Quanto à terceira, designemos por $X = ((P * Q) * R) * S$ e $Y = P * ((Q * S) * R)$. Com as notações da figura, vemos que as cúbicas $l_1 \cup l_2 \cup l_3$ e $m_1 \cup m_2 \cup m_3$ intersectam-se em nove pontos e que a cúbica dada \mathcal{C} passa por oito deles. Pelo teorema dos nove pontos, \mathcal{C} passa pelo nono e portanto $X = Y$.

► **19.3 Estrutura de grupo numa cúbica** ...



Fixemos um ponto $O \in \mathcal{C}$, e definamos uma operação binária em \mathcal{C} :

$$(P, Q) \rightarrow P + Q$$

da seguinte forma:

$$\begin{aligned} P + Q &= \text{intersecção com } \mathcal{C} \text{ da recta} \\ &\quad \text{que une } O \text{ com } P * Q \\ &= (P * Q) * O \end{aligned} \tag{19.2}$$

► **19.4 Teorema** ... A cúbica \mathcal{C} munida da operação binária $(P, Q) \rightarrow P + Q$, definida anteriormente, tem estrutura de grupo comutativo cujo elemento neutro é O .

Dem.:

- A comutatividade é imediata.

- Associatividade:

$$\begin{aligned}(P + Q) + R &= ((P + Q) * R) * O = (((P * Q) * O) * R) * O \\ P + (Q + R) &= (P * (Q + R)) * O = (P * ((Q * R) * O)) * O\end{aligned}\quad (19.3)$$

e os membros direitos são iguais pela terceira propriedade do Lema anterior.

- O é o elemento neutro. De facto, para todo o ponto simples $P \in \mathcal{C}$:

$$P + O = (P * O) * O = (O * P) * O = P$$

- O simétrico de um ponto P é $-P = P * (O * O)$. De facto, usando as duas primeiras propriedades do Lema anterior, tem-se:

$$\begin{aligned}P + (-P) &= P + (P * (O * O)) \\ &= (P * (P * (O * O))) * O \\ &= ((P * (O * O)) * P) * O \\ &= (O * O) * O = O + O = O\end{aligned}\quad (19.4)$$

► **19.5** Em termos da lei de grupo que acabamos de definir, o teorema de Mordell pode ser enunciado na seguinte forma:

“se uma cúbica não singular tem um ponto racional então o grupo dos seus pontos racionais é finitamente gerado”.

De aqui em diante escolhemos O como uma inflexão da cúbica \mathcal{C} (que tem sempre pelo menos uma). Quando O é uma inflexão tem-se que:

$$O * O = O, \quad \text{e} \quad -P = P * O$$

► **19.6 Lema ...** *Sejam P, Q, R pontos arbitrários numa cúbica não singular \mathcal{C} . Suponhamos ainda que O é uma inflexão de \mathcal{C} . Então:*

- (i). $P + Q + R = O$ se e só se P, Q e R são colineares.
- (ii). $P \neq O$ tem ordem 2, i.e., $2P = 0$ se e só se a tangente $T_P\mathcal{C}$ passa por O .
- (iii). $P \neq O$ tem ordem 3, i.e., $3P = 0$ se e só se P é uma inflexão de \mathcal{C} .

Dem.: [(i).] **Suponhamos que P, Q e R são pontos distintos colineares de \mathcal{C} . Então $P * Q = R$ e:**

$$\begin{aligned}(P + Q) + R &= ((P + Q) * R) * O \\ &= ((P * Q) * O) * R * O \\ &= ((R * O) * R) * O \\ &= O * O = O\end{aligned}\quad (19.5)$$

Reciprocamente, se $P + Q + R = 0$, então:

$$\begin{aligned}P + Q = -R &\Rightarrow (P * Q) * O = R * O \\ &\Rightarrow (P * Q) + O = R + O \\ &\Rightarrow P * Q = R \Rightarrow P, Q \text{ e } R \text{ são colineares}\end{aligned}\quad (19.6)$$

[(ii).] $P \neq O$ em \mathcal{C} tem ordem 2 sse $2P = P + P = O$, sse $(P * P) * O = O$ sse $P * P = O$. Mas este é o ponto onde $T_P\mathcal{C}$ intersecta \mathcal{C} outra vez. Logo $O \in T_P\mathcal{C}$.

[(iii).] Suponhamos que $P \neq O$ é uma inflexão, de tal forma que $P * P = P$. Então:

$$\begin{aligned} P + P &= (P * P) * O \\ &= P * O \neq O \end{aligned} \tag{19.7}$$

e portanto P não pode ter ordem 2. Além disso:

$$\begin{aligned} 3P &= (P + P) + P \\ &= (P * O) + P \\ &= ((P * O) * P) * O \\ &= O * O = O \end{aligned} \tag{19.8}$$

o que significa que P tem ordem 3.

Reciprocamente, se $P \neq O$ e $3P = 0$, isto é $P + P \neq 0$ e $(P + P) + P = 0$, então:

$$\begin{aligned} P + P = -P &\Rightarrow (P * P) * O = P * O \\ &\Rightarrow P * P = P \end{aligned} \tag{19.9}$$

o que significa que P é uma inflexão.

► **19.7 Inflexões numa cúbica ...** Seja \mathcal{C} uma cúbica não singular e P e Q duas inflexões distintas de \mathcal{C} . Então a recta PQ que os une contém uma terceira inflexão, nomeadamente o ponto $2P + 2Q$. De facto, a recta PQ intersecta \mathcal{C} num terceiro ponto R tal que $P + Q + R = 0$. Dai que $R = -P - Q$. Mas como P e Q são inflexões: $3P = 0 = 3Q$ e, portanto:

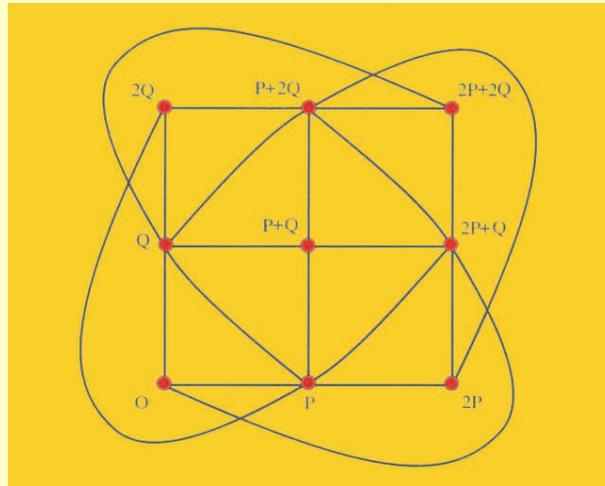
$$-P = 2P, \quad -Q = 2Q \Rightarrow R = 2P + 2Q \Rightarrow 3R = 6P + 6Q = O + O = O$$

isto é, R é uma inflexão.

Dadas três inflexões não colineares O, P e Q , em \mathcal{C} , podemos sempre construir nove inflexões distintas:

$$O, P, 2P, Q, P + Q, 2P + 2Q, 2Q, P + 2Q, 2P + 2Q$$

que formam uma configuração de nove pontos.



► **19.8 Forma normal de Weierstrass** ... Consideremos uma cúbica não singular \mathcal{C} , em $\mathbb{P}^2(\mathbb{C})$, definida por:

$$aX^3 + bY^3 + cZ^3 + eX^2Y + fXY^2 + gX^2Z + hXZ^2 + kY^2Z + lYZ^2 + mXYZ = 0 \quad (19.10)$$

\mathcal{C} tem pelo menos uma inflexão (porquê?), que podemos supôr ser o ponto $A = [0, 1, 0]$. Como $A \in \mathcal{C}$ vem que $b = 0$. Podemos também supôr que a tangente inflexional é a recta $T_A\mathcal{C} : Z = 0$. Esta recta pode ser parametrizada por:

$$t \mapsto [0, 1, 0] + t[1, 0, 0] = [t, 1, 0]$$

e o polinómio de intersecção de $T_A\mathcal{C}$ com \mathcal{C} é pois:

$$\varphi(t) = at^3X^3 + b + et^2X^2 + ftX$$

Como $I_A(\mathcal{C} \cap T_A\mathcal{C}) = 3$, devemos ter $e = f = 0$, mas $a \neq 0$, caso contrário a recta $Z = 0$ seria uma componente de \mathcal{C} .

Portanto, para já:

$$b = e = f = 0, \quad a \neq 0$$

A tangente $T_A\mathcal{C}$ tem por equação:

$$XF_X(0, 1, 0) + YF_Y(0, 1, 0) + ZF_Z(0, 1, 0) = 0$$

e como estamos a supôr que esta recta é $Z = 0$, vem que $F_X(0, 1, 0) = 0 = F_Y(0, 1, 0)$, mas $F_Z(0, 1, 0) = k \neq 0$, caso contrário $A = [0, 1, 0]$ seria ponto singular de \mathcal{C} . Podemos pois supôr que $k = 1$. Passando a coordenadas afins x, y , na carta afim $Z = 1$, vem então que a equação da cúbica é:

$$y^2 + ax^3 + c + gx^2 + hx + ly + mxy = 0$$

ou ainda:

$$y^2 + (mx + l)y + P(x) = 0$$

onde $P(x)$ é um polinómio do terceiro grau em x .

A substituição $y \rightarrow y - \frac{1}{2}(mx + l)$ transforma a curva na forma:

$$y^2 + \frac{1}{4}(mx + l)^2 + P(x) = 0$$

ou finalmente na forma canónica de Weierstrass:

$$y^2 = p(x) \quad (19.11)$$

onde $p(x)$ é um polinómio do terceiro grau em x .

► **19.9 Curva elípticas** ... Uma cúbica afim não singular pode ser posta na forma canónica:

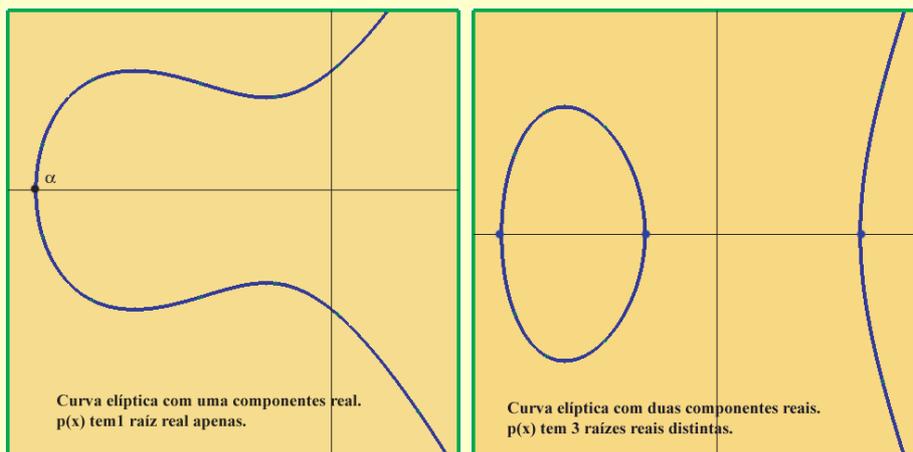
$$y^2 = p(x) = x^3 + ax^2 + bx + c \quad (19.12)$$

Quando as raízes de $p(x)$ são distintas a cúbica diz-se uma **curva elíptica**. Mais geralmente qualquer curva birracionalmente equivalente à curva (19.12) diz-se uma curva elíptica. Estas curvas surgem no problema do cálculo do comprimento de arco de uma elipse. Daí o nome de curva elíptica!

Suponhamos agora que a curva (19.12) é racional, isto é, que os coeficientes $a, b, c \in \mathbb{Q}$. Em particular, o polinómio $p(x) = x^3 + ax^2 + bx + c$ terá pelo menos uma raíz real α e podemos pôr:

$$p(x) = (x - \alpha)(x^2 + \beta x + \gamma), \quad \alpha, \beta, \gamma \in \mathbb{R}$$

É claro que poderá ter 3 raízes reais. Quando $p(x)$ tem apenas uma raíz real, e quando tem 3 raízes reais distintas, as curvas $y^2 = p(x)$ correspondentes têm o aspecto das figuras seguintes.



► **19.10 Fórmulas explícitas para a operação + no grupo ...** Consideremos uma cúbica afim \mathcal{C} não singular na forma canónica (de Weierstrass):

$$y^2 = p(x) = x^3 + ax^2 + bx + c \tag{19.13}$$

com as raízes de $p(x)$ distintas, i.e., a cúbica \mathcal{C} é uma **curva elíptica**.

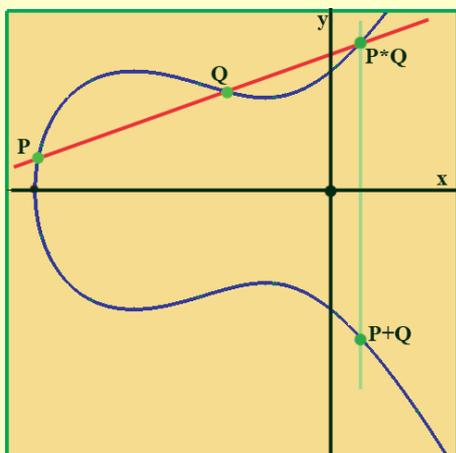
O fecho projectivo de (19.13) é a curva $\widehat{\mathcal{C}}$ definida por:

$$F(X, Y, Z) = Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3 \tag{19.14}$$

Esta curva intersecta a recta do infinito $Z = 0$ no ponto $O = [0, 1, 0]$. Este ponto é não singular e é uma inflexão de $\widehat{\mathcal{C}}$ com tangente inflexional $Z = 0$ (verifique estes factos, como exercício).

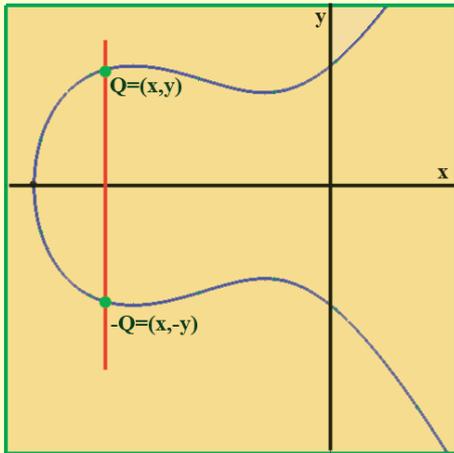
O ponto O é racional e será tomado como o elemento neutro do grupo.

► **19.11 Como somamos dois pontos P e Q de \mathcal{C} ? ...**



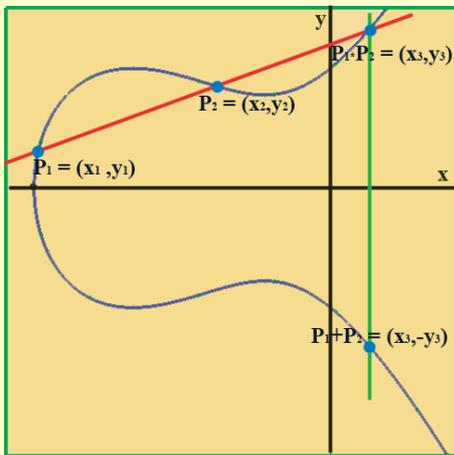
Primeiro traçamos a recta PQ e determinamos a terceira intersecção $P*Q$ dessa recta com \mathcal{C} . De seguida unimos este ponto com O , o que não é mais do que traçar a recta vertical que passa em $P*Q$ (porquê?). A cúbica \mathcal{C} definida por (19.13) é simétrica relativamente ao eixo dos x 's. Portanto para determinar $P+Q$, basta tomar o simétrico de $P*Q$ relativamente ao eixo dos x 's.

► **19.12 Qual o simétrico $-Q$ de um ponto Q de \mathcal{C} ? ...**



O negativo de um ponto $Q = (x, y)$ é o refletido relativamente ao eixo dos x 's, isto é, $-Q = (x, -y)$. De facto unindo Q com $-Q$ obtemos uma recta vertical e portanto o terceiro ponto de intersecção $Q * (-Q)$ é exactamente o ponto O . Agora unindo O com O obtemos a recta $Z = 0$ e tomando a terceira intersecção com $\widehat{\mathcal{C}}$ dá novamente O , uma vez que $I_O(\widehat{\mathcal{C}} \cap T_O \widehat{\mathcal{C}}) = 3$, uma vez que O é uma inflexão. Portanto $Q + (-Q) = 0$.

► 19.13 Uma fórmula explícita para $P_1 + P_2$...



Pondo:

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad P_1 * P_2 = (x_3, y_3)$$

de tal forma que:

$$P_1 + P_2 = (x_3, -y_3)$$

obtemos por cálculo as fórmulas seguintes:

$$\begin{cases} x_3 = \lambda^2 - a - x_1 - x_2 \\ y_3 = \lambda x_3 + \vartheta \end{cases} \quad (19.15)$$

onde

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \text{e} \quad \vartheta = y_1 - \lambda x_1 = y_2 - \lambda x_2 \quad (19.16)$$

De facto, a recta que une $P_1 = (x_1, y_1)$ com $P_2 = (x_2, y_2)$, tem por equação:

$$y = \lambda x + \vartheta, \quad \text{onde} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \text{e} \quad \vartheta = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

Por construção, esta recta intersecta a cúbica nos pontos P_1 e P_2 . Para determinar o terceiro ponto substituímos em (19.13):

$$y^2 = (\lambda x + \vartheta)^2 = x^3 + ax^2 + bx + c$$

ou ainda:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\vartheta)x + (c - \vartheta^2) = 0 = (x - x_1)(x - x_2)(x - x_3)$$

Igualando os coeficientes em x^2 de ambos os membros, obtemos as fórmulas (19.15) e (19.16).

► 19.14 Exemplo ... Consideremos a curva:

$$y^2 = x^3 + 17$$

Se $P_1 = (-1, 4)$ e $P_2 = (2, 5)$, para calcular $P_1 + P_2$, obtemos primeiro que:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1}{3}, \quad \text{e} \quad \vartheta = y_1 - \lambda x_1 = y_2 - \lambda x_2 = \frac{13}{5}$$

Portanto:

$$x_3 = \lambda^2 - x_2 - x_1 = -\frac{8}{9}, \quad y_3 = \lambda x_3 + \vartheta = \frac{109}{27}$$

e finalmente:

$$P_1 + P_2 = (-1, 4) + (2, 5) = (x_3, -y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right)$$

► **19.15 Problema ...** Representar o produto de dois inteiros consecutivos $y(y + 1)$ na forma de produto de três inteiros consecutivos $(x - 1)x(x + 1) = x^3 - x$.

Este problema conduz à curva \mathcal{C} dada por:

$$y^2 + y = x^3 - x$$

Fazendo a mudança de variável:

$$y \rightarrow \tilde{y} = y + \frac{1}{2}$$

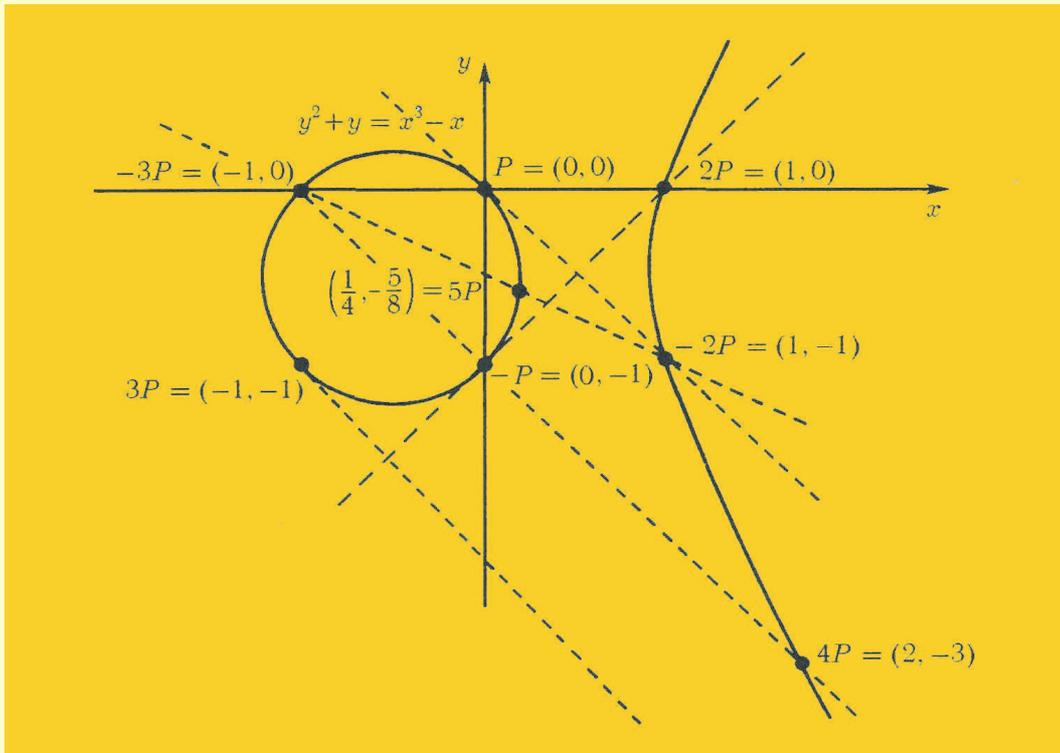
obtemos a curva:

$$\tilde{y}^2 = x^3 - x + \frac{1}{4}$$

Como $\tilde{y} = 0 \Leftrightarrow y = -\frac{1}{2}$, o processo geométrico de obter a soma de dois pontos é análogo ao descrito anteriormente substituindo o eixo dos x 's, i.e., a recta $y = 0$, pela recta $y = -1/2$.

A curva \mathcal{C} tem seis pontos óbvios com coordenadas inteiras:

$$(0, 0), (1, 0), (-1, 0), (0, -1), (1, -1), (-1, -1)$$



Se $P = (0, 0)$ todos os pontos indicados são gerados por P :

$$(1, 0) = 2P, \quad (-1, 0) = -3P, \quad (0, -1) = -P, \quad (1, -1) = -2P, \quad (-1, -1) = 3P$$

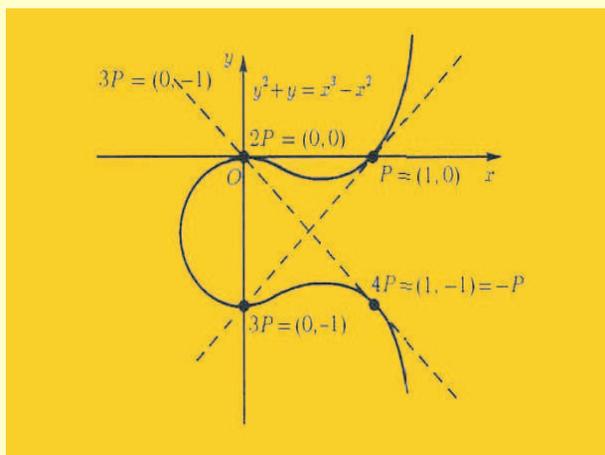
O ponto P gera um grupo cíclico infinito. Todos os pontos da forma $(2k + 1)P$ pertencem à componente conexa compacta da curva, que contém P , enquanto que os pontos da forma $2kP$ pertencem à componente ilimitada.

► **19.16 Exemplo** ... A curva \mathcal{C} dada por:

$$y^2 + y = x^3 - x^2$$

tem quatro pontos óbvios com coordenadas inteiras:

$$(1, 0), (0, 0), (0, -1) = -(0, 0), (1, -1) = -(1, 0)$$



A tangente a \mathcal{C} em $(1, 0)$ intersecta novamente \mathcal{C} no ponto $(0, -1)$, o que significa que $2(1, 0) = (0, 0)$. Portanto, $2(1, -1) = (0, -1)$.

A tangente a \mathcal{C} em $(0, 0)$ intersecta novamente \mathcal{C} no ponto $(1, 0)$, o que significa que $2(0, 0) = (1, -1)$. As equações $2(1, 0) = (0, 0)$, $2(0, 0) = (1, -1) = -(1, 0)$, implicam que $4(1, 0) = (1, -1) = -(1, 0)$, i.e., $5(1, 0) = (0, 0)$. Portanto, o subconjunto:

$$\{O, (1, 0), (0, 0), (0, -1), (1, -1)\}$$

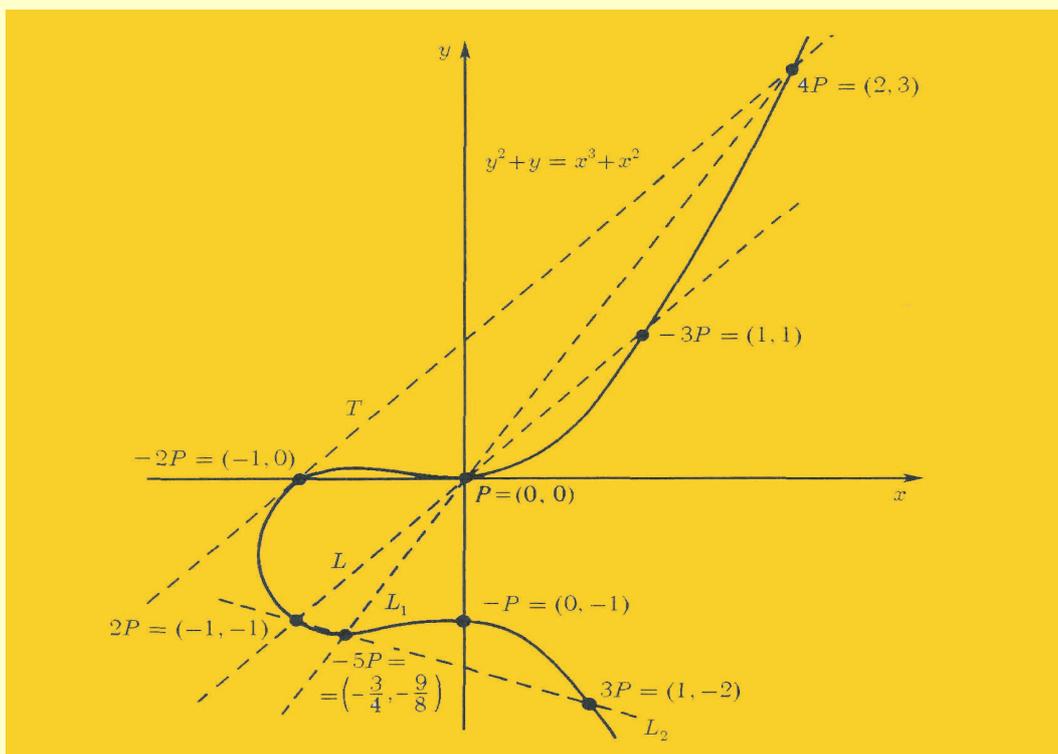
é um subgrupo cíclico de ordem 5 em $\mathcal{C}(\mathbb{Q})$.

► **19.17 Exemplo** ... A curva

$$y^2 + y = x^3 + x^2$$

tem quatro pontos óbvios com coordenadas inteiras:

$$(0, 0), (-1, 0), (0, -1) = -(0, 0), (-1, -1) = -(-1, 0)$$



O ponto $P = (0, 0)$ gera um grupo cíclico infinito. Por exemplo:

$$2P = (-1, -1), \quad -3P = (1, 1), \quad 3P = (1, -2), \quad 4P = (2, 3), \quad 5P = (-3/4, -9/8)$$

A tangente a \mathcal{C} em $-2P$ intersecta novamente \mathcal{C} no ponto $4P$, e a recta que une $2P$ com P , intersecta novamente \mathcal{C} no ponto $-3P$. O ponto $-5P$ constrói-se usando a recta que une P com $4P$, ou usando a recta que une $2P$ com $3P$.

FIM