

Pontos de Galois Sobre Curvas Quárticas Projetivas Não Singulares

Pedro Matos da Silva

Dissertação de Mestrado em Matemática

Mestrado em Matemática

Universidade Federal do Espírito Santo

Vitória, Maio de 2009

Livros Grátis

<http://www.livrosgratis.com.br>

Milhares de livros grátis para download.

Pontos de Galois Sobre Curvas Quárticas Projetivas Não Singulares

Pedro Matos da Silva

Dissertação submetida ao Programa de Pós-Graduação em Matemática da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do grau de Mestre em Matemática.

Aprovada em 22/05/2009 por:

Prof. Dr. Valmecir Antônio dos Santos Bayer - Orientador, UFES

Prof. Dr. Marcelo Escudeiro Hernandes, UEM

Prof. Dr. José Gilvan de Oliveira, UFES

Universidade Federal do Espírito Santo
Vitória, Maio de 2009

Sumário

0.1	Introdução	1
1	Preliminares	4
1.1	Espaços Projetivos	4
1.2	Curvas afins e curvas projetivas	6
1.3	Conjuntos algébricos	10
1.4	Aplicações regulares e racionais	11
1.5	O gênero de um curva	13
1.6	Multiplicidade de intersecção	14
2	Pontos de Galois	18
2.1	Contextualização	18
2.2	Projeção de uma quártica	21
2.3	O caso de uma cúbica plana não singular	33
2.4	Exemplos com $P \in C$	36

Resumo

Seja k um corpo algebricamente fechado de característica zero e seja C uma curva quártica projetiva não singular definida sobre k com corpo de funções racionais $k(C)$. Considere uma projeção de C , com um centro de projeção em C , sobre uma reta l . Esta projeção determina uma extensão de corpos $k(C) | k(l)$. Nesta dissertação estudamos as seguintes questões: Quando a extensão $k(C) | k(l)$ é galoisiana? Qual é o gênero do modelo não singular do fecho galoisiano desta extensão?

Abstract

Let k be an algebraically closed field of characteristic zero. Let C be a smooth plane projective quartic curve over k with rational function field of $k(C)$. We consider a projection from C to a line l with center at a point of C . This projection determines a field extension $k(C) | k(l)$. In this dissertation we study the following two questions: Under what conditions is the extension $k(C) | k(l)$ a Galois extension? What can be the genus of the nonsingular model of the Galois closure of this extension?

0.1 Introdução

Pontos de Galois associados a uma curva projetiva plana foram introduzidos em 1996 pelo matemático japonês Hisao Yoshihara. Um ponto do plano projetivo é chamado ponto de Galois para uma curva projetiva desse plano se uma projeção da curva, com centro nesse ponto, sobre uma reta induz uma extensão de Galois do corpo de funções da curva sobre o corpo de funções da reta. Muitas questões surgiram a partir desse conceito. Nessa dissertação estamos particularmente interessados no caso em que a curva é uma quártica não singular.

Para tornar os conceitos mais precisos vamos estabelecer as seguintes notações. Vamos supor que k seja um corpo algebricamente fechado de característica zero. Seja K um corpo de funções algébricas em uma variável sobre k . Um subcorpo K' de K (que contém k) é um subcorpo racional maximal de K se todo corpo intermediário entre K' e K , diferente de K' , não é racional. Vamos denotar um subcorpo maximal de K por K_m . Queremos compreender melhor a estrutura da extensão $K | K_m$. Quando esta extensão é galoisiana? Se L é o fecho galoisiano de $K | K_m$, qual é o grupo de Galois da extensão $L | K_m$? Qual é o gênero do corpo de funções L ? Em outras palavras, qual é o gênero do modelo não singular de uma curva plana que tenha L como corpo de funções?

Seja C uma curva projetiva plana não singular de grau d e seja π_P uma projeção de C sobre uma reta l , com centro de projeção num ponto P . Esta projeção induz uma extensão de corpos $k(C) | k(l)$. No caso em que P está sobre a curva temos que o grau de $k(C)$ sobre $k(l)$ é igual a $d - 1$ e se P é um ponto fora da curva então o grau dessa extensão é igual a d .

Nesta dissertação estudaremos os casos em que o grau $[k(C) : k(l)]$ é igual a 3, isto é, o caso em que C é uma quártica e P está em C e o caso em que C é uma cúbica não singular e o ponto P está fora de C . Quando a extensão $k(C) | k(l)$ for galoisiana diremos que P é um ponto de Galois associado a C .

Os resultados que obteremos são os seguintes. No caso em que C é uma quártica projetiva não singular e P é um ponto de C , a extensão $k(C) | k(l)$ é galoisiana se, e somente se, após uma eventual mudança projetiva de coordenadas, a equação afim de C torna-se $f(x, y) = y + g(x, y)$, onde $g(x, y)$ é um polinômio homogêneo de grau quatro sem fatores múltiplos e $g(x, 0) \neq 0$. A extensão $k(C) | k(l)$ é galoisiana se, e somente se, P é um ponto de inflexão cuja reta tangente tem multiplicidade de intersecção 4 com C em P , isto é, P é um ponto de inflexão não ordinário. Além disso, passam por P outras quatro retas tangentes inflexionais (naturalmente em pontos de C diferentes de P). A curva C nesse caso tem poucos pontos de Galois, a saber, a quantidade

de tais pontos é zero, um ou quatro. Para uma quártica genérica, o grupo de Galois de $k(C) | k(l)$ é isomorfo a S_3 , o grupo simétrico de 3 elementos e não há pontos de Galois. Também para uma quártica genérica o fecho galoisiano tem gênero 3. Quando P não é um ponto de Galois então o gênero do modelo não singular assume um dos valores do conjunto $\{6, 7, 8, 9, 10\}$. Exceto para um número finito de pontos de C o gênero do modelo não singular associado ao fecho galosiano de $k(C) | k(l)$ é igual a 10.

Se P não é ponto de Galois de C mas é um ponto de inflexão ordinário, isto é, a multiplicidade de intersecção de C com a reta tangente em P é igual a 3, então o gênero do fecho galoisiano de $k(C) | k(l)$, é igual a 10 menos o número de retas tangentes inflexionais de C distintas de T_P , onde T_P é a reta tangente em P .

Se P não é ponto de Galois de C mas é um ponto de inflexão não ordinário, isto é, a multiplicidade de intersecção de C com a reta tangente em P é igual a 4, então o gênero do fecho galoisiano de $k(C) | k(l)$ é igual a 9 menos o número de retas tangentes inflexionais de C distintas de T_P .

No caso em que C é uma cúbica projetiva plana não singular e P é um ponto de C então $k(C) | k(l)$ é uma extensão de grau dois e, portanto, a extensão é sempre galoisiana. No caso em que P é um ponto fora de C então os resultados que obteremos são os seguintes.

A extensão $k(C) | k(l)$ é galoisiana se, e somente se, P é um ponto comum de três retas tangentes inflexionais de C .

Para uma cúbica genérica temos que o grupo de Galois da extensão $k(C) | k(l)$ é isomorfo a S_3 , o grupo simétrico de 3 letras.

Quanto ao gênero do fecho galoisiano temos:

P é um ponto de Galois de C se, e somente se, $g(P) = 1$. Se P não é ponto de Galois de C então $g(P) \in \{2, 3, 4\}$. Exceto para um número finito de pontos de C temos $g(P) = 4$.

Organizamos o trabalho da seguinte forma:

No capítulo 1 apresentamos alguns conceitos e resultados básicos e gerais necessários para o desenvolvimento da dissertação. O capítulo tem também como objetivo fixar notações, uniformizar a linguagem além de ser uma tentativa de tornar o trabalho autosuficiente.

No capítulo 2 estão os resultados centrais da dissertação. Na seção 2.1 fazemos a apresentação e a contextualização das questões a serem abordadas. Na seção 2.2 enunciamos e provamos o resultado central do trabalho que é a descrição dos pontos de Galois sobre uma quártica projetiva plana não singular. Dedicamos a seção 2.3 ao caso da cúbica não singular com o centro de projeção fora da curva. Este estudo é relativamente mais simples do que

o caso da quártica. Finalmente na seção 2.4 apresentamos alguns exemplos que de uma certa forma complementam os resultados apresentados na seção 2.2.

Capítulo 1

Preliminares

Neste capítulo apresentaremos alguns conceitos e resultados necessários para o desenvolvimento desta dissertação. Admitiremos que o corpo k é algebricamente fechado de característica zero.

1.1 Espaços Projetivos

Sejam k um corpo qualquer, que pensamos como corpo de base (no decorrer do texto vamos fazer restrições ao corpo k), e $n \in \mathbb{N}$. O *espaço afim n -dimensional* é definido como

$$\mathbb{A}^n = \mathbb{A}^n(k) = \{(a_1, \dots, a_n) \mid a_i \in k\}.$$

O espaço projetivo n -dimensional é obtido da forma seguinte.

Defina no espaço afim $(n + 1)$ -dimensional a relação de equivalência \sim : Dados $(a_0, a_1, \dots, a_n), (b_0, b_1, \dots, b_n) \in \mathbb{A}^{n+1} \setminus \{(0, 0, \dots, 0)\}$ dizemos que

$$(a_0, a_1, \dots, a_n) \sim (b_0, b_1, \dots, b_n)$$

se, e somente se, existe $\lambda \in k, \lambda \neq 0$, tal que $b_i = \lambda a_i$ para $0 \leq i \leq n$. A classe de equivalência de (a_0, a_1, \dots, a_n) é representada por

$$(a_0 : a_1 : \dots : a_n).$$

O *espaço projetivo n -dimensional* é o conjunto

$$\mathbb{P}^n = \mathbb{P}^n(k) = \{(a_0 : a_1 : \dots : a_n) \mid a_i \in k, \text{ não todos nulos}\}.$$

Para cada $0 \leq i \leq n$, seja $U_i = \{(a_0 : a_1 : \dots : a_n) \in \mathbb{P}^n \mid a_i = 1\}$. Naturalmente temos que

$$\mathbb{P}^n = \bigcup_{i=0}^n U_i.$$

O conjunto $H_n = \mathbb{P}^n \setminus U_n = \{(a_0 : a_1 : \dots : a_{n-1} : 0) \in \mathbb{P}^n\}$ é chamado de *hiperplano no infinito* e os pontos $P \in H_n$ são os *pontos no infinito* de \mathbb{P}^n . Naturalmente esta escolha de H_n é apenas para uma certa conveniência.

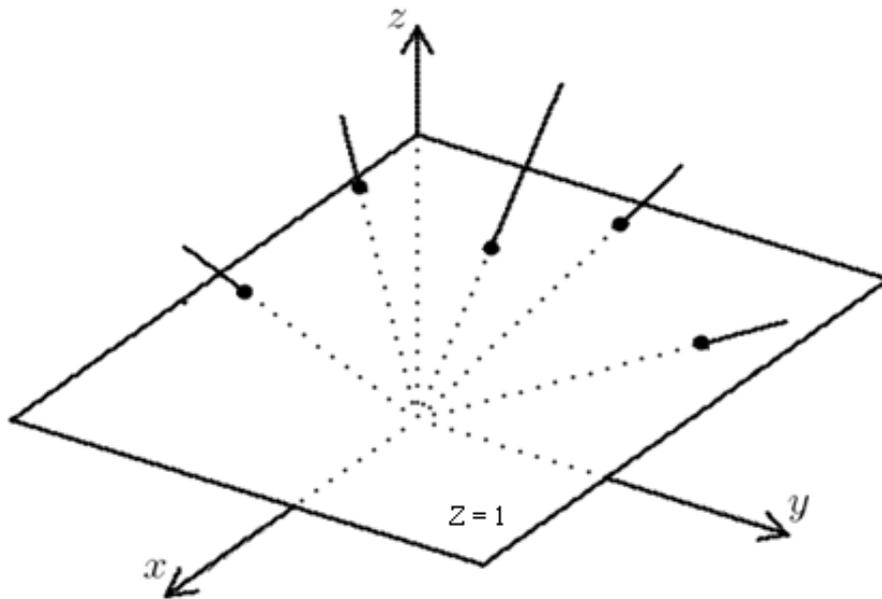
Vemos com facilidade que as aplicações, definidas por,

$$\begin{aligned} \varphi_i : \quad \mathbb{A}^n &\longrightarrow U_i \subset \mathbb{P}^n \\ (a_0, a_1, \dots, a_{n-1}) &\mapsto (a_0 : \dots : a_{i-1} : 1 : a_{i+1} : \dots : a_n) \end{aligned}$$

são bijeções e, portanto, nos fornecem $n + 1$ “cópias” de \mathbb{A}^n em \mathbb{P}^n .

Se $n = 1$, chamaremos o espaço projetivo \mathbb{P}^1 de *reta projetiva*. O espaço projetivo \mathbb{P}^2 , de dimensão 2, é chamado de *plano projetivo* e pode ser identificado com o conjunto das retas do espaço afim tridimensional \mathbb{A}^3 que passam pela origem.

Figura 1.1:



De uma maneira mais geral, podemos definir o *espaço projetivo associado a um espaço vetorial V* de dimensão arbitrária sobre um corpo k como segue.

Definição 1.1. O espaço projetivo $\mathbb{P}(V)$ associado ao espaço vetorial V é o conjunto dos subespaços unidimensionais de V .

1.2 Curvas afins e curvas projetivas

Seja k um corpo algebricamente fechado e sejam $f, g \in k[X, Y]$ polinômios não constantes em duas indeterminadas X e Y sobre k . É fácil mostrar (veja [10], página 9) que $f(X, Y) = 0$ e $g(X, Y) = 0$ têm as mesmas soluções em \mathbb{A}^2 se, e somente se, f e g possuem os mesmos fatores irredutíveis. Assim, dois polinômios, sem fatores irredutíveis múltiplos, definem o mesmo conjunto de zeros em \mathbb{A}^2 se, e somente se, eles diferem por um múltiplo constante não nulo. Isto nos permite fazer a seguinte definição:

Definição 1.2. *Uma curva algébrica plana afim ou, abreviadamente, curva é uma classe de equivalência de polinômios não constantes, que identifica dois polinômios se um deles é múltiplo constante não nulo do outro.*

Dizemos que a equação da curva é qualquer um dos polinômios da classe de equivalência que a define, conforme a definição acima. O grau da curva é o grau de qualquer polinômio que a define. As curvas de grau 1, 2, 3 e 4 são chamadas respectivamente de retas, cônicas, cúbicas e quárticas. Uma curva é irredutível se ela admite uma equação dada por um polinômio irredutível. As componentes irredutíveis de uma curva são as curvas definidas pelos fatores irredutíveis do polinômio que a define.

Seja f uma curva e seja P um ponto de f . Sem perda de generalidade (admitindo mudanças afins de coordenadas conforme definição 1.6 mais adiante) admitiremos $P = (0, 0)$. Podemos escrever

$$f = f_m + f_{m+1} + \cdots + f_d,$$

onde cada um dos f_i é um polinômio homogêneo de grau i para $m \leq i \leq d$, e $f_m \neq 0$. O polinômio f_m pode ser escrito:

$$f_m = (a_1X + b_1Y)^{n_1} \cdots (a_pX + b_pY)^{n_p},$$

onde os fatores $(a_iX + b_iY)$ são distintos. As retas dadas por

$$l_i = (a_iX + b_iY)$$

são as retas tangentes a f em P . O expoente n_i é a multiplicidade da tangente l_i . Vejamos os exemplos a seguir.

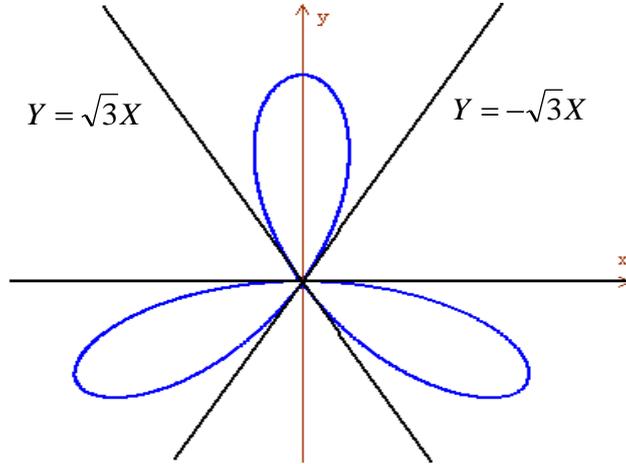
Exemplo 1.3. *A rosácea de três pétalas no plano complexo dada pela equação*

$$X^4 + 2X^2Y^2 + Y^4 - Y(Y - \sqrt{3}X)(Y + \sqrt{3}X) = 0$$

apresenta três tangentes distintas no ponto $(0, 0)$, a saber

$$Y = 0, \quad Y = \sqrt{3}X \quad \text{e} \quad Y = -\sqrt{3}X.$$

Figura 1.2: $C : X^4 + 2X^2Y^2 + Y^4 - Y^3 + 3X^2Y = 0$



Exemplo 1.4. *A cissóide*

$$X^2Y + Y^3 - X^2 = 0$$

tem uma única tangente no ponto $(0,0)$, que é $X = 0$, com multiplicidade 2.

Seja C uma curva definida por um polinômio f , dizemos que um ponto $P = (a, b) \in C$ é um *ponto simples* ou *ponto não singular* ou *ponto regular* de C se

$$\frac{df}{dX}(a, b) \neq 0 \quad \text{ou} \quad \frac{df}{dY}(a, b) \neq 0.$$

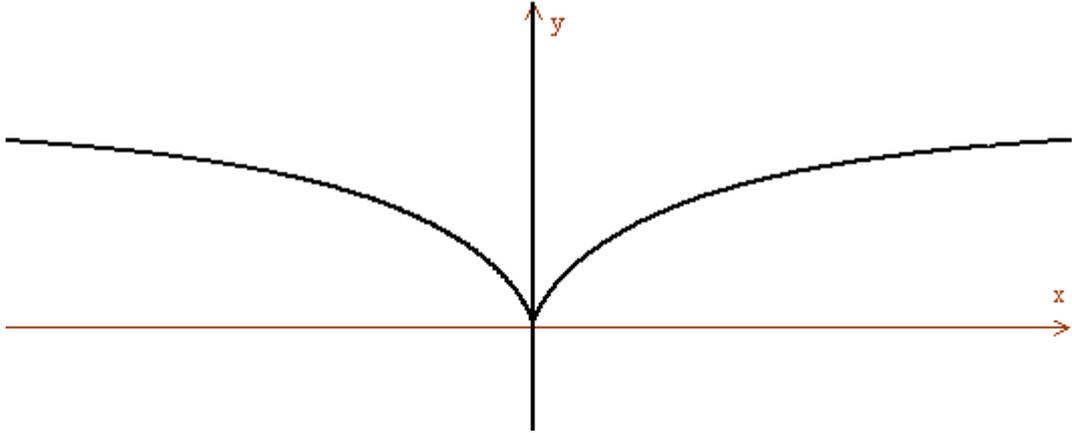
Um ponto de C que não é ponto simples é dito ser um *ponto singular* ou uma *singularidade*. Assim, um ponto $P = (a, b) \in \mathbb{A}^2$ é um ponto singular de C se, e somente se,

$$f(a, b) = \frac{df}{dX}(a, b) = \frac{df}{dY}(a, b) = 0.$$

Se $P = (a, b) \in C$ é um ponto regular, a única *reta tangente* a C em P é a reta dada pela equação:

$$T_P : \frac{df}{dX}(P)(X - a) + \frac{df}{dY}(P)(Y - b) = 0.$$

Seja $f = f_0 + f_1 + \dots + f_d$ um polinômio de grau d nas duas indeterminadas X e Y escrito como soma de componentes homogêneas, isto é, cada f_i é um

Figura 1.3: $C : X^2Y + Y^3 - X^2 = 0$ 

polinômio homogêneo de grau i , com $f_d \neq 0$. Considere a *homogeneização* de f , a saber, o polinômio homogêneo de grau d nas indeterminadas X, Y e Z obtido a partir de f da seguinte forma:

$$f^*(X, Y, Z) = f_0Z^d + f_1(X, Y)Z^{d-1} + \cdots + f_d(X, Y) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

O subconjunto de \mathbb{P}^2 : $\{(x : y : z) \in \mathbb{P}^2 \mid f^*(x, y, z) = 0\}$ claramente contém o conjunto de zeros de f em \mathbb{A}^2 quando olhamos \mathbb{A}^2 contido em \mathbb{P}^2 pela imersão $(x, y) \hookrightarrow (x : y : 1)$. Além disso, os pontos de \mathbb{P}^2 que estão no conjunto de zeros de f^* e que não estão no conjunto de zeros de f são exatamente os pontos infinitos de \mathbb{P}^2 que são zeros de f^* . Isto motiva a definição de curva projetiva da seguinte forma:

Definição 1.5. *Uma **curva plana projetiva** é uma classe de equivalência de polinômios homogêneos não constantes, em três indeterminadas, que identifica dois polinômios quando um é múltiplo constante não nulo do outro.*

Os conceitos introduzidos para curvas afins são estendidos de forma natural para as curvas projetivas.

Valem para polinômios homogêneos as seguintes relações:

1. Seja $F(X, Y, Z)$ um polinômio qualquer. Então F é homogêneo de grau d se, e somente se, $F(tx, ty, tz) = t^d F(x, y, z)$ para todos $x, y, z, t \in k$.

2. (Relação de Eüler) Seja $F(X, Y, Z)$ um polinômio homogêneo de grau d . Então,

$$d \cdot F(X, Y, Z) = X \frac{dF}{dX}(X, Y, Z) + Y \frac{dF}{dY}(X, Y, Z) + Z \frac{dF}{dZ}(X, Y, Z).$$

Seja C uma curva projetiva definida pelo polinômio homogêneo F . Um ponto $P = (a : b : c) \in C$ é um *ponto simples* ou *ponto não singular* ou *ponto regular* de C se vale

$$\frac{dF}{dX}(a, b, c) \neq 0 \quad \text{ou} \quad \frac{dF}{dY}(a, b, c) \neq 0 \quad \text{ou} \quad \frac{dF}{dZ}(a, b, c) \neq 0.$$

Um ponto de C que não é ponto simples é dito ser um *ponto singular* ou uma *singularidade*. Assim, um ponto $P = (a : b : c) \in \mathbb{P}^2$ é um ponto singular de C se, e somente se,

$$F(a, b, c) = \frac{dF}{dX}(a, b, c) = \frac{dF}{dY}(a, b, c) = \frac{dF}{dZ}(a, b, c) = 0.$$

Naturalmente, pela relação de Eüler, temos que $P = (a : b : c) \in \mathbb{P}^2$ é um ponto singular de C se, e somente se,

$$\frac{dF}{dX}(a, b, c) = \frac{dF}{dY}(a, b, c) = \frac{dF}{dZ}(a, b, c) = 0.$$

Se $P = (a : b : c) \in C$ é um ponto regular, a *reta tangente* a C em P é a reta (projetiva) definida pela equação:

$$T_P : X \frac{dF}{dX}(P) + Y \frac{dF}{dY}(P) + Z \frac{dF}{dZ}(P) = 0.$$

Em várias situações nesta dissertação consideramos mudanças de coordenadas.

Definição 1.6. Uma **transformação afim** ou **afinidade** em \mathbb{A}^2 é uma aplicação $T : \mathbb{A}^2 \rightarrow \mathbb{A}^2$ composta de uma translação com um isomorfismo linear.

Toda transformação afim é da forma $T(x_1, x_2) = (y_1, y_2)$, onde

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + a_1 \\ y_2 = a_{21}x_1 + a_{22}x_2 + a_2 \end{cases}$$

com $\det(a_{ij}) \neq 0$.

Definição 1.7. Seja $T : k^3 \rightarrow k^3$ um isomorfismo linear. Visto que uma tal aplicação preserva retas de k^3 passando pela origem, temos definida uma bijeção natural, que ainda designamos por $T : \mathbb{P}^2 \rightarrow \mathbb{P}^2$, chamada uma **projetividade** ou **mudança projetiva de coordenadas** em \mathbb{P}^2 .

1.3 Conjuntos algébricos

Os fatos listados nesta secção podem ser encontrados em [1]. Um ideal $I \subset k[X_1, \dots, X_n]$ define um *conjunto algébrico* em \mathbb{A}^n , a saber,

$$V(I) = \{(a_1, \dots, a_n) \in \mathbb{A}^n \mid q(a_1, \dots, a_n) = 0 \ \forall \ q(X_1, \dots, X_n) \in I\}$$

O Teorema da Base de Hilbert garante que todo ideal de $k[X_1, \dots, X_n]$ é finitamente gerado. Assim, os conjuntos algébricos de \mathbb{A}^n são exatamente o lugar de pontos satisfazendo um número finito de equações polinomiais em n indeterminadas sobre k . Além disso, a aplicação V explicitada acima que associa a cada ideal de $k[X_1, \dots, X_n]$ um subconjunto algébrico de \mathbb{A}^n satisfaz as propriedades seguintes:

1. $V(0) = \mathbb{A}^n$ e $V(k[X_1, \dots, X_n]) = \emptyset$;
2. Se $I \subset J$ então $V(I) \supset V(J)$;
3. $V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$;
4. $V(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} V(I_\lambda)$, onde Λ é uma família arbitrária de índices.

Portanto os subconjuntos algébricos de \mathbb{A}^n formam a coleção de conjuntos fechados de uma topologia em \mathbb{A}^n que é conhecida como *topologia de Zariski*. A topologia de Zariski em \mathbb{A}^n induz uma topologia em qualquer conjunto algébrico $V \subset \mathbb{A}^n$. É claro que os fechados de V são os seus subconjuntos algébricos. Note que a topologia de Zariski é uma topologia muito fraca e bem diferente da topologia usual do \mathbb{R}^n e de \mathbb{C}^n ; por exemplo, os fechados de \mathbb{A}^1 são, além do vazio e o próprio \mathbb{A}^1 , os conjuntos finitos; os fechados de \mathbb{A}^2 são, além do vazio e do próprio \mathbb{A}^2 , os conjuntos finitos e as curvas algébricas afins.

A aplicação V definida acima possui uma espécie de “inversa” que descrevemos a seguir: Um subconjunto $X \subset \mathbb{A}^n$ define um ideal em $k[X_1, \dots, X_n]$:

$$I(X) = \{q(X_1, \dots, X_n) \in k[X_1, \dots, X_n] \mid q(P) = 0 \ \forall \ P \in X\}.$$

Isto é, I leva o subconjunto X no ideal dos polinômios que se anulam em X . É de fácil verificação as propriedades de I listadas a seguir:

1. Se $X \subset Y$ então $I(X) \supset I(Y)$;
2. Para todo $X \subset \mathbb{A}^n$, tem-se que $X \subset V(I(X))$, valendo a igualdade se, e somente se, X é um conjunto algébrico.

3. Se $J \subset k[X_1, \dots, X_n]$ então $J \subset I(V(J))$.

Nem sempre a inclusão no item 3 acima é uma igualdade. Na verdade esta questão está ligada ao *Teorema dos Zeros de Hilbert*, que numa versão simplificada, afirma que se J é um ideal de $k[X_1, \dots, X_n]$ então

$$I(V(J)) = \sqrt{J},$$

onde,

$$\sqrt{J} = \{q \in k[X_1, \dots, X_n] \mid q^n \in J \text{ para algum } n\}.$$

No caso em que J é um ideal primo vale que $\sqrt{J} = J$. Assim, restringindo a correspondência I aos ideais primos tem-se uma inversa para V , que por sua vez, neste caso, deve ser restrita aos conjuntos algébricos irredutíveis que denominamos de variedades algébricas. Observamos ainda que um conjunto algébrico V é irredutível se, e somente se, $I(V)$ é um ideal primo.

1.4 Aplicações regulares e racionais

Seja V uma variedade afim em \mathbb{A}^n e $I(V)$ seu ideal (primo). O anel quociente

$$k[V] = \frac{k[X_1, \dots, X_n]}{I(V)}$$

pode ser visto de maneira natural como um anel de funções com domínio V e contradomínio k . Podemos ver isto da seguinte forma.

Defina uma *função polinomial* em V como sendo uma função $\varphi : V \rightarrow k$ tal que existe um polinômio $G \in k[X_1, \dots, X_n]$ satisfazendo

$$\varphi(P) = G(P) \text{ para todo } P \in V.$$

Assim, se dois polinômios $F, H \in k[X_1, \dots, X_n]$ são tais que $\varphi(P) = G(P)$ e $\varphi(P) = H(P)$ para todo $P \in V$ então $G(P) - H(P) = 0$ para todo $P \in V$ e, portanto $G - H \in I(V)$. Logo, em $k[V]$ temos que, $\overline{F} = \overline{G}$, onde a barra denota a classe de equivalência definida pelo ideal I . Desta forma, o anel das funções polinomiais em V é isomorfo a $k[V]$.

Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ conjuntos algébricos (em ambientes possivelmente distintos). Uma aplicação $\phi : V \rightarrow W$ é *polinomial* se existem m polinômios $G_1, \dots, G_m \in k[X_1, \dots, X_n]$ tais que

$$\phi(P) = (G_1(P), \dots, G_m(P)) \text{ para todo } P \in V.$$

Neste caso dizemos também que ϕ é uma aplicação regular de V em W . Naturalmente uma aplicação regular $\phi : V \rightarrow W$ induz um homomorfismo

de anéis $\phi^* : k[W] \rightarrow k[V]$ definido por $\phi^*(\varphi) = \varphi \circ \phi$. Na verdade, todo k -homomorfismo de k -álgebra $\Psi : k[W] \rightarrow k[V]$ é da forma $\Psi = \phi^*$ para alguma aplicação regular $\phi : V \rightarrow W$. Assim, há uma “equivalência” entre as aplicações regulares de V em W e k -homomorfismos de k -álgebras entre $k[W]$ e $k[V]$.

Seja V uma variedade, então $k[V]$ é um domínio. O *corpo de funções* de V é o corpo de frações do anel $k[V]$, e o denotamos por $k(V)$, isto é:

$$k(V) = \left\{ \frac{g}{h} \mid g, h \in k[V], h \neq 0 \right\}.$$

Observação 1.8. *Se C é uma curva algébrica irredutível, então C é uma variedade algébrica, assim temos bem definido $k(C)$ como o **corpo de funções** de C .*

Se $\varphi = \frac{g}{h} \in k(V)$, em princípio φ não é uma função, no sentido estrito da definição de função, devido aos zeros de h . No entanto φ é bem definida em $P \in V$ sempre que $h(P) \neq 0$. Então φ está definida fora dos zeros de h que é um fechado na topologia de Zariski de V . Logo o “domínio” de φ é um aberto de V . Fixado um ponto $P \in V$, podemos olhar para o conjunto de todas estas “funções” que estão definidas em P . Isto nos leva à definição do *anel local* de V em P , a saber,

$$\vartheta_{V,P} = \{ \varphi \in k(V) \mid \varphi \text{ é regular em } P \}.$$

Naturalmente, temos que $k[V] \subset \vartheta_{V,P} \subset k(V)$ para qualquer $P \in V$. Na verdade, vale:

$$k[V] = \bigcap_{P \in V} \vartheta_{V,P}.$$

Uma aplicação $\phi : V \dashrightarrow \mathbb{A}^n$ é uma *aplicação racional* se existem funções racionais $\varphi_1, \dots, \varphi_n$ tais que

$$\phi(P) = (\varphi_1(P), \dots, \varphi_n(P)) \quad \text{para todo } P \in \bigcap \text{dom}(\varphi_i)$$

Uma *aplicação racional* $\phi : V \dashrightarrow W$ entre duas variedades $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ é uma aplicação racional $\phi : V \dashrightarrow \mathbb{A}^m$ tal que a imagem do domínio de ϕ esteja contida em W . Uma aplicação racional $\phi : V \dashrightarrow W$ é *bi-racional* se existe uma aplicação racional $\psi : W \dashrightarrow V$ tal que $\phi \circ \psi = Id$ e $\psi \circ \phi = Id$ nos devidos domínios de definição.

Como podemos ver na proposição 12 da página 155 de [1], duas curvas são birracionalmente equivalentes se, e somente se, seus corpos de funções são

isomorfos. Na página 179 de [1] encontramos o Teorema 3, que nos mostra que toda curva projetiva C tem um modelo não singular \tilde{C} , isto é:

Se C é uma curva projetiva então existe uma curva projetiva não singular \tilde{C} birracionalmente equivalente a C .

Precisamos tomar um certo cuidado pois mesmo sendo C uma curva plana projetiva o seu modelo não singular \tilde{C} pode não ser uma curva plana projetiva.

1.5 O gênero de um curva

No estudo de variedades algébricas muitos objetos são associados a ela com o objetivo de obter classificações. Na exposição feita acima por exemplo, foram definidos o anel das funções regulares, o corpo de funções, o anel local associado a um ponto. No caso de curvas temos o grau. Alguns objetos são invariantes por determinados tipos de transformações e outros não.

O grau de uma curva algébrica plana afim é invariante por transformações afins de coordenadas, no entanto não é invariante por aplicações bi-rationais, por exemplo, toda cônica é bi-racionalmente equivalente a uma reta, no entanto uma cônica tem grau 2 e uma reta tem grau 1.

Como o matemático norueguês Abel (Niels Henrik Abel (1802-1829)) notou, o número de diferenciais de primeira espécie (também chamadas de 1-formas regulares) linearmente independentes sobre uma curva C é mais importante do que o grau, uma vez que é um invariante bi-racional. Este número é chamado de *gênero* de C e é denotado por $g(C)$. As curvas podem ser classificadas em três classes fundamentais, de acordo com o seu gênero.

1. $g(C) = 0$: curvas racionais.
2. $g(C) = 1$: curvas elípticas.
3. $g(C) \geq 2$: demais curvas.

No estudo de corpos de funções algébricas em uma variável (que são corpos de funções de curvas) temos o teorema fundamental da teoria que é o *Teorema de Riemann-Roch*. Esse teorema permite calcular o gênero de uma curva por um caminho bastante árduo.

Por outro lado, há uma fórmula do gênero dada por um teorema de M. Noether que permite calcular o gênero a partir do grau da curva e de contribuições de suas singularidades. Assim para o cálculo efetivo, precisamos lançar mão de processos locais de dessingularização da curva que normalmente se utiliza explosões do anel local.

Podemos dizer que esses processos são bi-rationais, uma vez que não há mudança no corpo de funções das curvas envolvidas. Por exemplo, é possível mostrar que toda curva algébrica possui um modelo plano (com mesmo corpo de funções) que tem como singularidades, no máximo pontos múltiplos ordinários. A partir daí torna-se mais fácil calcular a contribuição das singularidades (Veja [1]).

A fórmula de M. Noether nos diz que, para uma curva projetiva plana C de grau d , o seu gênero é:

$$g(C) = \frac{(d-1)(d-2)}{2} - \sum_{P \in C} \delta(P)$$

onde $\delta(P) = 0$ se P é um ponto regular da curva. Em particular, para uma curva projetiva plana não singular de grau d o seu gênero é

$$g(C) = \frac{(d-1)(d-2)}{2}$$

Por exemplo, as retas ($d = 1$) e as cônicas irreduzíveis ($d = 2$) têm gênero $g = 0$. As cúbicas não singulares têm gênero $g = 1$. Já as quárticas não singulares têm gênero $g = 3$. Perceba que não existe curva plana projetiva não singular com gênero $g = 2$.

Em [6], página 271, encontramos um importante resultado envolvendo gêneros de curvas que é a fórmula de Riemann-Hurwitz. Enunciaremos da seguinte forma:

Seja $f : C_1 \rightarrow C_2$ uma aplicação regular sobrejetiva entre as curvas suaves C_1 e C_2 . Então

$$2g_{C_1} - 2 = d(2g_{C_2} - 2) + \sum (e_P - 1),$$

onde g_{C_1} é o gênero de C_1 , g_{C_2} é o gênero de C_2 , $d = [k(C_1) : k(C_2)]$ e e_P é o índice de ramificação em $P \in C_1$.

1.6 Multiplicidade de intersecção

Há duas formas clássicas de definir a *multiplicidade* ou *índice de intersecção* de duas curvas projetivas num ponto qualquer do plano projetivo.

Uma primeira definição é via a codimensão do ideal gerado pelas equações das duas curvas no anel de polinômios localizado no ponto em estudo. Essa é a abordagem usada em [1].

A segunda utiliza a resultante dos dois polinômios. Nesta abordagem há um trabalho cuidadoso de escolher bem o sistema de coordenadas para efetuar os cálculos. Este é o caminho tomado em [10].

Estas duas definições naturalmente satisfazem os axiomas que determinam unicamente a multiplicidade de intersecção de curvas planas projetivas, que de fato, fornecem um algoritmo efetivo para a sua determinação. Listamos a seguir estes axiomas.

Dadas duas curvas algébricas planas projetivas em \mathbb{P}^2 , $F = F(X, Y, Z)$ e $G = G(X, Y, Z)$ (aqui estamos identificando a curva com sua equação) e um ponto P em \mathbb{P}^2 , a multiplicidade de intersecção de F com G em P , que denotaremos por $I(F \cdot G, P)$, satisfaz os sete axiomas seguintes. Além disso, esses axiomas determinam $I(F \cdot G, P)$ univocamente.

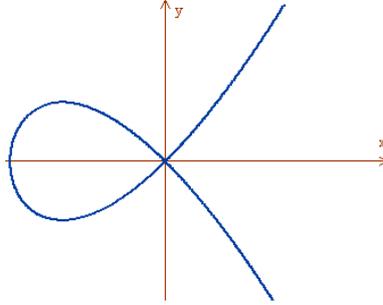
1. $I(F \cdot G, P) = I(G \cdot F, P) \in \mathbb{N} \cup \{\infty\}$.
2. $I(F \cdot G, P) = 0$ se, e somente se, $P \notin F \cap G$.
3. $I(F \cdot G, P) = \infty$ se, e somente se, P está numa componente comum de F e G .
4. Se $T : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ é uma mudança projetiva de coordenadas então $I(F \cdot G, P) = I(F^T \cdot G^T, T(P))$. Aqui F^T e G^T são as respectivas equações das curvas transformadas por T .
5. Se X, Y denotam os eixos coordenados afins $I(X \cdot Y, (0 : 0 : 1)) = 1$.
6. $I(F \cdot (G + AF), P) = I(F \cdot G, P)$ para todo $A \in K[X, Y, Z]$ homogêneo satisfazendo $\text{grau}(A) = \text{grau}(G) - \text{grau}(F)$.
7. $I(F \cdot (G_1 G_2), P) = I(F \cdot G_1, P) + I(F \cdot G_2, P)$.

Um mostra da efetividade do cálculo da multiplicidade de intersecção de duas curvas num ponto utilizando os axiomas acima listados pode ser vista no exemplo seguinte.

Exemplo 1.9. *Considere a curva $C : f(x, y) = x^3 + x^2 - y^2$ no plano complexo $\mathbb{A}^2(\mathbb{C})$ cujo traço real está representado na figura abaixo.*

Vamos calcular a multiplicidade de intersecção de C com a reta $X = 0$ em

Figura 1.4:



$P = (0 : 0 : 1)$:

$$\begin{aligned}
 I(F \cdot X, P) &= I((X^3 + X^2Z - Y^2Z) \cdot X, P) \\
 &= I((-Y^2Z + X(X^2 + XZ)) \cdot X, P) \\
 &= I((Y^2Z) \cdot X, P) = I(Y^2 \cdot X, P) + I(Z \cdot X, P) \\
 &= I(Y \cdot X, P) + I(Y \cdot X, P) + I(Z \cdot X, P) \\
 &= 1 + 1 + 0 = 2
 \end{aligned}$$

Dada uma curva plana projetiva C com equação F e dado um ponto P não singular de C . Neste caso, T_P é a única reta de \mathbb{P}^2 que tem multiplicidade de intersecção maior do que 1 com C em P , isto é, $I(F \cdot T_P, P) \geq 2$.

Se $I(C \cdot T_P, P) \geq 3$, dizemos que P é um *ponto de inflexão* de C e, neste caso, dizemos que T_P é uma *reta tangente inflexional*. No caso em que $I(C \cdot T_P, P) = 3$ dizemos que P é um *ponto de inflexão ordinário*.

Observamos que um ponto de inflexão é um ponto não singular. Naturalmente se $P \in C$ é um ponto singular de C então, para qualquer reta L passando por P , temos que $I(C \cdot L, P) \geq 2$.

Sejam C e D curvas planas projetivas e $P \in C \cap D$. Então

$$I(C \cdot D, P) \geq \text{mult}_P(C) \cdot \text{mult}_P(D).$$

Vale a igualdade acima se, e somente se, as tangentes de C em P forem todas distintas das tangentes de D em P .

Observe que no Cálculo Diferencial e Integral de Newton e Leibnitz os pontos de inflexão de uma curva dada pelo gráfico de uma função são aqueles pontos onde a segunda derivada muda de sinal. Geometricamente isto significa que a concavidade da curva muda. No contexto da geometria algébrica, para curvas dadas por gráficos de funções, os pontos de inflexão são pontos onde a segunda derivada se anula. Por exemplo, $P = (0, 0)$ é um ponto de inflexão de $Y = X^3$ em ambos os contextos, mas é ponto de inflexão de $Y = X^4$ apenas no contexto da geometria algébrica.

Com o conceito de multiplicidade de intersecção podemos enunciar um dos resultados centrais de [10], o Teorema de Bézout.

Teorema 1.10 (Teorema de Bézout). *Sejam F e G duas curvas planas projetivas sem componente em comum. Se o grau de F é d_F e o grau de G é d_G então*

$$d_F \cdot d_G = \sum_{P \in \mathbb{P}^2} I(F \cdot G, P).$$

O teorema de Bézout, em outras palavras, afirma que o número de pontos em comum, contados com as multiplicidades, de duas curvas planas projetivas F e G , sem componente em comum, é igual ao produto dos seus graus.

Capítulo 2

Pontos de Galois

2.1 Contextualização

Um dos principais objetivos desta dissertação é estudar propriedades de uma projeção central de uma curva no plano projetivo $\mathbb{P}^2(\mathbb{C})$ sobre uma reta, cujo centro de projeção é um ponto. Um protótipo desta situação é o exemplo seguinte. Seja C a cúbica não singular definida pela equação

$$F(X, Y, Z) = Y^2Z - X^3 + Z^3.$$

Considere o ponto $P = (0 : 1 : 0)$ e a reta $L : Y = 0$. Observe que $P \in C$. Pensando em $L = \mathbb{P}^1 = \{(a : 0 : c) \mid a, c \in \mathbb{C}, a \neq 0 \text{ ou } c \neq 0\}$, defina a projeção

$$\begin{aligned} \pi : C \setminus \{P\} &\longrightarrow \mathbb{P}^1 \\ (a : b : c) &\longmapsto (a : 0 : c) \end{aligned}$$

Podemos ver π da seguinte forma. Seja $L'_{(a:c)}$ a reta determinada por P e $(a : 0 : c)$, a saber, $L'_{(a:c)} : cX - aZ = 0$. Então $\pi(a : b : c) = L \cap L'_{(a:c)} = (a : 0 : c)$. Em coordenadas afins, π é a projeção vertical de $C_* = \{(a, b) \mid b^2 = a^3 - 1\}$ sobre o eixo x , isto é $\pi(a, b) = a$. Naturalmente, para $(a : c) \in \mathbb{P}^1$ genérico, existem dois pontos $Q, R \in C$ tais que $\pi(Q) = \pi(R) = (a : c)$, a saber, $Q = (a : b_1 : c)$ e $R = (a : b_2 : c)$, onde b_1 e b_2 são as duas raízes da equação $y^2c - a^3 + c^3 = 0$. Se $(a : c)$ é um ponto finito, isto é, $c \neq 0$, então podemos supor $c = 1$ e neste caso b_1 e b_2 são as duas raízes da equação $y^2 = a^3 - 1$. Na verdade, quando $a^3 = 1$, esta equação se reduz $y^2 = 0$ e, portanto ela possui apenas uma solução (dupla). Esta é uma situação que, na linguagem clássica, a aplicação π é chamada de um *recobrimento duplo* de $\mathbb{P}^1(\mathbb{C})$. Isto significa que, C “recobre” a reta projetiva $\mathbb{P}^1(\mathbb{C})$ “duas” vezes no sentido que, para $(a : b) \notin \{(1 : 1), (\omega : 1), (\omega^2 : 1)\}$, com $\omega^3 = 1$, tem-se que $\pi^{-1}(a : b)$ são dois pontos distintos de C . Esta é a situação geométrica. Do ponto de vista

algébrico, temos que π induz uma inclusão do corpo de funções de $\mathbb{P}^1(\mathbb{C})$ no corpo de funções de C , isto é $k(\mathbb{P}^1(\mathbb{C})) \subset k(C)$. Ora, $k(\mathbb{P}^1(\mathbb{C})) = k(x)$ e $k(C) = k(x, y) = k(x)[y]$, onde $y^2 = x^3 - 1$. Assim, $k(C) \mid k(\mathbb{P}^1(\mathbb{C}))$ é a extensão de corpos $k(x)[y] \mid k(x)$ de grau 2. Portanto, informações geométricas da projeção π podem ser obtidas da extensão $k(x)[y] \mid k(x)$. Isto é o que faremos para estudar os chamados “pontos de Galois” associados à curva C .

Daqui para frente admitiremos k sendo um corpo algebricamente fechado de característica zero. Seja $K \mid k$ um corpo de funções algébricas em uma variável.

Um subcorpo intermediário $k \subseteq K' \subseteq K$ é chamado *subcorpo racional maximal* se K' é racional e, para qualquer subcorpo intermediário K'' contendo K' , isto é, $K' \subseteq K'' \subseteq K$, tem-se necessariamente $K'' = K'$. Vamos fixar então um subcorpo racional maximal K_m de K . Pelo teorema de Lüroth, cada subcorpo K' satisfazendo $k \neq K' \subseteq K_m$ é racional. Estamos interessados em estudar a estrutura da extensão $K \mid K_m$. Por exemplo:

1. Quando ela é uma extensão galoisiana?
2. Se L é o fecho galoisiano de $K \mid K_m$, qual é o grupo de Galois da extensão $L \mid K_m$?

Definição 2.1. A *gonalidade* de K é definida por

$$\text{Gon}(K) = \min\{m \mid m = [K : k(t)]\},$$

onde t é uma transcendente de K sobre k .

Definição 2.2. Um subcorpo racional maximal satisfazendo

$$[K : K_m] = \text{Gon}(K)$$

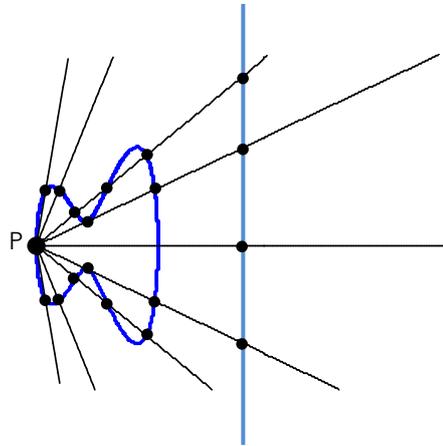
é chamado um subcorpo racional *g-maximal*.

Observe que existem muitos subcorpos racionais maximais que não são *g-maximal*s. Veja o exemplo abaixo.

Seja $K = k(x, y)$ o corpo de funções tal que $y^2 = x^3$ e seja $p = 2q + 3$ um número primo. Seja $z = x^q y$, claramente temos que $k(x, y) = k(x, z) = K$. Como $z^2 = x^{2q} \cdot y^2 = x^{2q+3} = x^p$, segue que $[K : k(z)] = p$. Isto decorre do fato que x é raiz do polinômio $X^p - z^2 \in k(z)[X]$, que é irredutível sobre $k(z)$. A irredutibilidade pode ser verificada em [8], III.1.14 Proposition. Consequentemente temos que $k(z)$ é um subcorpo racional maximal, mas não é *g-maximal*.

Quando K é o corpo das funções racionais de uma curva plana não singular C de grau $d \geq 2$ temos que, se K_m é um subcorpo racional g -maximal, então $[K : K_m] = d - 1$, e a extensão $K | K_m$ pode ser obtida por $\pi_p^* : k(\mathbb{P}^1) \hookrightarrow k(C)$, onde π_p é uma projeção de C sobre uma reta com um centro $P \in C$ (Estes resultados podem ser conferidos em [6], Theorem 5.3.17.).

Figura 2.1: Projeção π_p com centro em $P \in C$



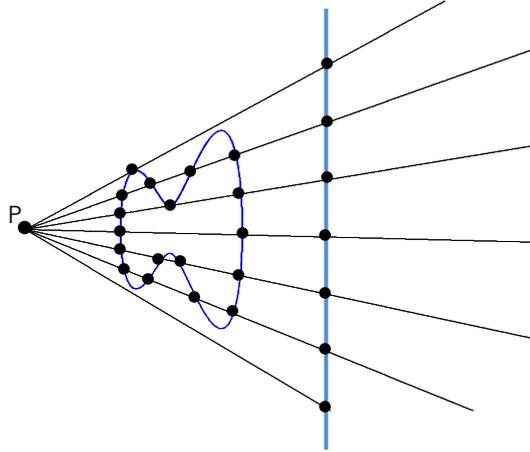
Seguindo a situação acima, também consideraremos uma projeção π_p de C em uma reta l com centro em $P \notin C$ (Veja a página 76 de [6]). Então temos uma extensão de corpos

$$\pi_p^* : k(\mathbb{P}^1) \hookrightarrow k(C) \text{ tal que } [k(C) : k(\mathbb{P}^1)] = d.$$

Neste caso vemos que $k(\mathbb{P}^1)$ é um subcorpo racional maximal $k(C)$, mas não é g -maximal.

Estamos interessados nas projeções centrais π_P , com $P \in C$, e com $P \notin C$, sendo C uma curva projetiva plana não singular. É fácil ver que a extensão de corpos não depende da reta l sobre a qual estamos projetando C , no entanto depende do ponto P , assim denotaremos o corpo de funções $k(\mathbb{P}^1)$ por K_P e L , o fecho galoisiano $k(C) | K_P$, por L_P .

Definição 2.3. Um ponto $P \in \mathbb{P}^2$ é chamado **ponto de Galois** ou **ponto galoisiano** da curva C se $k(C) | K_P$ é uma extensão galoisiana.

Figura 2.2: Projeção π_P com centro em $P \notin C$


Seja \tilde{C}_P o modelo não singular de uma curva cujo corpo de funções seja L_P , e seja $\tilde{\pi}_P : \tilde{C}_P \rightarrow C$ o recobrimento induzido por $k(C) \hookrightarrow L_P$. O gênero de \tilde{C}_P será denotado por $g(P)$ e o grupo de Galois $Gal(L_P/K_P)$ por G_P .

Observe que toda extensão de grau dois é galoisiana, assim, quando C é uma curva de grau 2, temos que as extensões são todas galoisianas qualquer que seja o ponto $P \in \mathbb{P}^2$, portanto $L_P = k(C)$, $g(P)$ é igual ao gênero de C , e as respostas às questões “1” e “2” são triviais. Nos concentraremos agora nos casos em que o grau da extensão $k(C) | K_P$ é igual a 3, isto é, quando $d = 3$ e $P \notin C$, e quando $d = 4$ e $P \in C$.

Definição 2.4. Denotaremos a quantidade de pontos de Galois da curva C por $\delta(C)$.

2.2 Projeção de uma quártica

Nesta seção estaremos interessados no caso da projeção central de uma quártica projetiva plana com centro $P \in C$.

Teorema 2.5. *Seja C uma curva quártica projetiva não singular em $\mathbb{P}^2(\mathbb{C})$ e P um ponto de C . Então temos,*

- (1) P é um ponto de Galois de C se, e somente se, $g(P) = 3$;

- (2) Se P não é ponto de Galois de C então $g(P) \in \{6, 7, 8, 9, 10\}$;
- (3) Genericamente, $g(P) = 10$ e $G_P \cong S_3$, o grupo simétrico de 3 letras;
- (4) A quantidade de pontos de Galois de C é $\delta(C) = 0, 1$, ou 4. Além disso, se C é uma quártica genérica então $\delta(C) = 0$.

Prova. Sejam C uma curva quártica plana projetiva não singular e P um ponto de C . Sejam $f = f(x, y) = 0$ uma equação afim para C e $f_i(x, y)$ a parte homogênea de grau i de f , isto é,

$$f(x, y) = f_4(x, y) + f_3(x, y) + f_2(x, y) + f_1(x, y) + f_0(x, y).$$

Vamos escrever também $\varphi_i(t) = f_i(1, t)$.

Após uma mudança projetiva de coordenadas conveniente podemos assumir que:

- (i) $P = (0, 0)$;
- (ii) a reta X e C se intersectam transversalmente em cada uma de suas intersecções;
- (iii) a reta Y é a reta tangente a C em P ;
- (iv) se l é uma reta que passa por P e por um ponto de C no infinito, então ela não é uma reta tangente em nenhum ponto de C .

Como existe uma quantidade finita de retas tangentes a C passando por P ¹, podemos considerar a “reta no infinito” como sendo uma das infinitas retas existentes satisfazendo a condição desejada.

Seja l_t a reta $y = tx$. Assim podemos supor que a projeção π_P é definida como sendo $\pi_P(C \cap l_t) = t \in \mathbb{A}^1$.

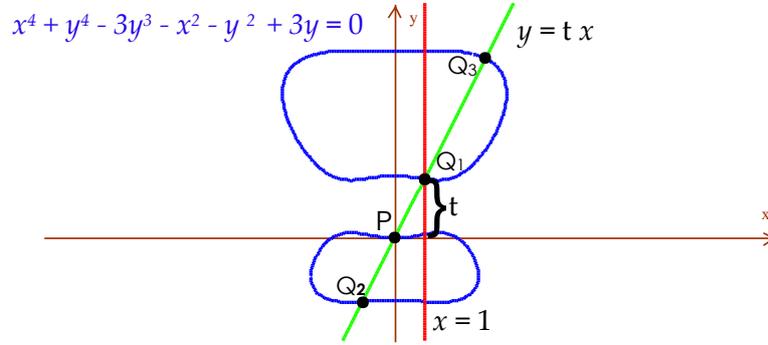
Considere no plano afim \mathbb{A}^2 a curva \hat{C} definida por

$$\hat{f}(x, t) = \frac{f(x, tx)}{x} = \varphi_4(t)x^3 + \varphi_3(t)x^2 + \varphi_2(t)x + \varphi_1(t).$$

Na verdade \hat{C} é a explosão de C na origem. Quando $t = \infty$, consideramos $x = sy$, onde $st = 1$. Denotaremos $k(t) = K_P$ e $k(C) = K$. Observe que pela definição de \hat{C} , temos $k(C) = k(\hat{C})$, pois $k(x, y) = k(x, t)$.

¹Que o número de retas tangentes a C passando por P é finito podemos verificar na página 90 de [10]

Figura 2.3:



Como $\varphi_4(t) \neq 0$, temos

$$\frac{d\hat{f}}{dx}(x, t) = 3\varphi_4(t)x^2 + 2\varphi_3(t)x + \varphi_2(t) \text{ não constante,}$$

e com esta hipótese, o discriminante $D(t)$ de $\hat{f}(x, t) \in k[t][x]$ (veja página 75 de [2]) está definido:

$$\begin{aligned} D(t) &= \det \begin{bmatrix} \varphi_4(t) & \varphi_3(t) & \varphi_2(t) & \varphi_1(t) & 0 \\ 0 & \varphi_4(t) & \varphi_3(t) & \varphi_2(t) & \varphi_1(t) \\ 3\varphi_4(t) & 2\varphi_3(t) & \varphi_2(t) & 0 & 0 \\ 0 & 3\varphi_4(t) & 2\varphi_3(t) & \varphi_2(t) & 0 \\ 0 & 0 & 3\varphi_4(t) & 2\varphi_3(t) & \varphi_2(t) \end{bmatrix} \\ &= \varphi_4(t) \cdot \det \begin{bmatrix} \varphi_4(t) & \varphi_3(t) & \varphi_2(t) & \varphi_1(t) \\ 2\varphi_3(t) & \varphi_2(t) & 0 & 0 \\ 3\varphi_4(t) & 2\varphi_3(t) & \varphi_2(t) & 0 \\ 0 & 3\varphi_4(t) & 2\varphi_3(t) & \varphi_2(t) \end{bmatrix} + \\ &\quad + 3 \cdot \varphi_4(t) \cdot \det \begin{bmatrix} \varphi_3(t) & \varphi_2(t) & \varphi_1(t) & 0 \\ \varphi_4(t) & \varphi_3(t) & \varphi_2(t) & \varphi_1(t) \\ 3\varphi_4(t) & 2\varphi_3(t) & \varphi_2(t) & 0 \\ 0 & 3\varphi_4(t) & 2\varphi_3(t) & \varphi_2(t) \end{bmatrix} \end{aligned}$$

portanto,

$$D(t) = -\varphi_4(\varphi_2^2\varphi_3^2 + 18\varphi_1\varphi_2\varphi_3\varphi_4 - 4\varphi_2^3\varphi_4 - 4\varphi_1\varphi_3^3 - 27\varphi_1^2\varphi_4^2),$$

onde $\varphi_i = \varphi_i(t)$.

Segue de ([2] p. 84), que

$$D(t) = -\varphi_4(t)^5 \prod_{i < j} (x_i - x_j)^2,$$

onde os x_i são as raízes de $\hat{f}(x, t) = 0$ no fecho algébrico de $k(t)$.

Observe ainda que, como $\varphi_4(t) \neq 0$, temos que,

$$D(t) = 0 \text{ se, e somente se, } \hat{f}(x, t) \text{ possui raiz múltipla.}$$

(veja [2], Proposição III.3.15).

Neste trabalho, terão grande importância os valores t , para os quais $\hat{f}(x, t)$ possua raízes múltiplas. Por isto, daqui por diante chamaremos de *discriminante de $\hat{f}(x, t) \in k[t][x]$* o polinômio $\psi(t) \in k[t]$ definido por

$$\psi(t) = \frac{D(t)}{-\varphi_4(t)},$$

isto é,

$$\begin{aligned} \psi(t) &= \varphi_2^2 \varphi_3^2 + 18\varphi_1 \varphi_2 \varphi_3 \varphi_4 - 4\varphi_2^3 \varphi_4 - 4\varphi_1 \varphi_3^3 - 27\varphi_1^2 \varphi_4^2 = \\ &= \varphi_4(t)^4 \prod_{i < j} (x_i - x_j)^2. \end{aligned}$$

Observe que também podemos considerar π_P como sendo a projeção de \hat{C} sobre o eixo $t \in \mathbb{A}^1(\mathbb{C})$.

Utilizando as notações já introduzidas anteriormente (página 14), escreveremos $I(C \cdot T_Q, Q)$ para denotar o índice de interseção de C com a reta T_Q tangente a C em $Q \in C$.

Lema 2.6. *Se $(t - \alpha)^{n_\alpha}$ é um fator de $\psi(t)$, então $n_\alpha = 1$ ou $n_\alpha = 2$.*

1. Para $\alpha \neq 0$ temos:

- (a) $n_\alpha = 2$ se, e somente se, a reta l_α é uma reta tangente a C em um ponto Q tal que $I(C \cdot T_Q, Q) = 3$; neste caso, Q é um ponto de inflexão ordinário de C .
- (b) $n_\alpha = 1$ se, e somente se, a reta l_α é uma reta tangente a C em um ponto Q tal que $I(C \cdot T_Q, Q) = 2$; neste caso, l_α é uma reta tangente “ordinária” de C .

2. Para $\alpha = 0$ temos:

- (a) $n_\alpha = 2$ se, e somente se, $I(C \cdot T_P, P) = 4$; neste caso, P é um ponto de inflexão de ordem 4 (reta tangente inflexional não ordinária) de C .
- (b) $n_\alpha = 1$ se, e somente se, $I(C \cdot T_P, P) = 3$ ou l_0 é uma reta bitangente. No caso $I(C \cdot T_P, P) = 3$, P é um ponto de inflexão ordinário de C .

Prova. Considere a aplicação de C sobre \mathbb{P}^1 (parte afim) $\pi_P : C \rightarrow \mathbb{P}^1$ tal que se $Q \in C \cap l_t$ então $\pi_P(Q) = t \in \mathbb{A}^1 \subset \mathbb{P}^1$. Então π_P induz uma imersão $\pi_P^* : \Gamma(\mathbb{P}^1) \rightarrow \Gamma(C)$. Suponha que $\alpha \in \mathbb{A}^1$ seja uma raiz de ψ . Observe que $s = t - \alpha$ é um parâmetro local em $\alpha \in \mathbb{A}^1$. Pela imersão π_P^* , podemos ver s no anel das funções regulares $\Gamma(C)$ ou ainda, no anel local $\vartheta_Q(C)$. Seja u um parâmetro local em $Q \in C$. Então podemos escrever

$$s = \lambda_m u^m + \lambda_{m+1} u^{m+1} + \cdots = u^m (\lambda_m + \lambda_1 u + \lambda_2 u^2 + \cdots)$$

onde $\lambda_i \in \mathbb{C}$ e $\lambda_m \neq 0$. Assim, mudando de parâmetro local em Q (já que $\lambda_m + \lambda_1 u + \lambda_2 u^2 + \cdots$ é inversível em $\vartheta_Q(C)$), podemos supor $s = u^m$. Como $gr(C) = 4$, vemos claramente que $1 \leq m \leq 3$. Suponha que $m = 3$. Como $s - u^3 = 0$ em $\vartheta_Q(\hat{C})$, podemos escrever

$$s - u^3 = \frac{g(x, t)}{h(x, t)} \text{ com } g(x, t), h(x, t) \in \Gamma(\hat{C}), g(Q) = 0 \text{ e } h(Q) \neq 0.$$

Assim g é múltiplo de \hat{f} em $\mathbb{C}[x, t]$, digamos $g(x, t) = g_1(x, t)\hat{f}(x, t)$ para algum $g_1(x, t)$. Logo,

$$(s - u^3)h(x, t) = g_1(x, t)\hat{f}(x, t).$$

Observe que necessariamente, $g_1(Q) \neq 0$ devido à ordem do zero da função $s - u^3$ em Q . Assim, $\hat{f}(x, t) = (s - u^3) \cdot \varepsilon(u)$, onde $\varepsilon(u)$ é um inversível em $\vartheta_Q(\hat{C})$.

Escolha uma raiz cúbica de s (no fecho algébrico), digamos $u_0 = \sqrt[3]{s}$ e ω uma raiz cúbica primitiva da unidade. Assim, numa vizinhança de $s = 0$, o discriminante ψ será

$$\begin{aligned} \psi(t) &= -\varepsilon(u)^5 (u_0 - u_0\omega)^2 (u_0 - u_0\omega^2)^2 (u_0\omega - u_0\omega^2)^2 \\ &= -\varepsilon(u)^5 (1 - \omega)^2 (1 - \omega^2)^2 (\omega - \omega^2)^2 u_0^6 \\ &= -\varepsilon(u)^5 (1 - \omega)^4 (1 - \omega^2)^2 \omega^2 \cdot s^2 \end{aligned}$$

Como $s = t - \alpha$, podemos escrever

$$\psi(t) = -\varepsilon(u)^5(1 - \omega)^4(1 - \omega^2)^2\omega^2(t - \alpha)^2 = \varepsilon_1(u) \cdot (t - \alpha)^2,$$

onde $\varepsilon_1(u)$ é inversível numa vizinhança de $t = \alpha$.

De maneira análoga, quando $m = 2$, obtemos que $\psi(t) = \varepsilon_2(u) \cdot (t - \alpha)$. Também quando $\alpha = 0$, uma análise análoga nos fornece o resultado do lema.

Como observamos anteriormente, podemos considerar π_P como a projeção de \hat{C} sobre o eixo t . Agora, considerando $Q_i \neq Q_j$ sempre que $i \neq j$, teremos teremos as seguintes opções para a imagem inversa de π_P em α :

1. Para $\alpha \neq 0$

- (a) $\pi_P^{-1}(\alpha) = \{Q_1, Q_2, Q_3\} \Leftrightarrow m_\alpha = 1 \Leftrightarrow n_\alpha = 0$;
- (b) $\pi_P^{-1}(\alpha) = \{Q_1, Q_2\} \Leftrightarrow m_\alpha = 2 \Leftrightarrow n_\alpha = 1$;
- (c) $\pi_P^{-1}(\alpha) = \{Q_1\} \Leftrightarrow m_\alpha = 3 \Leftrightarrow n_\alpha = 2$.

2. Para $\alpha = 0$

- (a) $\pi_P^{-1}(0) = \{P, Q_1, Q_2\} \Leftrightarrow m_0 = 1 \Leftrightarrow n_0 = 0$;
- (b) $\pi_P^{-1}(0) = \{P, Q_1\} \Leftrightarrow m_0 = 2 \Leftrightarrow n_0 = 1$;
- (c) $\pi_P^{-1}(0) = \{P\} \Leftrightarrow m_0 = 3 \Leftrightarrow n_0 = 2$.

Dado um t fixo, se $x_1, x_2, e x_3$ são as raízes de

$$\hat{f}(x, t) = \varphi_4(t)x^3 + \varphi_3(t)x^2 + \varphi_2(t)x + \varphi_1(t),$$

então as raízes de $f(x, tx)$ são x_1, x_2, x_3 e 0. Pelo Teorema de Bézout, como C tem grau 4 e l_α tem grau 1, as possibilidades dos pontos de interseção entre estas duas curvas, levando em consideração as multiplicidades, são:

1. Para $\alpha \neq 0$

- (a) $\pi_P^{-1}(\alpha) = (P, Q_1, Q_2, Q_3) \Leftrightarrow l_\alpha$ não é tangente a C
 $\pi_P^{-1}(\alpha) = (P, Q_1, Q_2, Q_3) \Leftrightarrow n_\alpha = 0$;
- (b) $\pi_P^{-1}(\alpha) = (P, Q_1, Q_1, Q_2) \Leftrightarrow l_\alpha$ é tangente a C em Q_1 ,
 com $I(C \cdot l_\alpha, Q_1) = 2$
 $\pi_P^{-1}(\alpha) = (P, Q_1, Q_1, Q_2) \Leftrightarrow n_\alpha = 1$;

- (c) $\pi_P^{-1}(\alpha) = (P, Q_1, Q_1, Q_1) \Leftrightarrow l_\alpha$ é tangente a C em Q_1 ,
 com $I(C \cdot l_\alpha, Q_1) = 3$
 $\pi_P^{-1}(\alpha) = (P, Q_1, Q_1, Q_1) \Leftrightarrow n_\alpha = 2$.

2. Para $\alpha = 0$

- (a) $\pi_P^{-1}(\alpha) = (P, P, Q_1, Q_2) \Leftrightarrow l_0$ é tangente a C em P ,
 com $I(C \cdot l_0, P) = 2$
 $\pi_P^{-1}(\alpha) = (P, P, Q_1, Q_2) \Leftrightarrow n_0 = 0$
- (b) $\pi_P^{-1}(\alpha) = (P, P, Q_1, Q_1) \Leftrightarrow l_0$ é bitangente a C , em P e em Q_1
 $\pi_P^{-1}(\alpha) = (P, P, Q_1, Q_1) \Leftrightarrow n_0 = 1$
- (c) $\pi_P^{-1}(\alpha) = (P, P, P, Q_1) \Leftrightarrow l_0$ é tangente a C em P ,
 com $I(C \cdot l_0, P) = 3$
 $\pi_P^{-1}(\alpha) = (P, P, P, Q_1) \Leftrightarrow n_0 = 1$
- (d) $\pi_P^{-1}(\alpha) = (P, P, P, P) \Leftrightarrow l_0$ é tangente a C em P ,
 com $I(C \cdot l_0, P) = 4$
 $\pi_P^{-1}(\alpha) = (P, P, P, P) \Leftrightarrow n_0 = 2$

Com estes resultado concluímos a demonstração do Lema 2.6. ■

Pela escolha de coordenadas vemos que $t = \alpha \neq 0$ é um ponto ramificado se, e somente se, l_α é uma reta tangente a C , ou equivalentemente α é uma raiz de $\psi(t) = 0$. Além disto, a condição (ii) nos garante que $t = \infty$ não é um ponto ramificado, e pela condição (iv), se $\varphi_4(\alpha) = 0$, então $t = \alpha$ não é um ponto ramificado. Sejam a e b os números de fatores simples e duplos de $\psi(t)$, respectivamente. Pelas condições de (i) a (iv), todos os pontos ramificados de $\pi_P : C \rightarrow l$ aparecem em $\hat{C} \rightarrow \mathbb{A}^1$, o que nos dá

$$\psi(t) = \lambda(t - \alpha_1) \dots (t - \alpha_a)(t - \alpha_{a+1})^2 \dots (t - \alpha_{a+b})^2,$$

com $\lambda, \alpha_1, \dots, \alpha_{a+b} \in k$, e $\lambda \neq 0$.

Agora, sendo m_α o índice de ramificação em α , temos $n_\alpha = m_\alpha - 1$, então, pela fórmula de Riemann-Hurwitz para o recobrimento $\pi_p : C \rightarrow l$, temos

$$\begin{aligned} 2g_C - 2 &= [k(C) : k(l)](2g_l - 2) + \sum (m_\alpha - 1) \\ 2 \times 3 - 2 &= 3(2 \times 0 - 2) + (a + 2b) \\ 4 &= -6 + (a + 2b) \end{aligned}$$

o que resulta em $a + 2b = 10$. Podemos assim concluir que o grau de $\psi(t)$ é igual a 10.

Dos resultados apresentados até aqui fica clara a seguinte observação.

Observação 2.7. *Seja $P \in C$, onde C é uma quártica não singular e seja T_P a tangente a C em P . Existem dois inteiros não negativos “ a ” e “ b ”, tais que $a + 2b = 10$ e o número de retas tangentes a C , distintas de T_P , é dado por:*

1. *Se T_P é uma tangente com índice de intersecção igual a 2*
 - “ a ” tangentes com índice de intersecção igual a 2;
 - “ b ” tangentes inflexionais.
2. *Se T_P é uma bitangente*
 - “ $a - 1$ ” tangentes com índice de intersecção igual a 2;
 - “ b ” tangentes inflexionais.
3. *Se T_P é uma inflexional com índice de intersecção igual a 3*
 - “ $a - 1$ ” tangentes com índice de intersecção igual a 2;
 - “ b ” tangentes inflexionais.
4. *Se T_P é uma inflexional com índice de intersecção igual a 4*
 - “ a ” tangentes com índice de intersecção igual a 2;
 - “ $b - 1$ ” tangentes inflexionais.

Levando em consideração que o índice de intersecção é invariante por mudança de coordenadas, temos que o número de retas tangentes passando por P também é invariante por mudança de coordenadas. Este argumento nos mostra que, se não exigíssemos a condição (ii), poderíamos ter a reta $X = 0$ tangente à curva C , e conseqüentemente $\hat{C} \rightarrow \mathbb{A}^1$ teria um ponto ramificado a menos. Isto nos leva à seguinte observação referente ao grau do discriminante $\psi(t)$.

Observação 2.8. *O grau do discriminante $\psi(t)$ é igual a:*

- 10 se, e somente se, $X = 0$ e C se intersectam transversalmente;
- 9 se, e somente se, $X = 0$ é tangente ordinária de C ;
- 8, se e somente se, $X = 0$ é tangente inflexional de C .

Seja D_P a curva não singular com o corpo de funções $M_P = k(t, z)$, onde $z^2 = \psi(t)$. Esta curva é chamada *curva discriminante*.

Suponha que $z^2 = \psi(t) = \lambda\psi_1(t)\psi_2(t)^2$, onde $\psi_1(t)$ e $\psi_2(t)$ têm apenas fatores simples. Então o grau de $\psi_1(t)$ é igual a a , o grau de $\psi_2(t)$ é igual a b , e obtemos $L_P = k(x, t, z)$.

Observe que $k[x, y, z]$ é o produto tensorial de $k[x, t]$ por $k[t, z]$ sobre $k[t]$ e, portanto \tilde{C}_P é a desingularização do produto fibrado de C por D_P sobre \mathbb{P}^1 . O diagrama seguinte ilustra esta situação.

$$\begin{array}{ccc} & C \times D_P & \\ \tilde{\pi}_P \swarrow & & \searrow \\ C & & D_P \\ \pi_P \searrow & & \swarrow \\ & \mathbb{P}^1 & \end{array}$$

Assim, concluímos que um ponto $Q \in C$ é um ponto ramificado do morfismo $\tilde{\pi}_P : \tilde{C}_P \rightarrow C$ se, e somente se, $\pi_P(Q) = \alpha$, com $\psi(\alpha) = 0$, e o índice de ramificação do recobrimento π_P no ponto Q é igual a um.

Então o número de pontos ramificados de $\tilde{\pi}_P$ é igual a a . Destas observações obtemos o seguinte lema.

Lema 2.9. *Se P não é um ponto de Galois, então $g(P) = 10 - b$, onde $0 \leq b \leq 4$.*

Prova. Como $a+2b = 10$, temos $b \leq 5$. No entanto, observe que se $b = 5$, então $\psi(t)$ seria um quadrado perfeito, e teríamos $z = \psi_2(t)$ ou $z = -\psi_2(t)$, o que nos daria $z \in k(t) \subset k(x, t) \Rightarrow k(x, t) = k(x, t, z) = L_P$, portanto π_P seria um recobrimento galoisiano, o que contradiz a hipótese. Portanto $b \leq 4$. Pela fórmula de Riemann-Hurwitz para o recobrimento $\tilde{\pi}_P : \tilde{C}_P \rightarrow C$, temos que

$$2g(P) - 2 = [k(\tilde{C}_P) : k(C)](2 \cdot g_C - 2) + a$$

$$2g(P) - 2 = 2(2 \cdot 3 - 2) + a$$

Portanto,

$$g(P) = \frac{10 + a}{2} = \frac{10 + (10 - 2b)}{2} = 10 - b.$$

O que prova o lema. ■

Após a demonstração deste lema podemos concluir os itens (1) e (2) do Teorema 2.5:

1. $g(P) = 3$ se, e somente se, P é um ponto de Galois;
2. $g(P) \in \{6, 7, 8, 9, 10\}$ se P não é um ponto de Galois.

Para computar a quantidade de pontos de inflexão sobre uma curva plana projetiva C , contando com multiplicidades, defina

$$W(C) := \sum_{Q \in C} [I(C \cdot T_Q, Q) - 2]$$

Lema 2.10. $W(C) = 24$.

Lembrando que $gr(C) = 4$ e $g(C) = 3$, a prova do Lema 2.10 segue dos resultados sobre pontos de inflexão que podem ser encontrados em [3], página 294. Estes resultados podem ser vistos como generalizações das fórmulas de Plücker clássicas.

O Lema 2.10 mostra que o conjunto dos pontos de inflexão de C é finito. Em particular obtemos o seguinte lema.

Lema 2.11. *Exceto para um número finito de pontos de C temos $g(P) = 10$.*

Prova. Se $I(C \cdot l_0, P) \neq 4$ e para cada α não nulo com $\psi(\alpha) = 0$, l_α não for uma reta tangente a C em um ponto de inflexão, então $g(P) = 10 - b = 10 - 0 = 10$. Como existem finitos pontos de inflexão em C , para um ponto genérico $P \in C$, temos $g(P) = 10$. ■

Este último lema nos mostra a primeira afirmação do item (3) do Teorema 2.5: a saber, em geral $g(P) = 10$.

Vamos mostrar agora que no caso genérico $G_P \cong S_3$. Como $g(P) = 10$ então a extensão $k(C) | K_m$ não é galoisiana. Portanto $[L : K_m] = 6$. Então $G_P \cong S_3$ ou $G_P \cong \mathbb{Z}_6$. Mais ainda como $k(C) | K_m$ não é galoisiana, pela correspondência de Galois, G_P possui 3 subgrupos de ordem 2, portanto $G_P \cong S_3$.

Para o item (4) do Teorema 2.5 temos a proposição seguinte.

Proposição 2.12. *O recobrimento $\pi_P : C \rightarrow \mathbb{P}_1$ é galoisiano se, e somente se, tomando uma transformação projetiva apropriada, a equação de C pode ser escrita como $f(x, y) = y + g(x, y)$, onde $g(x, y)$ é um polinômio homogêneo de grau quatro sem fator múltiplo e $g(x, 0) \neq 0$.*

Prova. O grau da extensão $k(C) | k(t)$ é igual a 3. Portanto, ela é galoisiana se, e somente se, o grupo de Galois a ela associado tem ordem 3.

Ora, a menos de isomorfismos, o único grupo de ordem 3 é o grupo cíclico de 3 elementos. Portanto a extensão é cíclica de grau 3, e usando o teorema 90 de Hilbert (p.213 de [4]) verifica-se que a extensão pode ser obtida da seguinte forma:

$$k(C) = k(x, t), \text{ onde } x^3 = \frac{a(t)}{b(t)}, \text{ com } a(t), b(t) \in k[t].$$

Colocando $y = tx$, obtemos que

$$b \left(\frac{y}{x} \right) x^3 = a \left(\frac{y}{x} \right).$$

Para se obter uma equação de grau 4, necessariamente a e b são polinômios de grau no máximo 1. Daí segue que C pode ser dada por uma equação da forma $a_1x^3y + a_2x^4 = b_1x + b_2y$, com $a_1, a_2, b_1, b_2 \in k$. Portanto, facilmente vemos que C é birracionalmente equivalente a uma curva definida por uma equação da forma $y + g(x, y) = 0$, onde $g(x, y)$ é um polinômio homogêneo de grau 4. Isto mostra a primeira parte da proposição.

Para mostrar que $g(x, y)$ não possui fatores múltiplos, suponha por contradição que pudéssemos escrever

$$g(x, y) = (a_1x + b_1y)^2(a_2x + b_2y)(a_3x + b_3y), \text{ com os } a_i \text{ e os } b_i \text{ em } k.$$

É fácil verificar que o ponto do infinito $(-b_1 : a_1 : 0)$ seria uma singularidade da curva C , contradizendo o fato que C é não singular. Finalmente, se $g(x, 0) = 0$ então o coeficiente de x^4 seria igual a zero e, portanto a curva C seria redutível, mas isto contradiz a nossa hipótese inicial.

Observe que a curva birracionalmente equivalente a C que obtivemos no final da demonstração é plana e não singular. Como a curva inicial C é plana e não singular, pela unicidade, a menos de transformação projetiva, do modelo não singular, necessariamente esta curva obtida é projetivamente equivalente a C . Isto conclui a prova da proposição. ■

Observação 2.13. Se $\pi_P : C \rightarrow \mathbb{P}_1$ é galoisiana, isto é, se $P \in C$ é um ponto de Galois, então $I(C \cdot Y, P) = 4$.

Pela Proposição 2.12, temos que C é dada por $f(x, y) = y + g(x, y)$ e a homogeneização de f é

$$F(X, Y, Z) = YZ^3 + (a_1X + b_1Y)(a_2X + b_2Y)(a_3X + b_3Y)(a_4X + b_4Y),$$

onde $a_i \neq 0$ para $i = 1, 2, 3, 4$, já que $g(x, 0) \neq 0$. Podemos então supor que o produto de todos a_i seja iguais a 1. Então podemos escrever

$$F(X, Y, Z) = YZ^3 + X^4 + YB(X, Y) = X^4 + Y(Z^3 + B(X, Y)),$$

onde $B(X, Y)$ é um polinômio homogêneo de grau 3 em X e Y . Assim, a multiplicidade de intersecção $I(Y \cdot C, P)$ será

$$\begin{aligned} I(Y \cdot F, P) &= I(Y \cdot [X^4 + Y(Z^3 + B(X, Y))], P) \\ &= I(Y \cdot X^4, P) \\ &= 4 \cdot I(Y \cdot X, P) = 4 \cdot 1 = 4. \end{aligned}$$

Para completar a prova do Teorema 2.5 precisamos verificar o item (4), a saber, temos que mostrar que o número de pontos de Galois de C é 0, 1 ou 4.

Observe que o corpo $k(x, y)$ é uma extensão galoisiana de $k(t)$ se, e somente se, $\sqrt{\psi(t)} \in k(t)$. Podemos expressar geometricamente esta condição como:

O ponto P é tal que $I(C \cdot l_0, P) = 4$, e se l_α ($\alpha \neq 0$) é uma reta tangente a C em algum ponto $Q \in C$, então $I(C \cdot l_\alpha, P) = 3$. Isto mostra que cada ponto de Galois determina quatro pontos tais que $I(C \cdot l_\alpha, P) = 3$, isto é, quatro pontos ordinários de inflexão. Calculando $\sum [I(C \cdot T_Q, Q) - 2]$ apenas para um ponto de Galois e para os quatro pontos que o seguem, temos

$$\sum_{Q \in C} [I(C \cdot T_Q, Q) - 2] = 2 + 1 + 1 + 1 + 1 = 6.$$

No entanto, pelo Lema 2.10 temos que

$$W(C) = \sum_{Q \in C} [I(C \cdot T_Q, Q) - 2] = 24,$$

concluimos que $\delta(C) \cdot 6 \leq 24$, portanto, $\delta(C) \leq 4$.

Se C é uma quártica genérica, então $\delta(C) = 0$, pois ela não possui pontos P tais que $I(C \cdot T_P, P) = 4$ (Veja [7], página 138).

Suponha que C tem um ponto de Galois P , então podemos assumir que $P = (0, 0)$ e que a equação afim que define C é escrita como $f(x, y) = y + g(x, y)$ como na proposição 2.12. No caso em que C tenha um outro ponto de Galois Q distinto de P , isto é, $Q \neq (0, 0)$, então vemos que $\delta(C) = 4$. Esta última afirmação é facilmente verificada considerando a transformação projetiva

$$\Psi(x, y) = (\omega x, \omega y),$$

onde ω é uma raiz cúbica primitiva da unidade. Veja que $\Psi(C) = C$ e que desta forma obtemos quatro pontos de Galois, a saber,

$$\begin{aligned} P_1 &= (0, 0) & P_2 &= (a, b) \neq (0, 0) \\ P_3 &= \Psi(P_2) = (\omega a, \omega b) & P_4 &= \Psi(\Psi(P_2)) = (\omega^2 a, \omega^2 b). \end{aligned}$$

Com este último resultado completamos a prova do Teorema 2.5. ■

2.3 O caso de uma cúbica plana não singular

Teorema 2.14. *Para cada cúbica C não singular plana e cada ponto $P \notin C$, temos:*

1. $g(P) = 1$ se, e somente se, P é um ponto de Galois;
2. $g(P) = 2, 3, 4$ se, e somente se, P não é um ponto de Galois;
3. $g(P) = 4$ e $G_P \cong S_3$ se P é ponto genérico.

Prova. Tomando uma mudança projetiva de coordenadas conveniente, podemos assumir que:

- (i) $P = (0, 0) \notin C$
- (ii) $X = 0$ e C se intersectam transversalmente em todas as suas intersecções.

Pela escolha de coordenadas temos

$$f(x, y) = f_3(x, y) + f_2(x, y) + f_1(x, y) + c,$$

onde c é um elemento não nulo k , e $f_i(x, y)$ é a parte homogênea de grau i de $f(x, y)$. Seja l_t a reta $y = tx$. Então podemos supor que a projeção é definida como $\pi_P(C \cap l_t) = t \in \mathbb{A}^1 \subset \mathbb{P}^1$.

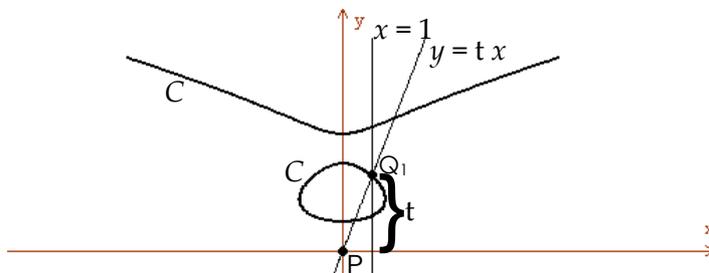
Novamente fazendo $f_i(1, t) = \varphi_i(t)$ teremos no plano afim $(x, t) \in \mathbb{A}^2$, a curva \check{C} definida por

$$\check{f}(x, t) = f(x, tx) = \varphi_3(t)x^3 + \varphi_2(t)x^2 + \varphi_1(t)x + c.$$

A relação $y = tx$ nos dá $k(x, y) = k(x, t)$, conseqüentemente $k(C) = k(\check{C})$. Desta forma estudaremos a extensão K/K_P , onde $K = k(x, t)$ e $K_P = k(t)$.

Sendo $\psi(t)$ o discriminante de $\check{f}(x, t) \in k[t][x]$, temos o seguinte lema por um argumento similar ao Lema 2.6.

Figura 2.4:



Lema 2.15. *Se $(t - \alpha)^{n_\alpha}$ é um fator de $\psi(t)$, então $n_\alpha = 1$ ou $n_\alpha = 2$. Além disso:*

- (1) $n_\alpha = 1$ se, e somente se, a reta l_α é uma reta tangente em um ponto que não seja ponto de inflexão de C ;
- (2) $n_\alpha = 2$ se, e somente se, a reta l_α é uma reta tangente a C em um ponto Q tal que $I(C \cdot T_Q, Q) = 3$.

Conforme a prova do Lema 2.6, temos as equivalências:

1. $\pi_P^{-1}(\alpha) = \{Q_1, Q_2, Q_3\} \Leftrightarrow m_\alpha = 1 \Leftrightarrow n_\alpha = 0$.
2. $\pi_P^{-1}(\alpha) = \{Q_1, Q_2\} \Leftrightarrow m_\alpha = 2 \Leftrightarrow n_\alpha = 1$.
3. $\pi_P^{-1}(\alpha) = \{Q_1\} \Leftrightarrow m_\alpha = 3 \Leftrightarrow n_\alpha = 2$.

Pela escolha das coordenadas, vemos que $t = \alpha$ é um ponto ramificado se, e somente se, l_α é uma reta tangente de C , ou equivalente $\psi(\alpha) = 0$. Além disto, a condição (ii) nos garante que $t = \infty$ não é um ponto ramificado. Assim consideraremos o recobrimento $\tilde{C} \rightarrow \mathbb{A}^1$.

Sejam a e b os números de fatores simples e duplos de $\psi(t)$, respectivamente. Novamente, sendo m_α o índice de ramificação em α , temos $n_\alpha = m_\alpha - 1$, e, lembrando que $g_C = g(C) = 1$ e $g_l = g(l) = 0$, pela fórmula de Riemann-Hurwitz temos que

$$2g_C - 2 = [k(C) : k(l)](2g_l - 2) + \sum(m_\alpha - 1)$$

$$2 \cdot 1 - 2 = 3(2 \cdot 0 - 2) + (a + 2b)$$

Segue que $a + 2b = 6$.

Daí temos que o grau de $\psi(t)$ é igual a 6.

Podemos ver que P é um ponto de Galois se, e somente se, $\psi(t)$ é um quadrado perfeito, ou seja, se e somente se $b = 3$. Assim, um ponto de Galois precisa de três pontos de inflexão.

Então temos o seguinte lema análogo ao Lema 2.9.

Lema 2.16. *Se P não é um ponto de Galois, então $g(P) = 4 - b$, onde $0 \leq b \leq 2$.*

Prova. Admitindo que P não seja um ponto de Galois, isto é, que $0 \leq b \leq 2$, pela fórmula de Riemann-Hurwitz para o recobrimento $\tilde{\pi}_P : \check{C}_P \rightarrow C$, temos que

$$2g(P) - 2 = [k(\check{C}_P) : k(C)](2 \times g_C - 2) + a$$

$$2g(P) - 2 = 2(2 \times 1 - 2) + a$$

Segue que

$$g(P) = \frac{2 + a}{2}.$$

Como $a + 2b = 6$, vemos imediatamente que $g(P) = 4 - b$ ■

Fica assim estabelecido o item (2) do Teorema 2.14.

Agora, poderíamos proceder como no caso da curva quártica não singular para computar a quantidade de pontos de inflexão ao calcular $W(C)$ utilizando os resultados encontrados em [3], página 294. No entanto, no caso de uma cúbica, só podemos ter pontos de inflexão ordinários. Assim podemos utilizar as fórmulas clássicas de Plücker e encontrar $W(C) = 9$. (Veja o capítulo 7 de [10]).

Assim, novamente temos uma quantidade finita de pontos de inflexão e, portanto a afirmação sobre a genericidade de C segue. Como C tem 9 pontos de inflexão, se $P \notin \bigcup_{\alpha} l_{\alpha}$, onde l_{α} são retas tangentes em pontos de inflexão, então $\psi(t)$ tem somente fatores simples, ou equivalentemente $b = 0$. Assim vemos que se P é um ponto genérico, então $g(P) = 4$. A prova de que $G_P \cong S_3$ é completamente análoga ao caso da quártica. Isto conclui a demonstração do Teorema 2.14.

Observação 2.17. *Perceba que para cada ponto de Galois precisamos de três retas inflexionais. Usando o fato de que C tem exatamente 9 retas inflexionais, encontramos*

$$\delta(C) < \infty.$$

Dos resultados apresentados até aqui fica clara a seguinte observação.

Observação 2.18. *Seja C uma curva cúbica suave e P um ponto fora de C . Pelo ponto P passam “ a ” retas tangente ordinárias de C , e “ b ” retas tangentes inflexionais ordinárias de C , de modo que $a + 2b = 6$.*

2.4 Exemplos com $P \in C$

Nesta secção vamos mostrar, através de exemplos, que todos os gêneros $g(P) \in \{3, 6, 7, 8, 9, 10\}$ obtidos por este processo conforme o Teorema 2.5 para curvas quárticas planas projetivas C não singulares e $P \in C$ ocorrem.

O Teorema 2.5 nos mostra que, se C é uma quártica suave e $P \in C$, então $g(P) \in \{3, 6, 7, 8, 9, 10\}$. No entanto não é demonstrado que, para cada $g \in \{3, 6, 7, 8, 9, 10\}$, existe alguma quártica C e algum ponto $P \in C$ tal que $g(P) = g$.

Nos exemplos a seguir, para cada $g \in \{3, 6, 7, 8, 9, 10\}$, vamos explicitar uma quártica C e um ponto $P \in C$ tal que $g(P) = g$.

Exemplo 2.19. *Se C é a curva quártica de Fermat $x^4 + y^4 = 1$, a configuração dos pontos de inflexão de C , no caso em que $P \in C$ é:*

1. *Se P é um **ponto de inflexão**, então $g(P) = 9$. Note que, neste caso, existem 12 **pontos de inflexão**.*
2. *Se P não é um **ponto de inflexão**, então $G_P \cong S_3$ e $g(P) = 10$.*

Assim vemos que $\delta(C) = 0$.

Prova. A curva quártica de Fermat $C : F = X^4 + Y^4 - Z^4 = 0$ é não singular e possui 12 pontos de inflexão. Além disso, se Q é um desses pontos de inflexão então $I(F \cdot T_Q, Q) = 4$, isto é, todos eles são pontos de inflexão não ordinários. Estes 12 pontos são

$$(0 : \lambda : 1), \quad (\lambda : 0 : 1) \quad \text{e} \quad (\rho : 1 : 0),$$

onde $\lambda^4 = 1$ e $\rho^4 = -1$. Para verificar este fato podemos usar as propriedades do índice de intersecção encontradas na página 14 desta dissertação. Observe inicialmente que

$$X^4 + Y^4 - Z^4 = Y^4 + (X - \lambda Z) \cdot B(X, Z),$$

onde $B(X, Z) = X^3 + \lambda X^2 Z + \lambda^2 X Z^2 + \lambda^3 Z^3$. Assim, para $P = (\lambda : 0 : 1)$, temos:

$$\begin{aligned}
 I(F \cdot (X - \lambda Z), P) &= I((Y^4 + X^4 - Z^4) \cdot (X - \lambda Z), P) \\
 &= I([Y^4 + (X - \lambda Z) \cdot B(X, Z)] \cdot (X - \lambda Z), P) \\
 &= I[Y^4 \cdot (X - \lambda Z)], P) \\
 &= 4 \cdot I[(Y \cdot (X - \lambda Z)], P) \\
 &= 4 \cdot I(Y \cdot Z, P) = 4 \cdot 1 = 4
 \end{aligned}$$

De forma análoga podemos verificar que se $P = (0 : \lambda : 1)$, então $I(F \cdot (Y - \lambda Z), P) = 4$ e se $P = (\rho : 1 : 0)$, então $I(F \cdot (Y - \rho X), P) = 4$.

Pelo Lema 2.10 temos que

$$\sum_{Q \in C} \{I(C \cdot T_Q, Q) - 2\} = 24,$$

o que nos garante a impossibilidade de existirem outros pontos de inflexão em C .

Agora, pelo Lema 2.6 e pelo Lema 2.9 temos que se um ponto $P \in C$ é tal que:

- (1) P não é ponto de inflexão de C , então $g(P) = 10$.
- (2) P é ponto de inflexão de C , então $g(P) = 9$.

Exemplo 2.20. *Seja C a quártica plana projetiva definida por*

$$F(X, Y, Z) = X^4 - Y^4 + X^2 Z^2 + Y^2 Z^2 + Y Z^3 = 0$$

e $P = (0 : 0 : 1)$. Então $g(P) = 8$.

Prova. Observe inicialmente que C é não singular. A parte afim de C é definida por $f(x, y) = x^4 - y^4 + x^2 + y^2 + y = 0$. Fazendo $y = tx$, temos $f(x, y) = x^4 - t^4 x^4 + x^2 + t^2 x^2 + tx$, o que nos fornece

$$\hat{f}(x, t) = \frac{1}{x} f(x, tx) = (1 - t^4)x^3 + (1 + t^2)x + t,$$

e conseqüentemente

$$\begin{aligned}\varphi_4(t) &= 1 - t^4 \\ \varphi_3(t) &= 0 \\ \varphi_2(t) &= 1 + t^2 \\ \varphi_1(t) &= t.\end{aligned}$$

Calculando o discriminante $\psi(t)$ encontramos

$$\begin{aligned}\psi(t) &= \varphi_2^2\varphi_3^2 + 18\varphi_1\varphi_2\varphi_3\varphi_4 - 4\varphi_2^3\varphi_4 - 4\varphi_1\varphi_3^3 - 27\varphi_1^2\varphi_4^2 \\ &= -4(t^2 + 1)^3(1 - t^4) - 27t^2(1 - t^4)^2 \\ &= -(t^2 + 1)^2(1 - t)(1 + t)[4(1 + t^2)^2 + 27t^2(1 - t^2)] \\ &= (t + i)^2(t - i)^2(t - 1)(t + 1)(-23t^4 + 35t^2 + 4).\end{aligned}$$

As quatro raízes distintas do polinômio $g(t) = -23t^4 + 35t^2 + 4$ são

$$\begin{aligned}\alpha_1 &= \sqrt{\frac{35 + 3\sqrt{177}}{46}} & \alpha_2 &= -\sqrt{\frac{35 + 3\sqrt{177}}{46}} \\ \alpha_3 &= i\sqrt{\frac{3\sqrt{177} - 35}{46}} & \alpha_4 &= -i\sqrt{\frac{3\sqrt{177} - 35}{46}}.\end{aligned}$$

Deste modo temos o discriminante $\psi(t)$ fatorado abaixo:

$$\psi(t) = -23(t + i)^2(t - i)^2(t - 1)(t + 1)(t - \alpha_1)(t - \alpha_2)(t - \alpha_3)(t - \alpha_4).$$

Agora, como $\psi(t)$ possui dois fatores duplos e seis fatores simples, usando o lema 2.9 temos

$$g(P) = 10 - b = 10 - 2 = 8.$$

Exemplo 2.21. *Seja C a quártica plana projetiva definida pelo polinômio*

$$F(X, Y, Z) = X(X - Y)(X + Y)(Y + 3Z) + 3YZ^3 = 0$$

e $P = (0 : 0 : 1)$. Então $g(P) = 7$.

Prova. Observe inicialmente que C é não singular. A parte afim da curva C é definida pelo polinômio

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

Fazendo $y = tx$, temos que $f(x, tx) = tx^4 - t^3x^4 + 3x^3 - 3t^2x^3 + 3tx$, o que nos fornece

$$\hat{f}(x, t) = \frac{1}{x}f(x, tx) = (t - t^3)x^3 + (3 - 3t^2)x^2 + 3t.$$

Conseqüentemente,

$$\begin{aligned}\varphi_4(t) &= t - t^3 = t(1 - t^2) \\ \varphi_3(t) &= 3 - 3t^2 = 3(1 - t^2) \\ \varphi_2(t) &= 0 \\ \varphi_1(t) &= 3t\end{aligned}$$

Assim o discriminante é dado por

$$\psi(t) = \varphi_2^2\varphi_3^2 + 18\varphi_1\varphi_2\varphi_3\varphi_4 - 4\varphi_2^3\varphi_4 - 4\varphi_1\varphi_3^3 - 27\varphi_1^2\varphi_4^2,$$

ou seja,

$$\begin{aligned}\psi(t) &= -4(3t)[3(1 - t^2)]^3 - 27(3t)^2[t(1 - t^2)]^2 \\ &= -4(3t)27(1 - t^2)^3 - 27(9t^2)t^2(1 - t^2)^2 \\ &= -81t(1 - t^2)^2[4(1 - t^2) + 3t^3] \\ &= -81t(1 - t)^2(1 + t)^2(3t^3 - 4t^2 + 4)\end{aligned}$$

Agora, calculando o discriminante tradicional de $g(t) = 3t^3 - 4t^2 + 4$ encontraremos

$$D(t) = \det \begin{bmatrix} 3 & -4 & 0 & 4 & 0 \\ 0 & 3 & -4 & 0 & 4 \\ 9 & -8 & 0 & 0 & 0 \\ 0 & 9 & -8 & 0 & 0 \\ 0 & 0 & 9 & -8 & 0 \end{bmatrix} = 8592.$$

Isto nos mostra que $g(t)$ não possui raízes múltiplas, portanto

$$g(t) = 3(t - \alpha_1)(t - \alpha_2)(t - \alpha_3),$$

com α_1 , α_2 e α_3 distintos. Este resultado nos mostra que

$$\psi(t) = -243t(t - \alpha_1)(t - \alpha_2)(t - \alpha_3)(1 - t)^2(1 + t)^2.$$

Agora, pela observação 2.8 e pelo lema 2.6 temos que Y é tangente inflexional ordinária em P e, além de Y , existem outras três tangentes inflexionais ordinárias passando por P , e três tangentes ordinárias. Isto é suficiente para concluir que $g(P) = 7$.

Exemplo 2.22. *Seja C a quártica projetiva plana definida por*

$$F(X, Y, Z) = (X^2 - 3Y^2)(XY + Y^2 + 3XZ - 3YZ + 3Z^2) + 3YZ^3 = 0$$

e $P = (0 : 0 : 1)$. Então $g(P) = 6$.

Prova. Observe inicialmente que C é não singular. A parte afim da curva C é dada por

$$f(x, y) = x^3y - 3xy^3 + x^2y^2 - 3y^4 + 3x^3 - 9xy^2 - 3x^2y + 9y^3 + 3x^2 - 9y^2 + 3y.$$

Fazendo $y = tx$ temos que

$$\begin{aligned} f(x, tx) &= tx^4 - 3t^3x^4 + t^2x^4 - 3t^4x^4 + 3x^3 - 9t^2x^3 - 3tx^3 + \\ &\quad + 9t^3x^3 + 3x^2 - 9t^2x^2 + 3tx, \end{aligned}$$

o que nos fornece

$$\begin{aligned} \hat{f}(x, t) &= \frac{1}{x}f(x, tx) = \\ &= (-3t^4 - 3t^3 + t^2 + t)x^3 + (9t^3 - 9t^2 - 3t + 3)x^2 + \\ &\quad + (-9t^2 + 3)x + 3t, \end{aligned}$$

consequentemente,

$$\begin{aligned} \varphi_4(t) &= -3t^4 - 3t^3 + t^2 + t, \\ \varphi_3(t) &= 9t^3 - 9t^2 - 3t + 3, \\ \varphi_2(t) &= -9t^2 + 3, \\ \varphi_1(t) &= 3t. \end{aligned}$$

Sendo o discriminante $\psi(t)$ dado por

$$\begin{aligned} \psi(t) &= (-9t^2 + 3)^2(9t^3 - 9t^2 - 3t + 3)^2 + \\ &\quad + 18(3t)(-9t^2 + 3)(9t^3 - 9t^2 - 3t + 3)(-3t^4 - 3t^3 + t^2 + t) - \\ &\quad - 4(-9t^2 + 3)^3(-3t^4 - 3t^3 + t^2 + t) - 4(3t)(9t^3 - 9t^2 - 3t + 3)^3 - \\ &\quad - 27(3t)^2(-3t^4 - 3t^3 + t^2 + t)^2 = \\ &= 27(3 - 22t + 17t^2 + 192t^3 - 327t^4 - 558t^5 + 1179t^6 + \dots \\ &\quad \dots + 540t^7 - 1296t^8). \end{aligned}$$

Podemos fatorar $\psi(t)$ como segue

$$\psi(t) = 27(\sqrt{3}t - 1)^2(\sqrt{3}t + 1)^2(-144t^4 + 60t^3 + 35t^2 - 22t + 3).$$

Agora, calculando o discriminante clássico de

$$g(t) = -144t^4 + 60t^3 + 35t^2 - 22t + 3,$$

encontraremos

$$D(t) = \det \begin{bmatrix} -144 & 60 & 35 & -22 & 3 & 0 & 0 \\ 0 & -144 & 60 & 35 & -22 & 3 & 0 \\ 0 & 0 & -144 & 60 & 35 & -22 & 3 \\ -576 & 180 & 70 & -22 & 0 & 0 & 0 \\ 0 & -576 & 180 & 70 & -22 & 0 & 0 \\ 0 & 0 & -576 & 180 & 70 & -22 & 0 \\ 0 & 0 & 0 & -576 & 180 & 70 & -22 \end{bmatrix} = 0.$$

Isto nos mostra que $g(t)$ possui pelo menos uma raiz múltipla. Mostraremos que $g(t)$ possui apenas uma raiz dupla.

Suponhamos, por absurdo, que $g(t)$ possua duas raízes duplas digamos, α_1 e α_2 . Então teríamos,

$$\psi(t) = 27(\sqrt{3}t - 1)^2(\sqrt{3}t + 1)^2(t - \alpha_1)^2(t - \alpha_2)^2,$$

o que nos forneceria um quadrado perfeito, e portanto, P seria um ponto de Galois. Pela observação 2.13 teríamos $I(C \cdot Y, P) = 4$, o que é uma contradição, uma vez que neste caso, $I(C \cdot Y, P) = 2$.

Concluimos então que $g(t)$ possui duas raízes simples α_1 e α_2 , e uma raiz dupla α_3 , ou seja,

$$g(t) = -144(t - \alpha_1)^2(t - \alpha_2)(t - \alpha_3).$$

Isto nos permite concluir que

$$\psi(t) = -3888(t - \alpha_1)(t - \alpha_2)(t - \alpha_3)^2(\sqrt{3}t - 1)^2(\sqrt{3}t + 1)^2.$$

Pela observação 2.8 e pelo lema 2.6 temos que X é uma tangente inflexional ordinária e, além de X , existem outras três tangentes inflexionais ordinárias passando por P . Podemos também perceber que, por P , passam duas retas tangentes ordinárias distintas de Y . Isto é suficiente para concluir que $g(P) = 6$.

Exemplo 2.23. *Seja C a curva plana projetiva definida pelo polinômio*

$$F(X, Y, Z) = YZ^3 + X^4 + Y^4 = 0$$

e $P = (0 : 0 : 1)$. Então, $g(P) = 3$.

Prova. Observe inicialmente que C é não singular. A parte afim da curva C é definida por

$$f(x, y) = y + g(x, y),$$

onde

$$\begin{aligned} g(x, y) &= x^4 + y^4 = (x^2 + iy^2)(x^2 - iy^2) = \\ &= (x + \alpha_1 y)(x - \alpha_1 y)(x + \alpha_2 y)(x - \alpha_2 y), \end{aligned}$$

com

$$\alpha_1 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \quad \text{e} \quad \alpha_2 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2},$$

portanto $g(x, y)$ não possui fator múltiplo. Agora, como $g(x, 0) = x^4 \neq 0$, pela Proposição 2.12, o ponto $P = (0, 0)$ é tal que $g(P) = 3$.

Referências Bibliográficas

- [1] Fulton, W.: Algebraic Curves: an Introduction to Algebraic Geometry, Benjamin, New York, 1969.
- [2] Garcia, A.; Lequain, Y. - Elementos de Álgebra. Projeto Euclides, IMPA, 2002.
- [3] Iitaka, S.: Algebraic Geometry, Graduate Texts in Math., Vol. 76 Springer-Verlag, New York/Heidelberg/Berlin, 1982.
- [4] Lang, S.: Algebra, Addison Wesley, New York, 1965.
- [5] Miura, K. and Yoshihara H.: Field theory for function fields of plane quartic curves, J. Algebra 226 (2000), 283-294.
- [6] Namba, M.: Geometry of Projective Algebraic Curves, Dekker, New York/Basel, 1984.
- [7] Shokurov, V. V.: Riemann Surfaces and Algebraic Curves, Vol. 23 Springer-Verlag, New York/Heidelberg/Berlin, 1988.
- [8] Stichtenoth, H.: Algebraic Function Fields and Codes. Universitext. Springer-Verlag, Berlin, 1993.
- [9] Stöhr, K.O., Voloch, J.F.: Weierstrass points and curves over finite fields. Proc. Lond. Math. Soc. 52, 1-19, 1986.
- [10] Vainsencher, I.: Introdução às Curvas Algébricas Planas, Coleção Matemática Universitária, SBM, 1996.
- [11] Watanabe, S.: The genera of Galois closure curves for plane quartic curves, Hiroshima Math. J. 38, 125-134, 2008.

Livros Grátis

(<http://www.livrosgratis.com.br>)

Milhares de Livros para Download:

[Baixar livros de Administração](#)

[Baixar livros de Agronomia](#)

[Baixar livros de Arquitetura](#)

[Baixar livros de Artes](#)

[Baixar livros de Astronomia](#)

[Baixar livros de Biologia Geral](#)

[Baixar livros de Ciência da Computação](#)

[Baixar livros de Ciência da Informação](#)

[Baixar livros de Ciência Política](#)

[Baixar livros de Ciências da Saúde](#)

[Baixar livros de Comunicação](#)

[Baixar livros do Conselho Nacional de Educação - CNE](#)

[Baixar livros de Defesa civil](#)

[Baixar livros de Direito](#)

[Baixar livros de Direitos humanos](#)

[Baixar livros de Economia](#)

[Baixar livros de Economia Doméstica](#)

[Baixar livros de Educação](#)

[Baixar livros de Educação - Trânsito](#)

[Baixar livros de Educação Física](#)

[Baixar livros de Engenharia Aeroespacial](#)

[Baixar livros de Farmácia](#)

[Baixar livros de Filosofia](#)

[Baixar livros de Física](#)

[Baixar livros de Geociências](#)

[Baixar livros de Geografia](#)

[Baixar livros de História](#)

[Baixar livros de Línguas](#)

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)