

Pontos singulares e pontos de Galois de quárticas planas singulares

Carolina Cruz Mendes Buosi
Dissertação de Mestrado em Matemática

Mestrado em Matemática
Universidade Federal do Espírito Santo

Vitória, 04 de agosto de 2011

Pontos singulares e pontos de Galois de quárticas planas singulares

Carolina Cruz Mendes Buosi

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 04 de agosto de 2011 por

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

Prof. Dr. José Gilvan de Oliveira, UFES

Profa. Dra. Miriam Abdon, UFF

Universidade Federal do Espírito Santo
Vitória, 04 de agosto de 2011

Dados Internacionais de Catalogação-na-publicação (CIP) (Biblioteca Central da Universidade Federal do Espírito Santo, ES, Brasil)	
B944p	<p>Buosi, Carolina Cruz Mendes, 1980-</p> <p>Pontos singulares e pontos de Galois de quárticas planas singulares / Carolina Cruz Mendes Buosi. – 2011. 54 f. : il.</p> <p>Orientador: Valmecir Antonio dos Santos Bayer. Dissertação (Mestrado em Matemática) Universidade Federal do Espírito Santo, Centro de Ciências Exatas.</p> <p>1. Curvas planas. 2. Galois, Teoria de. I. Bayer, Valmecir Antonio dos Santos. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.</p> <p style="text-align: right;">CDU: 51</p>

Dedicatória

Dedico este trabalho a meus filhos, que trazem leveza e alegria a minha vida.

Agradecimentos

Agradeço a Valmecir pelo privilégio de tê-lo como orientador.

A Marcelo, pelo apoio desde o primeiro dia do curso de verão até o momento da defesa. Assim mais um dos meus sonhos foi realizado ao seu lado.

Embora seja redundante, não poderia deixar de mencionar o quanto sou grata a minha mãe e meus irmãos, pela força que nossa união me dá.

E de maneira muito especial, agradeço a meus amigos pela sua presença marcante em minha vida.

Resumo

Neste trabalho estudamos curvas planas projetivas singulares de grau quatro e seus pontos de Galois. Para isto, fixamos k , um corpo algebricamente fechado de característica zero, como o corpo de base de nossa discussão. Para entender a estrutura dos corpos de funções dessas curvas, usamos projeções: escolhemos um ponto $P \in \mathbb{P}^2$ e projetamos uma curva $\mathcal{C} \subset \mathbb{P}^2$ sobre uma reta a partir de P , que é o centro da projeção. Esta projeção induz a extensão de corpos $k(\mathcal{C}) | k(\mathbb{P}^1)$, onde $k(\mathcal{C})$ é o corpo de funções racionais de \mathcal{C} . Queremos saber se existem corpos intermediários nesta extensão. Analisamos duas situações: P pertence à curva \mathcal{C} e P não pertence a \mathcal{C} .

Abstract

In this work we study singular plane projective curves of degree four and its Galois points. For this, we fix k , an algebraically closed field of characteristic zero, as the ground field of our discussion. To understand the structure of the function fields of these curves, we use projections: we choose a point $P \in \mathbb{P}^2$ and we project a curve $\mathcal{C} \subset \mathbb{P}^2$ to a line from P , that is the center of projection. This projection induces an extension field $k(\mathcal{C}) | k(\mathbb{P}^1)$, where $k(\mathcal{C})$ is the rational function field of \mathcal{C} . We want to know if there exist intermediate fields in this extension. We analyse two situations: P belongs to the curve \mathcal{C} and P doesn't belong to \mathcal{C} .

Introdução

O objetivo principal desta monografia é estudar pontos de Galois, internos e externos, de uma curva quártica plana projetiva singular sobre um corpo algebricamente fechado de característica zero. Ela é uma continuação natural das dissertações de G. S. Souza [11] e de P. M. Silva [10] sobre o mesmo assunto, no entanto, em quárticas não singulares. No caso singular, o estudo torna-se mais minucioso e exige mais ferramentas para tratar os pontos singulares.

A noção de pontos de Galois associados a uma curva projetiva plana $\mathcal{C} \subset \mathbb{P}^2$ surge quando consideramos uma projeção central de \mathcal{C} sobre uma reta $L \subset \mathbb{P}^2$ a partir de um ponto $P \notin L$, que denominamos centro de projeção. Esta projeção induz uma extensão finita de corpos, a saber, o corpo de funções racionais de L pode ser visto como um subcorpo do corpo de funções de \mathcal{C} . Este corpo de funções racionais de L na verdade não depende da escolha de L , mas depende do centro de projeções P . Assim, vamos utilizar as notações seguintes: $K = k(\mathcal{C})$ será o corpo de funções da curva \mathcal{C} e $K_P = k(L)$ será o corpo de funções da reta L .

Seguindo a nomenclatura de Yoshihara [8], o ponto P será chamado ponto de Galois associado a \mathcal{C} se a extensão de corpos $K | K_P$ for galoisiana. Além disso, no caso em que $P \notin \mathcal{C}$, diremos que ele é um ponto de Galois externo e, no caso em que $P \in \mathcal{C}$, diremos que ele é um ponto de Galois interno.

Por outro lado, se a extensão $K | K_P$ não for galoisiana (então P não é um ponto de Galois), consideramos o fecho galoisiano (fecho normal) L_P de K e estudamos a estrutura de subcorpos da extensão $L_P | K_P$.

Organizamos a dissertação da forma seguinte. No primeiro capítulo apresentamos alguns conceitos e resultados básicos sobre curvas algébricas planas afins e projetivas necessários para o desenvolvimento dos assuntos a serem tratados. Além disso, estabelecemos as principais notações. Para este capítulo a principal referência é o livro de W. Fulton [1].

No segundo capítulo apresentamos alguns resultados sobre singularidades de curvas algébricas planas com o objetivo de compreender os pontos singulares que podem ocorrer numa quártica plana. Concluimos o capítulo dando todas as possíveis singularidades de uma tal quártica destacando a sua multiplicidade e o seu número de ramos. Também apresentamos exemplos

ilustrativos em cada situação. As referências principais para este capítulo são W. Fulton [1], M. Namba [9] e A. Garcia [2].

No terceiro e último capítulo tratamos dos resultados mais importantes do trabalho. Os primeiros teoremas, que determinam os gêneros das curvas, permitem-nos calcular o gênero de qualquer quártica plana singular. Um dos principais resultados deste capítulo e também da dissertação é o Teorema 3.5 da sessão 3.2, que descreve os possíveis grupos de Galois da extensão $L_{\mathcal{P}} | K_{\mathcal{P}}$. A referência para o capítulo é o artigo de K. Miura [7].

Sumário

1	Preliminares	1
1.1	Espaços afins e conjuntos algébricos	1
1.2	Propriedades locais das curvas algébricas planas	3
1.3	Curvas algébricas planas projetivas	6
1.4	Fórmula de Riemann-Hurwitz	9
2	Singularidades de quárticas planas	11
2.1	Singularidades com um ramo	12
2.2	Singularidades com vários ramos	14
2.3	As singularidades de uma quártica plana	18
3	Pontos de Galois em quárticas singulares	23
3.1	Pontos de Galois internos	25
3.2	Pontos de Galois externos	36
3.3	O caso das quárticas de gênero dois	49
	Referências Bibliográficas	53

Capítulo 1

Preliminares

O objetivo deste capítulo é apresentar alguns conceitos e resultados básicos sobre curvas algébricas necessários para o desenvolvimento do assunto tratado na dissertação. Além disso, utilizamos o capítulo para estabelecer notações. A referência básica para isto é o livro "Algebraic Curves: An Introduction to algebraic Geometry" de W. Fulton ([1]). Estaremos admitindo que o corpo de base k é algebricamente fechado e de característica zero; por exemplo, podemos pensar em $k = \mathbb{C}$.

1.1 Espaços afins e conjuntos algébricos

Vamos denotar por $\mathbb{A}^n(k)$ o produto cartesiano $(k \times \dots \times k)$, (n vezes) que será chamado n -espaço afim sobre k . Se $F \in k[X_1, \dots, X_n]$ for um polinômio nas indeterminadas X_1, \dots, X_n sobre k , um ponto $P = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$ é um *zero* de F quando $F(P) = F(a_1, \dots, a_n) = 0$. Quando F não for constante, o conjunto dos zeros de F é chamado de *hipersuperfície* definida por F . Uma hipersuperfície em $\mathbb{A}^2(k)$ é chamada *curva algébrica plana afim*. De uma forma mais geral, se S for um conjunto qualquer de polinômios em $k[X_1, \dots, X_n]$, vamos denotar por

$$V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \forall F \in S\}$$

o conjunto dos zeros comuns dos polinômios de S . Claramente vemos que

$$V(S) = \bigcap_{F \in S} V(F).$$

Um subconjunto $X \subset \mathbb{A}^n(k)$ é um *conjunto algébrico afim*, ou simplesmente *conjunto algébrico*, quando $X = V(S)$ para algum subconjunto S de $k[X_1, \dots, X_n]$. Por outro lado, para um subconjunto qualquer X de $\mathbb{A}^n(k)$, consideremos o conjunto dos polinômios que se

anulam em X . É imediato verificar que este conjunto forma um ideal do anel $k[X_1, \dots, X_n]$, que é chamado *ideal de X* e será denotado por $I(X)$, isto é,

$$I(X) = \{F \in k[X_1, \dots, X_n] \mid F(\mathbf{a}_1, \dots, \mathbf{a}_n) = 0 \forall (\mathbf{a}_1, \dots, \mathbf{a}_n) \in X\}.$$

Se um conjunto algébrico afim for irredutível então ele é chamado uma *variedade afim*. Isto significa que ele não pode ser obtido como união de dois subconjuntos algébricos próprios.

Quando $V \subset \mathbb{A}^n$ for uma variedade afim temos que $I(V)$ é um ideal primo em $k[X_1, \dots, X_n]$. Segue que o anel quociente

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

é um domínio de integridade. Este anel é chamado *anel de coordenadas* de V . Esta nomenclatura vem do fato que $\Gamma(V)$ pode ser visto como um anel de funções de V em k , onde as classes $x_i = X_i + I(V)$ representam funções que geram este anel e, portanto, podem ser vistas como *funções coordenadas*. Podemos verificar isto da maneira seguinte. Seja $\mathcal{F}(V)$ o conjunto de todas as funções de V em k . $\mathcal{F}(V)$ tem naturalmente uma estrutura de anel com as operações usuais de soma e produto de funções (pois k é um corpo). Uma função $\varphi \in \mathcal{F}(V)$ é chamada *função polinomial* quando existe um polinômio $g \in k[X_1, \dots, X_n]$ tal que $\varphi(P) = g(P) \forall P \in V$.

Naturalmente o conjunto $\mathcal{P}(V)$ dessas funções polinomiais é um subanel de $\mathcal{F}(V)$. Além disso, pela própria definição, existe um homomorfismo sobrejetivo natural de $k[X_1, \dots, X_n]$ em $\mathcal{P}(V)$ cujo núcleo é $I(V)$. Portanto, temos que $\mathcal{P}(V) \simeq \Gamma(V)$.

Sejam $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ duas variedades afins. Uma função $\varphi : V \rightarrow W$ é chamada *aplicação polinomial* quando existem polinômios $T_1, \dots, T_m \in k[X_1, \dots, X_n]$ tais que

$$\varphi(\mathbf{a}_1, \dots, \mathbf{a}_n) = (T_1(\mathbf{a}_1, \dots, \mathbf{a}_n), \dots, T_m(\mathbf{a}_1, \dots, \mathbf{a}_n)) \forall (\mathbf{a}_1, \dots, \mathbf{a}_n) \in V.$$

Exemplo 1.1.

A aplicação

$$\begin{aligned} \varphi : \mathbb{A}^1(k) &\rightarrow V(Y^2 - X^3) \subset \mathbb{A}^2(k) \\ \mathbf{a} &\mapsto (\mathbf{a}^2, \mathbf{a}^3) \end{aligned}$$

é uma aplicação polinomial.

Observe que toda função $\varphi : V \rightarrow W$ induz um homomorfismo de anéis $\tilde{\varphi} : \mathcal{F}(W) \rightarrow \mathcal{F}(V)$, dado por $\tilde{\varphi}(f) = f \circ \varphi$. Além disso, se φ for uma aplicação polinomial $\varphi = (T_1, \dots, T_m)$, então $\tilde{\varphi}(\Gamma(W)) \subset \Gamma(V)$. Logo, $\tilde{\varphi}$ restringe-se a um homomorfismo de $\Gamma(W)$ em $\Gamma(V)$. Assim, se $f \in \Gamma(W)$ for o $I(W)$ -resíduo de um polinômio F , então $\tilde{\varphi}(f) = f \circ \varphi$ é o $I(V)$ -resíduo do

polinômio $F(T_1, \dots, T_m)$. Se $V = \mathbb{A}^n$ e $W = \mathbb{A}^m$, então $T_1, \dots, T_m \in k[X_1, \dots, X_n]$ determinam, de maneira única, uma aplicação polinomial $T : \mathbb{A}^n \rightarrow \mathbb{A}^m$, que denotamos por $T = (T_1, \dots, T_m)$.

Por outro lado, dada uma aplicação polinomial $T = (T_1, \dots, T_m)$ de \mathbb{A}^n em \mathbb{A}^m e $F \in k[X_1, \dots, X_m]$, podemos colocar $\tilde{T}(F) = F^T = F(T_1, \dots, T_m)$. As aplicações $\varphi \rightarrow \tilde{\varphi}$ e $T \rightarrow \tilde{T}$ determinam uma correspondência entre a categoria das variedades e seus morfismos e a categoria das k -álgebras finitas e seus homomorfismos.

Para ideais I de $k[X_1, \dots, X_n]$ e conjuntos algébricos V de \mathbb{A}^m , denotaremos por I^T o ideal em $k[X_1, \dots, X_n]$ gerado pelo conjunto $\{F^T \mid F \in I\}$ e por V^T o conjunto algébrico $T^{-1}(V) = V(I^T)$, onde $I = I(V)$. Se V for a hipersuperfície definida por F , então V^T é a hipersuperfície definida por F^T (no caso em que F^T não é constante).

Uma *mudança afim de coordenadas* em \mathbb{A}^n é uma aplicação polinomial

$$T = (T_1, \dots, T_n) : \mathbb{A}^n \rightarrow \mathbb{A}^n$$

tal que cada T_i é um polinômio de grau um e T é uma aplicação bijetiva. Se $T_i = \sum a_{ij}X_j + a_{i0}$, então $T = T'' \circ T'$, onde T' é uma aplicação linear ($T'_i = \sum a_{ij}X_j$) e T'' é uma translação ($T''_i = X_i + a_{i0}$). Como toda translação possui inversa (que também é uma translação), segue que T será injetiva (e sobrejetiva) se, e somente se, T' for invertível.

1.2 Propriedades locais das curvas algébricas planas

Sejam V uma variedade afim em \mathbb{A}^n e $\Gamma(V)$ o seu anel de coordenadas. Como $\Gamma(V)$ é um domínio de integridade, podemos considerar o seu corpo de frações. Este corpo é chamado o *corpo de funções racionais* de V , e é denotado por $k(V)$. Assim, um elemento de $k(V)$ é uma *função racional* sobre V . Na verdade, rigidamente falando, um elemento de $k(V)$ não é uma função, pois pode haver pontos de V onde ela pode não estar definida. No entanto, por razões de tradição, continuamos a chamar tais elementos de funções. Se f for uma tal função racional sobre V , e $P \in V$, dizemos que uma função racional f de V está definida em P se existirem $a, b \in \Gamma(V)$, tais que $f = \frac{a}{b}$ e $b(P) \neq 0$.

Seja $P \in V$. Definimos $\mathcal{O}_P(V)$ como sendo o conjunto das funções racionais sobre V que estão definidas em P . Assim, $\mathcal{O}_P(V)$ forma um subanel de $k(V)$ contendo $\Gamma(V)$. Então temos as seguintes inclusões:

$$k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V).$$

O anel $\mathcal{O}_P(V)$ é denominado *anel local* de V em P .

Um ponto $P \in V$ onde uma função racional f de V não está definida é chamado *pólo* de f . Uma função racional f de V que está definida em todos os pontos de V é chamada *função regular* em V .

Proposição 1.1. 1. O conjunto dos pólos de uma função racional sobre V é um subconjunto algébrico de V .

2. O subconjunto de $k(V)$ formado pelas funções regulares de V é exatamente o anel de coordenadas de V , a saber, $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$.

Demonstração: Veja [1], página 43. ■

Suponha que $f \in \mathcal{O}_P(V)$. Podemos definir o *valor* de f em P , isto é, $f(P)$, como se segue: existem $\mathbf{a}, \mathbf{b} \in \Gamma(V)$, com $\mathbf{b}(P) \neq 0$, tais que $f = \frac{\mathbf{a}}{\mathbf{b}}$. Então coloque $f(P) = \frac{\mathbf{a}(P)}{\mathbf{b}(P)}$. Esta definição independe das funções polinomiais \mathbf{a} e \mathbf{b} utilizadas.

Observe que $\mathcal{O}_P(V)$ é de fato um anel local no sentido da Álgebra Comutativa. Para isto, observe que $\mathcal{M}_P(V) = \{f \in \Gamma(V) \mid f(P) = 0\}$ é um ideal maximal em $\Gamma(V)$. Assim, $\mathcal{O}_P(V)$ é o anel obtido pela localização de $\Gamma(V)$ em $\mathcal{M}_P(V)$, a saber,

$$\mathcal{O}_P(V) = \Gamma(V)_{\mathcal{M}_P(V)} = \left\{ \frac{\mathbf{a}}{\mathbf{b}} \mid \mathbf{b} \notin \mathcal{M}_P(V) \right\}.$$

Vamos denotar o (único) ideal maximal de $\mathcal{O}_P(V)$ por $\mathcal{M}_P(V)$. Ele é o núcleo do homomorfismo sobrejetivo $f \rightarrow f(P)$ de $\mathcal{O}_P(V)$ sobre k ; logo $\frac{\mathcal{O}_P(V)}{\mathcal{M}_P(V)}$ é isomorfo a k . Um elemento $f \in \mathcal{O}_P(V)$ é invertível em $\mathcal{O}_P(V)$ se, e somente se, $f(P) \neq 0$. Portanto, $\mathcal{M}_P(V)$ é exatamente o conjunto dos elementos de $\mathcal{O}_P(V)$ que não têm inverso multiplicativo. Mais geralmente temos o lema seguinte.

Lema 1.1. As condições abaixo sobre um anel R são equivalentes:

1. O conjunto dos elementos não invertíveis em R forma um ideal de R .
2. R possui um único ideal maximal que contém todo ideal próprio de R .

Demonstração: Veja [1], página 44. ■

Um anel R é chamado *nöetheriano* quando todo ideal de R for finitamente gerado. O Teorema da base de Hilbert nos diz que se R for um anel nöeteriano então o anel de polinômios $R[X]$ também é nöeteriano (veja [1], página 13).

Proposição 1.2. $\mathcal{O}_P(V)$ é um domínio nöetheriano local.

Demonstração: Veja [1], página 44. ■

Proposição 1.3. *Seja R um domínio de integridade que não é corpo. Então as afirmações abaixo são equivalentes:*

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

Demonstração: Veja [1], página 46. ■

Um anel R satisfazendo as condições da Proposição 1.3 é denominado *anel de valorização discreta*. Um elemento $t \in R$ como na Proposição 1.3 item 2, é chamado um *parâmetro uniformizante local* ou simplesmente um *parâmetro local*. O parâmetro local não é único. No entanto, se $s \in R$ for outro parâmetro local então existe um elemento invertível $u \in R$ tal que $s = ut$.

Seja K o corpo das frações de R . Assim, quando o parâmetro t está fixado, todo elemento não nulo $z \in K$ possui uma expressão única $z = ut^n$, com u invertível em R e $n \in \mathbb{Z}$. O expoente n é chamado a *ordem* de z , e escrevemos $n = \text{ord}(z)$. Definimos $\text{ord}(0) = \infty$. O conjunto $\mathcal{M} = \{z \in K \mid \text{ord}(z) > 0\}$ é o ideal maximal do anel local $R = \{z \in K \mid \text{ord}(z) \geq 0\}$.

Seja \mathcal{C} uma curva algébrica plana afim. Como estamos supondo k algebricamente fechado, segue do Teorema dos Zeros de Hilbert que \mathcal{C} é definida por um polinômio (não constante) a menos de multiplicação por um fator constante não nulo. O grau de \mathcal{C} é o grau de qualquer um dos polinômios que a define. Suponha que $F \in k[X, Y]$ seja um tal polinômio. Considere a decomposição de F em fatores irredutíveis, digamos, $F = \prod F_i^{e_i}$. Dizemos que cada curva definida por F_i é uma *componente* de F e e_i é a *multiplicidade* desta componente.

Seja $P = (a, b) \in \mathcal{C}$. Dizemos que P é um *ponto simples* (ou *ponto regular*, ou ainda, *ponto não singular*) de \mathcal{C} quando

$$\frac{\partial F}{\partial X}(P) \neq 0 \text{ ou } \frac{\partial F}{\partial Y}(P) \neq 0.$$

Neste caso a reta $\frac{\partial F}{\partial X}(P)(X-a) + \frac{\partial F}{\partial Y}(P)(Y-b) = 0$ é chamada *reta tangente* a \mathcal{C} em P . Quando um ponto não é simples ele é chamado de *ponto singular*. Uma curva que possui somente pontos simples é chamada de *curva não singular*.

Suponha que $P = (0, 0)$ e escreva $F = F_m + F_{m+1} + \dots + F_n$, onde F_i é um polinômio homogêneo em $k[X, Y]$ de grau i , e $F_m \neq 0$. Definimos m como sendo a multiplicidade de \mathcal{C} em $P = (0, 0)$. Veremos mais adiante que, na verdade, esta multiplicidade não depende do sistema

de coordenadas e escrevemos $\mathfrak{m} = \mathfrak{m}_P(\mathcal{C})$. P é um ponto simples se, e somente se, $\mathfrak{m} = 1$. Se $\mathfrak{m} = 2$, então P é chamado um *ponto duplo*; se $\mathfrak{m} = 3$ ele é chamado um *ponto triplo*.

Como F_m é um polinômio homogêneo em duas variáveis, ele se fatora como um produto de fatores lineares, digamos, $F_m = \prod L_i^{r_i}$, onde as retas L_i são distintas. Neste caso estas retas são chamadas de *retas tangentes* a \mathcal{C} em $P = (0, 0)$, e cada r_i é a multiplicidade de L_i como reta tangente em P . Quando \mathcal{C} possui $\mathfrak{m} \geq 2$ tangentes (simples e distintas) em P , dizemos que P é um *ponto múltiplo ordinário* (ou *ponto singular ordinário*) de \mathcal{C} . Um ponto duplo ordinário é chamado de *nó*.

Para estender essas definições a um ponto $P \in \mathcal{C}$ qualquer, basta considerar uma mudança afim de coordenadas e mover P para a origem. (Para mais detalhes, veja [1], página 40).

O teorema seguinte caracteriza implicitamente os pontos simples de curvas algébricas.

Teorema 1.1. *Seja \mathcal{C} uma curva algébrica plana e $P \in \mathcal{C}$. Então P é um ponto simples de \mathcal{C} se, e somente se, $\mathcal{O}_P(\mathcal{C})$ for um anel de valorização discreta. Neste caso, se $L = aX + bY + c$ for uma reta não tangente a \mathcal{C} por P , então a imagem de L em $\mathcal{O}_P(\mathcal{C})$ é um parâmetro uniformizante local para $\mathcal{O}_P(\mathcal{C})$.*

Demonstração: Veja [1], página 70. ■

O teorema seguinte garante que a multiplicidade de um ponto numa curva algébrica plana é um objeto intrínseco, isto é, independe do sistema de coordenadas.

Teorema 1.2. *Seja \mathcal{C} uma curva algébrica plana irredutível e seja $P \in \mathcal{C}$. Se n for um inteiro suficientemente grande, então*

$$m_P(\mathcal{C}) = \dim_{\mathbb{K}} \frac{M_P(\mathcal{C})^n}{M_P(\mathcal{C})^{n+1}}$$

Em particular, a multiplicidade de \mathcal{C} em P depende somente do anel local $\mathcal{O}_P(\mathcal{C})$.

Demonstração: Veja [1], página 71. ■

1.3 Curvas algébricas planas projetivas

Algumas propriedades globais de curvas algébricas são melhor entendidas no contexto da geometria projetiva. Um exemplo típico disto é Teorema de Bézout, que enunciaremos em seguida. O espaço projetivo $\mathbb{P}^n(\mathbb{k})$ sobre o corpo \mathbb{k} é o conjunto de todas as retas de \mathbb{k}^{n+1} que passam pela origem. Representaremos um elemento do espaço projetivo como um ponto qualquer de uma tal reta. Assim, dois pontos de $\mathbb{k}^{n+1} - \{0\}$ representam o mesmo elemento em

$\mathbb{P}^n(k)$ quando um é obtido do outro pela multiplicação por um elemento não nulo de k . Falando de forma mais rigorosa, $\mathbb{P}^n(k)$ é o espaço quociente de $k^{n+1} - \{0\}$ pela relação de equivalência seguinte: dados $P = (x_0, x_1, \dots, x_n)$ e $Q = (y_0, y_1, \dots, y_n)$ em $k^{n+1} - \{0\}$, temos que

$$P \sim Q \Leftrightarrow Q = \lambda P, \text{ para algum } \lambda \neq 0 \text{ em } k.$$

Denotaremos um ponto de $\mathbb{P}^n(k)$ por suas coordenadas homogêneas, a saber,

$$P = (x_0 : x_1 : \dots : x_n).$$

Um *conjunto algébrico projetivo* em $\mathbb{P}^n(k)$ é o conjunto de zeros de um conjunto de polinômios homogêneos em $n + 1$ variáveis sobre k . Todos os conceitos introduzidos relativos a conjuntos algébricos afins podem ser estendidos a conjuntos algébricos projetivos. Podemos ver o espaço afim n -dimensional \mathbb{A}^n imerso em \mathbb{P}^n pela aplicação:

$$\begin{aligned} \varphi : \mathbb{A}^n &\rightarrow \mathbb{P}^n(k) \\ (x_1, x_2, \dots, x_n) &\mapsto (1 : x_1 : x_2 : \dots : x_n) \end{aligned}$$

Neste caso diremos que a imagem de $\mathbb{A}^n(k)$ por esta aplicação em $\mathbb{P}^n(k)$ são os *pontos finitos* ou *pontos afins* de $\mathbb{P}^n(k)$. O conjunto dos pontos de $\mathbb{P}^n(k)$ que têm $x_0 = 0$ são chamados *pontos do infinito*.

Uma *curva algébrica plana projetiva* é o conjunto algébrico projetivo de $\mathbb{P}^2(k)$ definida por um polinômio homogêneo não constante em três variáveis, que denotaremos neste caso por X, Y, Z . Além disso, vamos considerar os pontos do infinito de $\mathbb{P}^2(k)$ como sendo os pontos $P = (x : y : z)$ tais que $z = 0$ e os pontos finitos são tais que $z \neq 0$. Dois polinômios definem a mesma curva quando diferem apenas pela multiplicação por uma constante não nula de k . Para um tratamento sistemático dessa teoria, veja, por exemplo, [1], capítulo 5.

O *grau* de uma curva projetiva é o grau de um polinômio homogêneo que a define. Seja \mathcal{C} uma curva plana projetiva definida pelo polinômio homogêneo $F = F(X, Y, Z)$. A parte afim de \mathcal{C} é a curva algébrica afim definida pela desomogeneização de F em relação à variável Z , a saber, $F_*(X, Y) = F(X, Y, 1)$. A escolha da variável Z é completamente arbitrária.

A teoria local de uma curva projetiva é análoga à teoria local das curvas afins, tomando uma desomogeneização conveniente da equação homogênea que define a curva projetiva dada.

Seja $P \in \mathbb{P}^2$. O anel local de P é o conjunto $\mathcal{O}_P(\mathbb{P}^2)$, definido por:

$$\left\{ \frac{G}{H} \mid G, H \in k[X, Y, Z], \text{gr}(G) = \text{gr}(H), G(P) \neq 0 \right\},$$

onde G e H são homogêneos. Assim, $\mathcal{O}_P(\mathbb{P}^2)$ é um anel local e é isomorfo ao anel $\mathcal{O}_P(\mathbb{A}^2)$, onde \mathbb{A}^2 é um dos planos afins que contêm P .

Para simplificar a redação, usaremos o polinômio que define uma curva no lugar da própria curva. Sejam F, G , curvas planas projetivas e $P \in \mathbb{P}^2$. Definimos o *índice de interseção* ou *multiplicidade de interseção* de F e G no ponto P , que denotaremos por $I_P(F, G)$, por

$$I_P(F, G) = \dim_k \frac{\mathcal{O}_P(\mathbb{P}^2)}{(F_*, G_*)}.$$

Dadas duas curvas planas projetivas F e G , dizemos que elas se *intersectam propriamente* num ponto P quando F e G não possuem componente comum passando por P . Dizemos que elas se *intersectam transversalmente* em P quando P for um ponto simples de F e de G , e a reta tangente a F em P for diferente da reta tangente a G em P .

A multiplicidade de interseção satisfaz as propriedades seguintes:

1. $I_P(F, G) \in \mathbb{N}$ para quaisquer curvas projetivas F, G e um ponto $P \in \mathbb{P}^2$ tais que F e G intersectam-se propriamente em P . Além disso, $I_P(F, G) = \infty$ quando F e G não se intersectam propriamente em P .
2. $I_P(F, G) = 0$ se, e somente se, $P \notin F \cap G$. Além disso, $I_P(F, G)$ só depende das componentes F e G que passam por P .
3. Se T for uma mudança projetiva de coordenadas em \mathbb{P}^2 , e $T(Q) = P$, então

$$I_Q(F^T, G^T) = I_P(F, G).$$

4. $I_P(F, G) = I_P(G, F) \forall F, G$.
5. $I_P(F, G) \geq m_P(F) \cdot m_P(G)$. Além disso, a igualdade ocorre quando F e G não possuem tangente comum em P .
6. Se $F = \prod F_i^{r_i}$ e $G = \prod G_j^{s_j}$, então $I_P(F, G) = \sum_{i,j} r_i s_j I_P(F_i, G_j)$.
7. $I_P(F, G) = I_P(F, G + AF)$, para qualquer polinômio homogêneo A em $k[X, Y, Z]$ tal que $\text{gr}(G) = \text{gr}(A) + \text{gr}(F)$.

É possível mostrar que estas sete propriedades caracterizam completamente $I_P(F, G)$. Além disso, a definição feita anteriormente, a saber,

$$I_P(F, G) = \dim_k \frac{\mathcal{O}_P(\mathbb{P}^2)}{(F_*, G_*)},$$

satisfaz estas propriedades e é, portanto, unicamente determinado por elas. (Veja [1], página 75).

Teorema 1.3 (Teorema de Bézout). *Sejam F e G curvas planas projetivas de graus m e n , respectivamente, sem componentes comuns. Então*

$$\sum_{P \in \mathbb{P}^2} I_P(F, G) = m \cdot n.$$

Demonstração: Veja [1], página 112. ■

1.4 Fórmula de Riemann-Hurwitz

Sejam \mathcal{X} e \mathcal{Y} curvas algébricas projetivas não singulares, não necessariamente planas. Seja ainda $f : \mathcal{X} \rightarrow \mathcal{Y}$ um morfismo regular sobrejetivo. Considere o homomorfismo $\tilde{f} : k(\mathcal{Y}) \rightarrow k(\mathcal{X})$, que é naturalmente injetivo. O grau da extensão $[k(\mathcal{X}) : k(\mathcal{Y})]$ é chamado de *grau* do morfismo f e será denotado por $\text{gr}(f)$. Sejam $P \in \mathcal{X}$ e $Q = f(P) \in \mathcal{Y}$ e os seus respectivos anéis locais \mathcal{O}_P e \mathcal{O}_Q . Naturalmente estes são anéis de valorização discreta, uma vez que as curvas não são singulares. Seja $t \in \mathcal{O}_Q$ um parâmetro uniformizante. O inteiro $e_P = \text{ord}_P(t)$ é chamado *índice de ramificação* de f em P . Temos então os seguintes fatos:

Lema 1.2. *Para cada $Q \in \mathcal{Y}$ temos que $\sum_{f(P)=Q} e_P = \text{gr}(f) = [k(\mathcal{X}) : k(\mathcal{Y})]$.*

Demonstração: Veja [9], página 271. ■

Se $e_P \geq 2$, dizemos que P (respectivamente $f(P)$) é um *ponto de ramificação* (respectivamente *ponto ramificado*) de f . O conjunto de todos os pontos de ramificação (respectivamente pontos ramificados) é um conjunto finito em \mathcal{X} (respectivamente em \mathcal{Y}). Dizemos também que f é um *recobrimento ramificado*. Então

$$f : \mathcal{X} - f^{-1}(B) \rightarrow \mathcal{Y} - B$$

é um recobrimento usual (não ramificado), onde B é o conjunto de todos os pontos ramificados de f , chamado de *lugar de ramificação* de f . O teorema seguinte é um resultado clássico que nos será bastante útil.

Teorema 1.4 (Fórmula de Riemann-Hurwitz). *Sejam \mathcal{X} e \mathcal{Y} curvas algébricas projetivas não singulares, não necessariamente planas, de gêneros g_X e g_Y . Seja ainda $f : \mathcal{X} \rightarrow \mathcal{Y}$ um morfismo regular sobrejetivo. Então*

$$2g_X - 2 = \text{gr}(f)(2g_Y - 2) + \sum_{P \in \mathcal{X}} (e_P - 1).$$

Demonstração: Veja [9], página 271. ■

Capítulo 2

Singularidades de quárticas planas

Neste capítulo estamos interessados em estudar os tipos de singularidades que podem ocorrer numa quártica plana. Para isto vamos investigar sucintamente pontos singulares de curvas algébricas planas.

Seja \mathcal{C} uma curva algébrica plana irredutível e $P \in \mathcal{C}$. Após uma mudança conveniente de coordenadas podemos supor $P = (0, 0)$. Seja $f(X, Y) \in k[X, Y]$ um polinômio irredutível que define \mathcal{C} .

Sabemos que $\Gamma(\mathcal{C}) = \frac{k[X, Y]}{(f)} = k[x, y]$ é o anel de coordenadas de \mathcal{C} , onde $x = X + (f)$ e $y = Y + (f)$ e (f) denota o ideal gerado por f em $k[X, Y]$.

Como f é irredutível, $\Gamma(\mathcal{C})$ é um domínio. Seja $k(\mathcal{C})$ o corpo de funções de \mathcal{C} e vamos denotar por \mathcal{O}_P o anel local de \mathcal{C} em P . Como já observamos anteriormente, temos as inclusões:

$$k \subset \Gamma(\mathcal{C}) \subset \mathcal{O}_P \subset k(\mathcal{C}).$$

Além disso,

$$\frac{\Gamma(\mathcal{C})}{\mathcal{M}_P} \simeq k$$

onde \mathcal{M}_P é o ideal maximal de $\Gamma(\mathcal{C})$ formado pelas funções que se anulam em P .

Como já observamos anteriormente, o anel \mathcal{O}_P é um domínio nœtheriano local unidimensional. O *fecho inteiro* de \mathcal{O}_P em $k(\mathcal{C})$ é o subanel $\overline{\mathcal{O}}_P$ de $k(\mathcal{C})$ formado pelos elementos que satisfazem uma equação polinomial mônica com coeficientes em \mathcal{O}_P , isto é, $\varphi \in \overline{\mathcal{O}}_P$ se, e somente se, existirem $n \in \mathbb{N}$ e $h_0, h_1, \dots, h_{n-1} \in \mathcal{O}_P$ tais que

$$\varphi^n + h_{n-1}\varphi^{n-1} + \dots + h_1\varphi + h_0 = 0.$$

Mais geralmente, se R for um domínio, podemos definir, copiando a definição acima, o fecho inteiro de \overline{R} em seu corpo de frações. Quando $\overline{R} = R$ dizemos que R é *integralmente fechado* (em seu corpo de frações).

Exemplo 2.1. O fecho inteiro de \mathbb{Z} em \mathbb{Q} é o próprio \mathbb{Z} . Assim, \mathbb{Z} é integralmente fechado.

Seja $\alpha = \frac{p}{q}$, tal que $(p, q) = 1$ e $p, q \in \mathbb{Z}$. Queremos mostrar que se α satisfaz uma equação com coeficientes em \mathbb{Z} da forma

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

então $\alpha \in \mathbb{Z}$.

Substituindo $\alpha = \frac{p}{q}$, obtemos:

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0$$

Multiplicando por q^n , temos:

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_1pq^{n-1} + a_0q^n = 0.$$

Logo,

$$p^n = (-a_{n-1}p^{n-1} - \cdots - a_0q^{n-1})q.$$

Como $(p, q) = 1$, então $q = 1$ ou $q = -1$. Daí $\alpha = p$ ou $\alpha = -p$.

Portanto, $\alpha \in \mathbb{Z}$.

Também pode-se mostrar que esta operação de se tomar o fecho inteiro é de fato uma operação de fecho. Assim, $\overline{\mathcal{O}_P}$ é um domínio nœtheriano local, unidimensional e integralmente fechado. No caso em que seu ideal maximal é um ideal principal, segue da Proposição 1.3 que ele é um domínio de valorização discreta. Portanto, $\overline{\mathcal{O}_P} \simeq k[[t]]$, onde t é um parâmetro uniformizante local. Segue do Teorema 1.1 que P é um ponto regular em \mathcal{C} se, e somente se, $\overline{\mathcal{O}_P} = \mathcal{O}_P \simeq k[[t]]$.

2.1 Singularidades com um ramo

Para estudar melhor as singularidades de \mathcal{C} precisamos considerar o completamento de seu anel local $\mathcal{O}_P = k[[x, y]]$ (em relação à topologia \mathcal{M}_P -ádica, onde \mathcal{M}_P é o seu ideal maximal). Supondo $P = (0, 0)$, é possível verificar que este completamento é exatamente $k[[X, Y]] = \frac{k[[X, Y]]}{(f)}$, onde f é um polinômio que define \mathcal{C} (considerado como uma série). (Veja [1], página 49). $k[[X, Y]]$ é o anel das séries formais em X, Y com coeficientes em k .

Vamos denotar por \mathcal{O}_P o anel $k[[x, y]] = \frac{k[[X, Y]]}{(f)}$.

Pode-se verificar que $k[[X, Y]]$ é um anel local cujo ideal maximal é gerado por X e Y . O mesmo vale para $k[[x, y]]$; a saber, ele é um anel local cujo ideal maximal é gerado por x e y .

Segue daí que, em ambos os casos, os invertíveis são exatamente as séries de ordem zero, isto é, as séries que têm o termo constante não nulo.

O anel $k[[X, Y]]$ é um domínio de fatoração única, (veja [2]). Portanto podemos considerar a fatoração de f neste anel. Se f continuar irredutível em $k[[X, Y]]$ então \mathcal{O}_P é um domínio. Por outro lado, f pode ser redutível em $k[[X, Y]]$, digamos,

$$f = f_1 f_2 \cdots f_s,$$

onde os f_j são irredutíveis em $k[X, Y]$. É conhecido que, nesta situação, os f_j são distintos. Em outras palavras, o anel \mathcal{O}_P não possui elementos nilpotentes. Cada f_j é chamado de *ramo* de \mathcal{C} em P .

Nesta seção vamos supor que $s = 1$, isto é, \mathcal{C} tem um único ramo em P . Neste caso, \mathcal{O}_P é um domínio e podemos considerar o seu corpo de frações. Seja $\overline{\mathcal{O}}_P$ o fecho inteiro de \mathcal{O}_P em seu corpo de frações. Então $\overline{\mathcal{O}}_P$ é também um anel local. (Para mais detalhes, veja [1], capítulo 2, seção 4).

Teorema 2.1. *Se \mathcal{C} tem apenas um ramo em P então o anel $\overline{\mathcal{O}}_P$ é um anel de valorização discreta.*

Demonstração: Como $\overline{\mathcal{O}}_P$ é um domínio nöetheriano local cujo ideal maximal é principal, segue da Proposição 4, página 46 de [1], que $\overline{\mathcal{O}}_P$ é um anel de valorização discreta. ■

Seja $\nu : \overline{\mathcal{O}}_P - \{0\} \rightarrow \mathbb{N}$, a valorização discreta de $\overline{\mathcal{O}}_P$.

Definição 2.1. *O semigrupo de \mathcal{C} em P é o sub-semigrupo S_P de \mathbb{N} definido por $S_P = \nu(\overline{\mathcal{O}}_P - \{0\})$.*

O semigrupo S_P tem complementar $(\mathbb{N} - S_P)$ finito, (veja [5]). Este é chamado *conjunto das lacunas de S_P* . Se l for a maior destas lacunas, define-se o *condutor* de S_P como sendo o número natural $c_P = l + 1$. Assim, c_P é o menor elemento de S tal que, a partir dele, todos os elementos de \mathbb{N} pertencem a S_P , isto é, c_P é caracterizado pelas condições seguintes:

1. $c_P - 1 \notin S$;
2. se $n \in \mathbb{N}$ e $n > c_P$ então $n \in S$.

Este condutor (numérico) está relacionado com o ideal condutor que definiremos a seguir. Considere o conjunto

$$\mathcal{C}_P = \{\alpha \in \mathcal{O}_P \mid \alpha \cdot \overline{\mathcal{O}}_P \subset \mathcal{O}_P\}.$$

Podemos verificar que \mathcal{C}_P é um ideal de \mathcal{O}_P e também de $\overline{\mathcal{O}}_P$. Na verdade \mathcal{C}_P é maximal em \mathcal{O}_P em relação a esta propriedade.

Definição 2.2. \mathcal{C}_P é chamado ideal condutor de $\overline{\mathcal{O}}_P$ em \mathcal{O}_P .

Também pode-se verificar que \mathcal{C}_P é gerado por t_P^c em \mathcal{O}_P ou em $\overline{\mathcal{O}}_P$. Considerando $\overline{\mathcal{O}}_P \simeq k[[t]]$, podemos ver que $\mathcal{C}_P = t_P^c \cdot \overline{\mathcal{O}}_P = t^c \cdot \mathcal{O}_P$, que é o conjunto das séries de potências de ordem $\geq c_P$.

Exemplo 2.2. Seja \mathcal{C} a curva definida pela equação $f(X, Y) = Y^2 - X^3$ e $P = (0, 0)$. Então $c_P = 2$.

De fato, o semigrupo S_P neste caso é gerado por 2 e 3 em \mathbb{N} , isto é,

$$S_P = 2\mathbb{N} + 3\mathbb{N} = [2, 3] = \{2r + 3s \mid r, s \in \mathbb{N}\} = \{0, 2, 3, 4, 5, 6, \dots\}.$$

Logo, $\mathbb{N} - S_P = \{1\}$, e portanto $c_P = 2$.

O resultado seguinte faz uma ligação entre a valorização e a multiplicidade de interseção.

Teorema 2.2. Seja \mathcal{C} uma curva definida por $f \in k[X, Y]$ com um único ramo em $P \in \mathcal{C}$. Se $g \in k[[X, Y]] - fk[[X, Y]]$, escreva $\overline{g} = g + fk[[X, Y]] \in \mathcal{O}_P$. Então

$$v(\overline{g}) = I_P(g, f).$$

Demonstração: Veja [5], página 65. ■

Exemplo 2.3. Se $P = (0, 0) \in \mathcal{C}$ for um ponto regular então $S_P = \mathbb{N}$ e $c_P = 0$.

De fato, se P for regular então $m_P(\mathcal{C}) = 1$, isto é, $f = f_1 + f_2 + \dots$. Tome \mathcal{C}' tal que $m_P(\mathcal{C}') = 1$ e que tenha tangente distinta de f . Seja g o polinômio que define \mathcal{C}' . Então $1 = I_P(f, g) \in S_P$. Logo $S_P = \mathbb{N}$, e portanto, $c_P = 0$.

Exemplo 2.4. Seja \mathcal{C} uma quártica definida por $f = Y^3 - X^4$ e $P = (0, 0)$. Então

$$S_P = 3\mathbb{N} + 4\mathbb{N} = [3, 4] = \{3r + 4s \mid r, s \in \mathbb{N}\} = \{0, 3, 4, 6, 7, 8, \dots\}.$$

Logo, $\mathbb{N} - S_P = \{1, 2, 5\}$. E portanto, $c_P = 6$.

2.2 Singularidades com vários ramos

Suponhamos agora $s \geq 2$ e $P = (0, 0)$. Então \mathcal{C} possui vários ramos em P , isto é, f fatora-se no anel das séries formais $k[[X, Y]]$, em s fatores irredutíveis (distintos), digamos, $f = f_1 f_2 \cdots f_s$.

O anel $\mathcal{O}_P = \frac{k[[X, Y]]}{(f)} = \frac{k[[X, Y]]}{(f_1 \cdot f_2 \cdots f_s)}$ não é mais um domínio. No entanto ainda podemos considerar o fecho inteiro de \mathcal{O}_P em seu anel total de frações. Vamos continuar denotando este fecho inteiro por $\overline{\mathcal{O}}_P$.

Para simplificar a notação, daqui por diante, vamos abolir o índice P nos objetos.

Para cada $j = 1, 2, \dots, s$ vamos denotar, como no caso anterior, $\mathcal{O}_j = \frac{k[[X, Y]]}{(f_j)}$, que é um domínio, pois f_j é irredutível. Ainda vamos denotar por S_j o semigrupo associado a f_j , c_j o seu condutor (numérico), \mathcal{C}_j o seu ideal condutor, k_j o corpo de frações de \mathcal{O}_j e $\overline{\mathcal{O}}_j$ o fecho inteiro de \mathcal{O}_j em k_j . Cada $\overline{\mathcal{O}}_j$ é um domínio de valorização discreta, e portanto, para cada j temos que $\overline{\mathcal{O}}_j \simeq k[[t_j]]$. Seja $\nu_j : k[[t_j]] - \{0\} \rightarrow \mathbb{N}$ a valorização associada ao ramo f_j . Naturalmente o condutor de $\overline{\mathcal{O}}$ em \mathcal{O} é

$$\mathcal{C} = \{\varphi \in \overline{\mathcal{O}} \mid \varphi \cdot \overline{\mathcal{O}} \subset \mathcal{O}\}.$$

Valem os resultados seguintes para esta situação, que podem ser encontrados em [9], capítulo 2.

O anel \mathcal{O} pode ser identificado com um subanel de $\mathcal{O}_1 \times \mathcal{O}_2 \times \dots \times \mathcal{O}_s$, via o seguinte monomorfismo, que em geral, não é isomorfismo:

$$\begin{aligned} \xi : \mathcal{O} &\rightarrow \mathcal{O}_1 \times \mathcal{O}_2 \times \dots \times \mathcal{O}_s \\ g + f\mathcal{R} &\mapsto (g + f_1\mathcal{R}, g + f_2\mathcal{R}, \dots, g + f_s\mathcal{R}) \end{aligned}$$

onde estamos denotando $k[[X, Y]]$ por \mathcal{R} .

Assim, temos o seguinte diagrama, onde $\overline{\mathcal{O}}$ é o fecho inteiro de \mathcal{O} no seu anel total de frações:

$$\begin{array}{ccccc} & & \overline{\mathcal{O}}_1 & \times \dots \times & \overline{\mathcal{O}}_s \\ & & \downarrow & & \downarrow \\ \overline{\mathcal{O}} & & \mathcal{O}_1 & \times \dots \times & \mathcal{O}_s \\ \downarrow & \nearrow & & & \\ \mathcal{O} & & & & \end{array}$$

Proposição 2.1. *O anel total de frações de \mathcal{O} é naturalmente identificado com o anel total de frações de $\mathcal{O}_1 \times \mathcal{O}_2 \times \dots \times \mathcal{O}_s$, que pode ser identificado com $k_1 \times k_2 \times \dots \times k_s$.*

Demonstração: Veja [2]. ■

Temos ainda as seguintes observações, a respeito do anel $\overline{\mathcal{O}}_1 \times \overline{\mathcal{O}}_2 \times \dots \times \overline{\mathcal{O}}_s$.

1. $\overline{\mathcal{O}}_1 \times \overline{\mathcal{O}}_2 \times \dots \times \overline{\mathcal{O}}_s$ é integralmente fechado em $k_1 \times k_2 \times \dots \times k_s$.
2. $\overline{\mathcal{O}}_1 \times \overline{\mathcal{O}}_2 \times \dots \times \overline{\mathcal{O}}_s$ é uma extensão finita de $\mathcal{O}_1 \times \mathcal{O}_2 \times \dots \times \mathcal{O}_s$, já que cada extensão $[\overline{\mathcal{O}}_j : \mathcal{O}_j]$ é finita.

Para entender melhor os anéis e os ideais condutores relacionados com \mathcal{O} , é conveniente ter em mente o seguinte diagrama, onde as linhas verticais significam inclusões.

$$\begin{array}{ccccc}
 \overline{\mathcal{O}} & \xlongequal{\quad} & \overline{\mathcal{O}}_1 \times \cdots \times \overline{\mathcal{O}}_s & \xlongequal{\quad} & \overline{\mathcal{O}}_1 \times \cdots \times \overline{\mathcal{O}}_s \\
 \mathcal{C} \Big\downarrow & & \mathcal{C} \Big\downarrow & & \mathcal{C}_1 \Big\downarrow \quad \quad \quad \mathcal{C}_s \Big\downarrow \\
 \mathcal{O} & \xlongequal{\quad} & \mathcal{O}_1 \times \cdots \times \mathcal{O}_s & \xlongequal{\quad} & \mathcal{O}_1 \times \cdots \times \mathcal{O}_s \\
 & & \mathcal{C} \Big\downarrow & & \\
 & & \mathcal{O} & &
 \end{array}$$

Como é ilustrado no diagrama, \mathcal{C} é o condutor de $\overline{\mathcal{O}}$ em \mathcal{O} , $\hat{\mathcal{C}}$ é o condutor de $\mathcal{O}_1 \times \mathcal{O}_2 \times \cdots \times \mathcal{O}_s$ em \mathcal{O} , $\tilde{\mathcal{C}}$ é o condutor de $\overline{\mathcal{O}}_1 \times \overline{\mathcal{O}}_2 \times \cdots \times \overline{\mathcal{O}}_s$ em $\mathcal{O}_1 \times \mathcal{O}_2 \times \cdots \times \mathcal{O}_s$ e cada um dos \mathcal{C}_j é o condutor de $\overline{\mathcal{O}}_j$ em \mathcal{O}_j para cada $j = 1, \dots, s$. Além disso, $\overline{\mathcal{O}} \simeq \overline{\mathcal{O}}_1 \times \overline{\mathcal{O}}_2 \times \cdots \times \overline{\mathcal{O}}_s$.

Para cada $j = 1, \dots, s$ vamos usar a notação $\mathfrak{h}_j = \frac{f}{f_j}$. Podemos identificar o ideal $(\mathfrak{h}_1, \dots, \mathfrak{h}_s) \bmod (f)$ em \mathcal{O} , via inclusão de \mathcal{O} em $\mathcal{O}_1 \times \mathcal{O}_2 \times \cdots \times \mathcal{O}_s$ explicitada anteriormente, com o ideal $\mathfrak{h}_1\mathcal{O}_1 \times \mathfrak{h}_2\mathcal{O}_2 \times \cdots \times \mathfrak{h}_s\mathcal{O}_s$ em $\mathcal{O}_1 \times \mathcal{O}_2 \times \cdots \times \mathcal{O}_s$. Após identificações temos as seguintes igualdades:

1. $\hat{\mathcal{C}} = \mathfrak{h}_1\mathcal{O}_1 \times \mathfrak{h}_2\mathcal{O}_2 \times \cdots \times \mathfrak{h}_s\mathcal{O}_s$.
2. $\tilde{\mathcal{C}} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_s$.
3. $\mathcal{C} = \mathfrak{h}_1\mathcal{C}_1 \times \cdots \times \mathfrak{h}_s\mathcal{C}_s$.

Teorema 2.3 (Gorenstein). *Sejam \mathcal{O} o completamento do anel local de um ponto singular, com s ramos, de uma curva algébrica projetiva plana irreduzível, $\overline{\mathcal{O}}$ o fecho inteiro de \mathcal{O} em seu anel total de frações e \mathcal{C} o condutor de \mathcal{O} em $\overline{\mathcal{O}}$. Então*

$$\delta_{\mathcal{P}} := \dim_{\mathbf{k}} \frac{\overline{\mathcal{O}}}{\mathcal{O}} = \dim_{\mathbf{k}} \frac{\mathcal{O}}{\mathcal{C}} = \sum_{j=1}^s \frac{c_j}{2} + \frac{1}{2} \sum_{1 \leq i < j \leq s} I_{\mathcal{P}}(f_i, f_j).$$

Demonstração: Veja [4]. ■

É conveniente ter em mente o diagrama seguinte:

$$\begin{array}{c}
\overline{\mathcal{O}}_1 \times \cdots \times \overline{\mathcal{O}}_s \\
| \\
\mathcal{O}_1 \times \cdots \times \mathcal{O}_s \\
| \\
\mathcal{O} \\
| \\
\widehat{\mathcal{C}} = \mathfrak{h}_1 \mathcal{O}_1 \times \cdots \times \mathfrak{h}_s \mathcal{O}_s \\
| \\
\mathcal{C} = \mathfrak{h}_1 \mathcal{C}_1 \times \cdots \times \mathfrak{h}_s \mathcal{C}_s
\end{array}$$

O Teorema de Gorenstein nos diz que há uma simetria nas dimensões dos quocientes dados por este diagrama.

Proposição 2.2. $\delta_P \geq \frac{1}{2} m_P(\mathcal{C})(m_P(\mathcal{C}) - 1)$. A igualdade vale se, e somente se,

1. cada ramo irredutível de \mathcal{C} em P é não singular ou é uma cúspide simples (de multiplicidade m_j com $\sum_j m_j = m_P(\mathcal{C})$) e
2. as retas tangentes a estes ramos são mutuamente distintas.

Demonstração: Veja página 120 de [9]. ■

Corolário 2.1. 1. $\delta_P = 0$ se, e somente, se P for um ponto regular de \mathcal{C} .

2. $\delta_P = 1$ se, e somente, se P for uma singularidade do tipo nó duplo ou do tipo cúspide simples de multiplicidade dois.

Demonstração: 1. P é um ponto regular de \mathcal{C} se, e somente, se $m_P(\mathcal{C}) = 1$, o que é equivalente a $\delta_P = 0$.

2. Quando P for um nó ou uma cúspide simples de multiplicidade dois, $m_P(\mathcal{C}) = 2$. O resultado segue imediatamente. ■

Teorema 2.4 (Fórmula do gênero). *Sejam \mathcal{C} uma curva plana irredutível de grau d , $\varepsilon : \mathcal{X} \rightarrow \mathcal{C}$ o morfismo do modelo não-singular \mathcal{X} de \mathcal{C} em \mathcal{C} , e $g(\mathcal{X})$ o gênero de \mathcal{X} . Então*

$$g(\mathcal{X}) = \frac{(d-1)(d-2)}{2} - \sum \delta_P,$$

onde \sum estende-se sobre os pontos singulares de \mathcal{C} .

Demonstração: Veja página 126 de [9]. ■

2.3 As singularidades de uma quártica plana

Vamos agora descrever os tipos e as quantidades de singularidades que podem ocorrer numa quártica plana. Seja \mathcal{C} uma quártica projetiva plana, isto é, \mathcal{C} tem grau $d = 4$. Pela fórmula do gênero dada pelo Teorema 2.4, o gênero de \mathcal{C} (ou do modelo não singular de \mathcal{C}) satisfaz

$$g(\mathcal{C}) = 3 - \sum \delta_P,$$

onde P é ponto singular de \mathcal{C} . Portanto, $g(\mathcal{C}) \leq 3$ e vale:

$$g(\mathcal{C}) = 3 \text{ se, e somente se, } \mathcal{C} \text{ é não singular.}$$

Assim, se \mathcal{C} for uma quártica singular então $g(\mathcal{C}) \leq 2$. Além disso, segue também da fórmula do gênero que \mathcal{C} pode ter no máximo três singularidades.

Proposição 2.3. *Se \mathcal{C} é uma quártica plana e $P \in \mathcal{C}$, um ponto triplo de \mathcal{C} (isto é, $m_P(\mathcal{C}) = 3$), então P é a única singularidade de \mathcal{C} .*

Demonstração: Suponha que $Q \neq P$ seja um ponto singular de \mathcal{C} . Então $m_Q(\mathcal{C}) \geq 2$. Considere a reta l por P e Q .

Então

$$I_P(\mathcal{C}, l) \geq m_P(\mathcal{C}) \cdot m_P(l) = 3 \cdot 1 = 3$$

$$I_Q(\mathcal{C}, l) \geq m_Q(\mathcal{C}) \cdot m_Q(l) = 2 \cdot 1 = 2.$$

Logo, $\sum_{R \in \mathbb{P}^2} I_R(\mathcal{C}, l) \geq 3 + 2 = 5$.

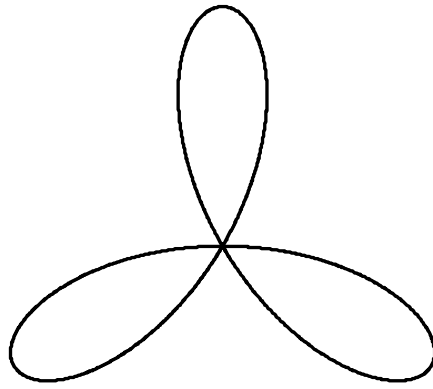
Mas pelo Teorema de Bézout, $\sum_{R \in \mathbb{P}^2} I_R(\mathcal{C}, l) = \text{gr}(\mathcal{C}) \cdot \text{gr}(l) = 4 \cdot 1 = 4$,

Chegamos assim a uma contradição. Portanto P é a única singularidade de \mathcal{C} . ■

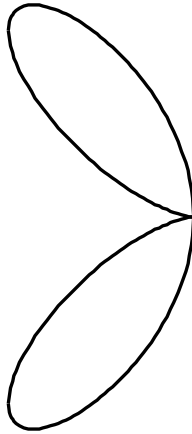
Para as quárticas planas com um ponto triplo que, neste caso, são curvas racionais, podemos enunciar o teorema seguinte:

Teorema 2.5. *Suponha que \mathcal{C} seja uma quártica plana singular com um ponto triplo P . Então uma das três situações ocorre:*

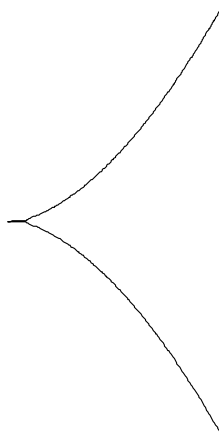
1. *Há três ramos não singulares de \mathcal{C} em P . Neste caso, as tangentes a estes ramos são mutuamente distintas e, portanto, P é uma singularidade ordinária. Eis um ponto triplo ordinário:*



2. Há dois ramos de \mathcal{C} em \mathbf{P} : um não singular e outro singular de multiplicidade dois. Neste caso, as tangentes a estes ramos são distintas e o ramo singular é uma cúspide simples de multiplicidade dois. Veja na figura:



3. Há apenas um ramo de \mathcal{C} em \mathbf{P} . Neste caso o ramo em \mathbf{P} é uma cúspide simples de multiplicidade três. O gráfico seguinte ilustra este caso:

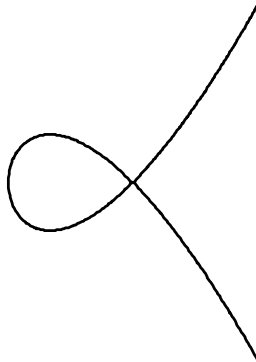


Demonstração: Para eliminar os demais casos basta aplicar o Teorema de Bézout a \mathcal{C} e às retas tangentes convenientes por \mathbf{P} . ■

Suponhamos agora que \mathcal{C} seja uma quártica plana singular que não possui ponto triplo. Então todas as singularidades de \mathcal{C} são pontos duplos. Além disso, como já observamos anteriormente, há no máximo três tais pontos. Passamos a descrever os tipos de pontos duplos que podem ocorrer em \mathcal{C} .

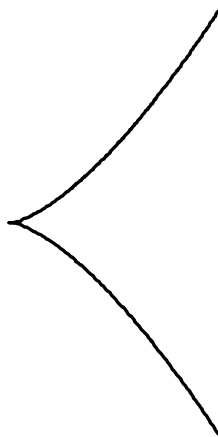
1. Nó

Um nó é um ponto duplo ordinário, isto é, uma singularidade P tal que $m_P(\mathcal{C}) = 2$ e \mathcal{C} possui dois ramos em P e duas tangentes distintas em P . Assim, $s_P = 2$. Pelo Corolário 2.1, $\delta_P = 1$. A figura seguinte exhibe um nó:



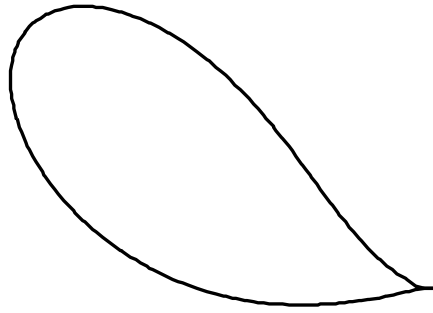
2. Cúspide simples de multiplicidade dois

Em geral, uma cúspide é uma singularidade P tal que $m_P(\mathcal{C}) \geq 2$ e há um único ramo de \mathcal{C} em P . Em particular, há apenas uma tangente a \mathcal{C} em P . No nosso caso $m_P(\mathcal{C}) = 2$ e $s_P = 1$. Pelo Corolário 2.1, $\delta_P = 1$. O gráfico abaixo ilustra uma singularidade como esta:



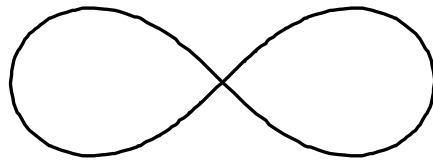
3. Tacnó

Uma tacnó é uma singularidade P de multiplicidade $m_P(\mathcal{C}) = 2$ e $\delta_P = 2$, que possui dois ramos com a mesma tangente, isto é, $s_P = 2$, e $T_P\mathcal{C}_1 = T_P\mathcal{C}_2$, onde \mathcal{C}_i são os ramos da curva \mathcal{C} e cada $T_P(\mathcal{C}_i)$ é a reta tangente a \mathcal{C}_i em P . Observe o gráfico:



4. Nó bi-inflexional

Uma singularidade P deste tipo é um nó tal que cada ramo que passa por P possui uma tangente distinta da do outro ramo. A Lemniscata de Bernoulli é um exemplo desta singularidade:



Capítulo 3

Pontos de Galois em quárticas singulares

Sejam k um corpo algebricamente fechado de característica zero, \mathcal{C} uma curva algébrica plana irredutível de grau d ($d \geq 1$) e $K = k(\mathcal{C})$ o seu corpo de funções. Seja \mathcal{C} singular, isto é, \mathcal{C} possui pelo menos um ponto singular.

Seja \mathcal{X} o modelo não singular de \mathcal{C} , que em geral não é mais uma curva plana. Assim, $K = k(\mathcal{C}) = k(\mathcal{X})$. Considere o morfismo birracional canônico $\varepsilon : \mathcal{X} \rightarrow \mathcal{C}$ tal que :

1. Se S for o conjunto dos pontos singulares de \mathcal{C} , então ε é um isomorfismo entre os abertos $\mathcal{X} - \varepsilon^{-1}(S)$ e $\mathcal{C} - S$.
2. Se $Q \in S$ então o conjunto $\varepsilon^{-1}(Q)$ é finito, digamos

$$\varepsilon^{-1}(Q) = \{\tilde{Q}_1, \tilde{Q}_2, \dots, \tilde{Q}_s\},$$

onde s é o número de ramos em Q .

Fixe um ponto $P \in \mathbb{P}^2$, que vamos considerar como centro de projeção. Considere o conjunto das retas de \mathbb{P}^2 que passam por P , que pode ser identificado com a reta projetiva \mathbb{P}^1 . O morfismo $\pi_P : \mathcal{X} \rightarrow \mathbb{P}^1$ é a aplicação racional definida por $\pi_P : \mathcal{X} \ni R \mapsto \overline{P\varepsilon(R)} \in \mathbb{P}^1$, onde $\overline{P\varepsilon(R)}$ é a reta passando por P e por $\varepsilon(R)$.

Observação 3.1. *O grau de π_P é $d - m_P$, onde $m_P(\mathcal{C})$ é a multiplicidade de P em \mathcal{C} .*

De fato, seja r uma reta qualquer de \mathbb{P}^2 passando por P . Pelo Teorema de Bézout,

$$\sum_{Q \in \mathbb{P}^2} I_Q(r, \mathcal{C}) = \text{gr}(r)\text{gr}(\mathcal{C}) = 1 \cdot d = d.$$

Isto é, uma reta qualquer $r \in \mathbb{P}^2$ por P intersecta a curva \mathcal{C} em d pontos, contando as multiplicidades. Logo, uma reta genérica de \mathbb{P}^2 intersecta \mathcal{C} em $d - m_P(\mathcal{C})$ pontos distintos.

Então temos uma extensão de corpos dada pela inclusão $\pi_P^* : k(\mathbb{P}^1) \hookrightarrow k(\mathcal{C})$, que depende apenas do centro de projeções P . Por isso denotamos o corpo de funções $k(\mathbb{P}^1)$ por K_P , isto é, $K_P = \pi_P^*(k(\mathbb{P}^1))$. Seja n o grau da extensão $K | K_P$.

Naturalmente, pelo Teorema de Lüroth (veja [13], página 107), todo corpo intermediário entre K e K_P é também um corpo racional. Estamos interessados na estrutura da extensão de corpos $K | K_P$. Mais especificamente, nas seguintes questões:

1. Quando esta extensão é galoisiana?
2. No caso em que $K | K_P$ não for galoisiana, denote por L_P seu fecho galoisiano. O que podemos dizer sobre L_P ?
3. Qual é o grupo de Galois da extensão $L_P | K_P$?
4. O que podemos dizer sobre os subcorpos intermediários da extensão K e K_P ?

Definição 3.1. *O ponto $P \in \mathbb{P}^2$ é chamado ponto de Galois associado à curva \mathcal{C} quando $K | K_P$ for uma extensão galoisiana. Além disso, quando $P \in \mathcal{C}$ ele é chamado ponto de Galois interno, e quando $P \notin \mathcal{C}$, ponto de Galois externo.*

Observe que $L_P | K_P$ é uma extensão finita e $K_P \subset K \subset L_P$. Seja $\tilde{\mathcal{C}}_P$ a curva algébrica projetiva suave (não necessariamente plana) que tem L_P como corpo de funções e considere a aplicação de recobrimento $\tilde{\pi}_P : \tilde{\mathcal{C}}_P \rightarrow \mathcal{X}$ induzida pela extensão $L_P | K$. Denotamos a composição $\pi_P \circ \tilde{\pi}_P$ por θ_P . É claro que θ_P é galoisiana, pois o corpo de funções de $\tilde{\mathcal{C}}_P$ é L_P , o fecho galoisiano de $K | K_P$.

É conveniente ter em mente o diagrama abaixo:

$$\begin{array}{ccccc}
 R \in \tilde{\mathcal{C}}_P & \xrightarrow{\quad\quad\quad} & L_P & & \\
 \searrow \tilde{\pi}_P & & \downarrow & & \\
 \theta_P \downarrow \cdots & & \mathcal{X} \ni \tilde{Q} \xrightarrow{\varepsilon} Q \in \mathcal{C} & \xrightarrow{\quad\quad\quad} & K \\
 \swarrow \pi_P & & \downarrow & & \\
 \alpha \in \mathbb{P}^1 & \xrightarrow{\quad\quad\quad} & K_P & &
 \end{array}$$

Observação 3.2. *Se o centro de projeções P for um ponto singular de uma quártica \mathcal{C} , então $n = \text{gr}(\pi_P) = 1$ ou 2 .*

Com efeito, se P for singular, então $m_P(\mathcal{C}) \geq 2$. Além disso, $gr(\pi_P) = d - m_P(\mathcal{C}) = 4 - m_P(\mathcal{C})$. Observamos então que todo ponto singular de \mathcal{C} é ponto de Galois. Ele é chamado de *ponto de Galois singular interno* associado a \mathcal{C} . Em particular, chamamos o ponto de Galois $P \in \mathbb{P}^2$ com $m_P(\mathcal{C}) = 0$ ou 1 de *ponto de Galois regular* associado a \mathcal{C} . Denotamos o número de pontos de Galois regulares associados a \mathcal{C} por $\delta(\mathcal{C})$.

Seja $\theta_P : \tilde{\mathcal{C}}_P \rightarrow \mathbb{P}^1$ o recobrimento galoisiano considerado acima. O *tipo de ramificação* de θ_P é definido como se segue.

Seja $B_{\theta_P} = m_1 Q_1 + m_2 Q_2 + \dots + m_r Q_r$, $2 \leq m_1 \leq m_2 \leq \dots \leq m_r$, o lugar de ramificação de θ_P . Aqui m_i é o índice de ramificação de θ_P em Q_i . Isto significa que, se $R \in \theta_P^{-1}(Q_i)$, então existem sistemas de coordenadas locais ξ e η em torno de R e Q_i , respectivamente, tais que $\xi(R) = 0$ e $\eta(Q_i) = 0$ e θ_P é dado localmente da seguinte forma: $\eta = \xi^{m_i}$. Dizemos então que θ_P tem tipo de ramificação (m_1, m_2, \dots, m_r) .

3.1 Pontos de Galois internos

Nesta seção vamos considerar uma quártica singular \mathcal{C} e vamos estudar o caso em que o centro de projeção é o ponto $P \in \mathcal{C}$.

Teorema 3.1. *Seja \mathcal{C} uma quártica plana projetiva. Suponha que \mathcal{C} contenha uma singularidade com multiplicidade três. Então o gênero de $\tilde{\mathcal{C}}_P$ é $g(\tilde{\mathcal{C}}_P) = 0$ ou 1 . Em outras palavras, $\tilde{\mathcal{C}}_P$ é uma curva racional ou uma curva elíptica.*

Demonstração: Sejam Q um ponto triplo de \mathcal{C} e f um polinômio que define \mathcal{C} . Após uma possível mudança de coordenadas, podemos supor $Q = (0, 0)$. Então temos três casos:

1. Q é um ponto triplo ordinário.

Segue da Proposição 2.2 que $\delta_Q = 3$. Pela Fórmula do gênero (Teorema 2.4), $g(\tilde{\mathcal{C}}_P) = 0$.

2. Q é um ponto triplo com dois ramos.

Neste caso f se fatora em $k[X, Y]$ sob a forma $f = f_1 \cdot f_2$, com f_1 regular e f_2 uma cúspide. Assim, $m_Q(f_1) = 1$, $m_Q(f_2) = 2$. Pelos Exemplos 2.2 e 2.3, $c_1 = 0$ e $c_2 = 2$.

Como f_1 e f_2 possuem tangentes distintas em Q , $I_Q(f_1, f_2) = m_Q(f_1) \cdot m_Q(f_2) = 1 \cdot 2 = 2$.

Pelo Teorema de Gorenstein, $\delta_Q = \frac{1}{2}(c_1 + c_2 + I_Q(f_1, f_2)) = \frac{1}{2}(0 + 2 + 2) = 2$.

Assim, $g(\tilde{\mathcal{C}}_P) = 3 - \delta_Q = 1$.

3. Q é uma singularidade com apenas um ramo e multiplicidade três.

Como a multiplicidade do único ramo da singularidade é três, a forma de menor grau da equação que define \mathcal{C} é de grau três. Podemos escrever $f = f_3 + f_4$.

Pelo Exemplo 2.4, $c = 6$. Segue do Teorema de Gorenstein que $\delta_Q = 3$. Logo, $\mathfrak{g}(\tilde{\mathcal{C}}_P) = 0$. ■

Vamos estudar os pontos de ramificação do morfismo $\pi_P : \mathcal{X} \rightarrow \mathbb{P}^1$ (veja o diagrama da página 22). Seguem da definição de π_P as seguintes afirmações:

Afirmção 3.1. *Se Q for um ponto suave de \mathcal{C} , então existe um único ponto $\tilde{Q} \in \mathcal{X}$ tal que $\varepsilon(\tilde{Q}) = Q$. Neste caso, o índice de ramificação de π_P em \tilde{Q} (denotado por $e_{\tilde{Q}}$) é igual ao índice de interseção entre \mathcal{C} e a reta por P e Q (em Q), a saber, $I_Q(\mathcal{C}, \overline{PQ})$. Assim, se \overline{PQ} é a reta tangente não inflexional a \mathcal{C} em Q , então $e_{\tilde{Q}} = 2$. Se Q for um ponto de inflexão de \mathcal{C} então $e_{\tilde{Q}} \geq 3$.*

Afirmção 3.2. *Se Q for um ponto singular de \mathcal{C} , denote por $s = s_Q(\mathcal{C})$ o número de ramos analíticos de \mathcal{C} em Q . Sejam $\gamma_1, \gamma_2, \dots, \gamma_s$ estes ramos e $\tilde{Q}_1, \tilde{Q}_2, \dots, \tilde{Q}_s$ os pontos correspondentes no modelo não singular \mathcal{X} . Então $\varepsilon^{-1}(Q) = \{\tilde{Q}_1, \tilde{Q}_2, \dots, \tilde{Q}_s\}$.*

Se \overline{PQ} não for a reta tangente ao ramo γ_j , então $e_{\tilde{Q}_j} = I_Q(\gamma_j, \overline{PQ}) = m_Q(\gamma_j)$.

No entanto, se \overline{PQ} for a reta tangente ao ramo γ_j , então $e_{\tilde{Q}_j} = I_Q(\gamma_j, \overline{PQ}) > m_Q(\gamma_j)$.

Observação 3.3.

Da fórmula de Riemann-Hurwitz aplicada ao morfismo $\pi_P : \mathcal{X} \rightarrow \mathbb{P}^1$, segue que

$$\sum_{R \in \mathcal{X}} (e_R - 1) + (d - m_P(\mathcal{C}))(2g(\mathbb{P}^1) - 2) = 2g(\mathcal{X}) - 2.$$

Assim,

$$\sum_{R \in \mathcal{X}} (e_R - 1) = 2g(\mathcal{X}) - 2 + 2(4 - m_P(\mathcal{C})) = 2g(\mathcal{X}) + 6 - 2m_P(\mathcal{C}).$$

Para um ponto singular $P \in \mathcal{C}$, as questões (1) a (4) são triviais. De fato, se P é singular então $m_P(\mathcal{C}) \geq 2$; logo, o grau de $K | K_P$ é $d - m_P(\mathcal{C}) \leq 4 - 2 = 2$. Como toda extensão de grau menor ou igual a dois é normal, segue que a extensão é galoisiana. Se $K \neq K_P$, então $L_P = K$, $\text{Gal}(L_P | K_P) \simeq \mathbb{Z}_2$ e não existem corpos entre K e K_P .

Então, supondo que P seja um ponto suave de \mathcal{C} , ou seja, $m_P(\mathcal{C}) = 1$, segue da Observação acima que

$$\sum_{R \in \mathcal{X}} (e_R - 1) = 2g(\mathcal{X}) + 6 - 2 \cdot 1 = 2g(\mathcal{X}) + 4.$$

Além disso, $n = \text{gr}(\pi_P) = \text{gr}(\mathcal{C}) - 1 = 4 - 1 = 3$. Isto é, o grau da extensão $K | K_P$ é três. Portanto o grau da extensão $L_P | K_P$ é no máximo seis. E o grau da extensão $L_P | K_P$ é no máximo dois.

Após uma possível mudança projetiva de coordenadas, podemos supor que:

- (i) O centro de projeção P em questão é $P = (0 : 0 : 1)$,
- (ii) $Y = 0$ é a reta tangente a \mathcal{C} em P ,
- (iii) Os pontos singulares de \mathcal{C} estão fora da reta $X = 0$,
- (iv) A reta $X = 0$ e \mathcal{C} intersectam-se somente transversalmente, isto é, sempre que $Q \in \mathcal{C} \cap (X)$, tem-se $I_Q(\mathcal{C}, X) = 1$.
- (v) se l é uma reta passando por P e por um ponto de \mathcal{C} no infinito, então l não é tangente a \mathcal{C} e não passa por pontos singulares de \mathcal{C} .

Aqui X, Y, Z são as coordenadas projetivas de \mathbb{P}^2 . Ao passar das coordenadas projetivas para as coordenadas afins, onde estamos supondo que a reta do infinito é dada por $Z = 0$, vamos usar $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$, ou seja, o plano afim é dado por $Z = 1$.

Seja $t \in k$ e considere a reta (afim) l_t dada por $y = tx$. Assim, podemos assumir que a projeção π_P , definida na parte regular de \mathcal{C} , é dada por $\pi_P(\mathcal{C} \cap l_t) = t$. No plano afim \mathbb{A}^2 com coordenadas (x, t) , seja $\hat{\mathcal{C}}$ definida pela equação (afim):

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

onde $\varphi_i(t) = f_i(1, t)$ e $f_i(x, y)$ é a parte homogênea de grau i de $f(x, y)$, ($1 \leq i \leq 4$). Assim, $K_P = k(t)$ e $K = k(x, y) = k(x, t)$, pois pela definição de $\hat{\mathcal{C}}$, temos $k(\hat{\mathcal{C}}) = k(\mathcal{C})$. Isto significa que a extensão $K | K_P$ também é obtida da equação $\hat{f}(x, t) = 0$, considerando $\hat{f}(x, t) \in k(t)[x]$. Logo, podemos estudar $\pi_P : \mathcal{X} \rightarrow \mathbb{P}^1$ considerando a projeção de $\hat{\mathcal{C}}$ no eixo t .

Observe também que, na verdade \hat{f} é a equação que fornece a explosão de \mathcal{C} na origem, isto é, $\hat{\mathcal{C}}$ nada mais é do que a explosão de \mathcal{C} em $P = (0, 0)$. Assim, quando $t = \infty$ ou $(t = (1 : 0))$, podemos considerar $x = sy$, onde $st = 1$. Logo podemos estudar o morfismo $\pi : \mathcal{X} \rightarrow \mathbb{P}^1$ considerando a projeção de $\hat{\mathcal{C}}$ no eixo t .

Podemos encontrar os pontos de ramificação de π_P usando o discriminante de $\hat{f}(x, t)$. Seja $\Psi(t)$ o discriminante de $\hat{f}(x, t) \in k[t][x]$, isto é,

$$\Psi(t) = (\varphi_4(t))^4 \prod_{i < j} (x_i - x_j)^2,$$

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

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

segundo a referência [3], capítulo 3, seção III-3.

Definição 3.2. *Seja Q um ponto não singular de \mathcal{C} e T_Q a reta tangente a \mathcal{C} em Q .*

- *Se $I_Q(\mathcal{C}, T_Q) = 3$ dizemos que $Q \in \mathcal{C}$ é um ponto de inflexão de ordem 1 de \mathcal{C} e neste caso T_Q é chamada uma tangente 1-inflexional de \mathcal{C} .*
- *De forma geral, se $I_Q(\mathcal{C}, T_Q) = r + 2$, dizemos que Q é um ponto de inflexão de ordem r de \mathcal{C} e, neste caso, T_Q é chamada uma tangente r -inflexional de \mathcal{C} .*

Observando que \hat{f} é a equação de $\hat{\mathcal{C}}$, que é a explosão de \mathcal{C} em $(0,0)$, e que $m_P(\mathcal{C}) = 1$, obtemos a seguinte relação entre os índices de interseção fornecida pela Relação de Nöether (veja [2], proposição 19, página 175): $I_P(\mathcal{C}, T_P) = I_{\hat{P}}(\hat{\mathcal{C}}, T_{\hat{P}}) + 1$, onde T_P e $T_{\hat{P}}$ são respectivamente as retas tangentes de \mathcal{C} e $\hat{\mathcal{C}}$ em P e \hat{P} .

Lema 3.1. *O discriminante $\Psi(t)$ pode ser expresso como um produto: $\Psi(t) = \Psi_0(t)\Psi_1(t)$, onde $\Psi_0(t)$ é a parte suave de $\Psi(t)$ e $\Psi_1(t)$ é a singular. Se $(t - \alpha)^{n_\alpha}$ for um fator de $\Psi_0(t)$, então $n_\alpha = 1$ ou 2 .*

Se $\alpha \neq 0$, então

1. *$n_\alpha = 2$ se, e somente, se a reta l_α for uma tangente 1-inflexional de \mathcal{C} .*
2. *$n_\alpha = 1$ se, e somente se, a reta l_α for uma tangente não inflexional de \mathcal{C} .*

Se $\alpha = 0$, então

1. *$n_\alpha = 2$ se, e somente, se a reta l_0 for uma tangente 2-inflexional de \mathcal{C} . (Isto é, P é um ponto de inflexão de ordem 2 de \mathcal{C}).*
2. *$n_\alpha = 1$ se, e somente, se a reta l_0 for uma tangente 1-inflexional de \mathcal{C} ou l_0 for uma reta bitangente.*

Demonstração: Veja [8], página 287. ■

Lema 3.2. *Se $(t - \beta)^m$ for um fator de $\Psi_1(t)$, então a reta $y = \beta x$ passa por algum ponto singular de \mathcal{C} .*

Em particular, o lema acima afirma que o discriminante $\Psi(t)$ detecta os pontos de inflexão e os pontos singulares de \mathcal{C} .

Observação 3.4.

Sabe-se que $-\varphi_4(t)\Psi(t) = \text{res}(\hat{f}, \partial\hat{f}/\partial x)$, onde $\text{res}(\hat{f}, \partial\hat{f}/\partial x)$ é a resultante de \hat{f} e $\partial\hat{f}/\partial x$, em relação a x . Se $\varphi_4(\alpha) = 0$ então a condição (v) (página 25), implica que l_α não é tangente a \mathcal{C} . Logo, α não é um ponto ramificado.

Agora suponha que $P \in \mathcal{C}$ não seja um ponto de Galois de \mathcal{C} . Isto significa que $L_P \neq K$. Segue que o grau da extensão $L_P | K$ é igual a dois, uma vez que já sabemos que no caso presente $[L_P : K_P] \leq 6$ e $[K : K_P] = 3$. Consideremos então os pontos ramificados do recobrimento duplo $\tilde{\pi}_P : \tilde{\mathcal{C}}_P \rightarrow \mathcal{X}$.

Proposição 3.1. *Sejam $\Delta(\mathcal{X}/\mathbb{P}^1)$ e $\Delta(\tilde{\mathcal{C}}_P/\mathbb{P}^1)$ os lugares de ramificação de π_P e θ_P , respectivamente. Então $\Delta(\mathcal{X}/\mathbb{P}^1) = \Delta(\tilde{\mathcal{C}}_P/\mathbb{P}^1)$.*

Demonstração: Veja Lema 1.4 de [12]. ■

Lema 3.3. *Um ponto $Q \in \mathcal{X}$ é um ponto ramificado de $\tilde{\pi}_P$ se, e somente se, as condições abaixo são satisfeitas:*

1. Se $\pi_P(Q) = \alpha$ então $\pi_P^{-1}(\alpha) = \{Q, Q'\}$.
2. π_P tem índice de ramificação um em Q , dois em Q' .

Demonstração: Seja $Q \in \mathcal{X}$ um ponto ramificado qualquer de $\tilde{\pi}_P$ e suponha que $\pi_P(Q) = \alpha$. Se a cardinalidade de $\pi_P^{-1}(\alpha)$ fosse três, Q não seria ramificado. E como estamos supondo que P não é galoisiano, a cardinalidade de $\pi_P^{-1}(\alpha)$ não pode ser um. Logo, a cardinalidade de $\pi_P^{-1}(\alpha)$ é dois, isto é, existe $\mathcal{X} \ni Q' \neq Q$ tal que $\pi_P^{-1}(\alpha) = \{Q, Q'\}$.

Segue da Proposição 3.1 que o recobrimento de Galois tem o mesmo índice de ramificação em cada ponto de ramificação. Suponha que R seja um ponto ramificado de $\tilde{\pi}_P$ tal que o índice de ramificação de π_P em R seja três. Seja $\pi_P(R) = \beta$. Então $\theta_P = \pi_P \circ \tilde{\pi}_P$ teria índice de ramificação seis em $t = \beta$. Portanto $\text{Aut}_{K_P}(L_P)$ deve conter um subgrupo cíclico de ordem seis. Como $\text{gr}(\pi_P) = [K : K_P] = 3$, segue que $\text{Gal}(L_P | K_P) \simeq S_3$. Mas S_3 não possui subgrupo cíclico de ordem seis, logo, o índice de ramificação de π_P em R não pode ser três.

Agora suponha que R' seja um ponto ramificado de $\tilde{\pi}_P$ tal que o índice de ramificação de π_P em R' seja dois. Seja $\pi_P(R') = \gamma$. Então θ_P tem índice de ramificação quatro em $t = \gamma$. Como o grau de θ_P é seis e um grupo de ordem seis não pode ter um subgrupo de ordem quatro, chegamos novamente a uma contradição.

Portanto, se $Q \in \mathcal{X}$ for um ponto ramificado de $\tilde{\pi}_P$, então o índice de ramificação de π_P em Q é um. Fixando $\alpha \in \mathbb{P}^1$, temos $\sum_{\pi_P(T)=\alpha} e_T = \text{gr}(\pi_P)$, segue que $e_Q + e_{Q'} = 3$, isto é, $1 + e_{Q'} = 3$. Logo, $e_{Q'} = 2$. A implicação recíproca é imediata. ■

Lema 3.4. *Se P não é um ponto de Galois, então $g(\tilde{C}_P) = 3g(X) + 1 - a_P$, ($0 \leq a_P \leq g(X) + 1$).*

Demonstração: Sejam a_P e b_P os números de pontos de ramificação de π_P cujos índices de ramificação sejam três e dois, respectivamente. Pelo Lema 3.3, o número de pontos ramificados de $\tilde{\pi}_P : \tilde{C}_P \rightarrow X$ é b_P . Pelo Teorema de Riemann-Hurwitz aplicado ao morfismo $\tilde{\pi}_P$, temos

$$2g(\tilde{C}_P) - 2 = (\text{gr}(\tilde{\pi}_P))(2g(X) - 2) + b_P.$$

Pela Observação 3.3, $((3-1)a_P + (2-1)b_P) = 2g(X) + 6 - 2m_P(\mathcal{C})$. Substituindo b_P na equação acima, obtemos

$$2g(\tilde{C}_P) - 2 = (\text{gr}(\tilde{\pi}_P))(2g(X) - 2) + 2g(X) + 6 - 2m_P(\mathcal{C}) - 2a_P$$

Como $m_P(\mathcal{C}) = 1$ e $\text{gr}(\tilde{\pi}_P) = 2$,

$$g(\tilde{C}_P) = 3g(X) - a_P + 1.$$

Entretanto, se $b_P = 0$, então todos os pontos de ramificação de π_P têm índice de ramificação três. Pela Proposição 3.1 de [12], π_P é cíclico. Então π_P é um recobrimento galoisiano. Contradição. Portanto, $b_P \neq 0$. Como $b_P \in \mathbb{N}$, $b_P > 0$. Como $2a_P + b_P = 2g(X) + 4$, segue que $a_P < g(X) + 2$.

Assim, $g(\tilde{C}_P) = 3g(X) + 1 - a_P$, ($0 \leq a_P \leq g(X) + 1$). ■

Teorema 3.2. *Suponha que todas as singularidades da quártica plana projetiva \mathcal{C} tenham multiplicidade igual a dois. Então o gênero de \tilde{C}_P é dado por $g(\tilde{C}_P) = g(X)$ ou $3g(X) + 1 - a_P$, ($0 \leq a_P \leq g(X) + 1$), onde P é o centro de projeção.*

Demonstração: Se P não for um ponto de Galois, basta usar o Lema 3.4. Se P for um ponto de Galois, então θ_P é cíclico. Logo, podemos concluir que $\tilde{C}_P \simeq X$; e daí $g(\tilde{C}_P) = g(X)$. ■

Observação 3.5.

Ainda de acordo com [12], $b_P = 0$ se, e somente se, $\tilde{\pi}_P$ é galoisiano, o que neste caso é equivalente a dizer que P é um ponto de Galois suave, uma vez que $m_P(\mathcal{C}) = 1$. Assim, $b_P \neq 0$ se, e somente se, $\text{Gal}(K | K_P)$ não for cíclico. Como o grau de θ_P é seis, podemos concluir que $\text{Gal}(K | K_P) \simeq S_3$ se, e somente se, $b_P \neq 0$.

Teorema 3.3. *Se \mathcal{C} tiver uma tacnó cuspidal, então \mathcal{C} não tem ponto de Galois regular.*

Demonstração: Suponha que \mathcal{C} tenha uma singularidade Q do tipo tacno cuspidal. Então $m_Q(\mathcal{C}) = 3$ e $s_Q(\mathcal{C}) = 2$. Considere $S \in \mathcal{C}$ um ponto qualquer. Como a reta \overline{SQ} não é tangente em Q , temos

$$\sum_{R \in \varepsilon^{-1}(Q)} (e_R - 1) = (2 - 1) + (1 - 1) = 1$$

Logo, Q é um ponto de ramificação de π_P com índice de ramificação dois para todo $S \in \mathcal{C}$. Portanto, $b_P \neq 0$. Pela Observação 3.5, S não é ponto de Galois suave. Como S é genérico, podemos afirmar que \mathcal{C} não possui ponto de Galois suave. ■

Lema 3.5. *Suponha que \mathcal{C} não tenha uma singularidade do tipo cuspidal simples de multiplicidade três. Então $a = 0$ para qualquer ponto $P \in \mathcal{C}$.*

Demonstração: Suponhamos que $a_P \neq 0$ para algum $P \in \mathcal{C}$. Então π_P possui algum ponto de ramificação com índice de ramificação três. Logo, existe uma reta r passando por P que intersecta \mathcal{C} em um ponto P' , tal que $I_{P'}(r, \mathcal{C}) = 3$. Ou seja, \mathcal{C} tem uma singularidade do tipo cuspidal simples de multiplicidade três. ■

Teorema 3.4. *Se P for um ponto qualquer de \mathcal{C} , então G_P é isomorfo a S_3 , o grupo simétrico de três objetos, e $g(\tilde{\mathcal{C}}_P) = 3g(\mathcal{X}) + 1$.*

Demonstração: Se P for um ponto qualquer de \mathcal{C} , então segue do Lema 3.5 que

$$g(\tilde{\mathcal{C}}_P) = 3g(\mathcal{X}) + 1.$$

Como $b \neq 0$, segue da Observação 3.5 que $G_P \simeq S_3$. ■

Observação 3.6.

Suponha que \mathcal{C} tenha um ponto triplo ordinário Q e que a reta l_α passe por P e Q . Então a reta l_α passa por Q com número de interseção três, ou seja, $I_Q(\mathcal{C}, l_\alpha) = 3$ e $\varepsilon^{-1}(Q)$ consiste em três pontos em \mathcal{X} . Logo, pela Afirmação 3.2, l_α não é tangente a \mathcal{C} . Portanto π_P não é ramificado sobre $t = \alpha$.

Exemplos

Considere a quártica projetiva plana \mathcal{C} definida pela equação afim $y + g(x, y) = 0$, onde $g(x, y)$ é um polinômio homogêneo de grau quatro e $g(x, 0) \neq 0$. Esta condição nos diz que y não é um divisor de $g(x, y)$.

Afirmação 1: $P = (0, 0)$ é um ponto de Galois suave da curva \mathcal{C} .

Prova: Escrevendo $f(x, y) = y + g(x, y)$, temos $\hat{f}(x, t) = g(1, t)x^3 + t$. Como a extensão de corpos $K | K_P$ é dada por $\hat{f}(x, t) = 0$, ou seja, $x^3 = \frac{-t}{g(1, t)}$, segue que $\text{gr}(\pi_P) = 3$. Logo, $m_P(\mathcal{C}) = 1$, isto é, $P = (0, 0)$ é ponto de Galois suave.

Homogeneizando $f(x, y)$ em relação a z , temos $F(x, y, z) = yz^3 + g(x, y)$, onde x, y, z são as coordenadas homogêneas de \mathbb{P}^2 .

Afirmção 2: Os pontos singulares de \mathcal{C} estão todos no infinito (ou seja, sobre a reta $z = 0$), e satisfazem $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y} = 0$.

Prova: Os pontos singulares de \mathcal{C} são aqueles onde $\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0$. Resolvendo, obtemos

$$\frac{\partial g}{\partial x} = z^3 + \frac{\partial g}{\partial y} = 3yz^2 = 0 \Rightarrow z = 0$$

Logo, os pontos singulares de \mathcal{C} estão sobre a reta $z = 0$. Substituindo $z = 0$ na equação acima, vemos que os pontos singulares de \mathcal{C} satisfazem $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y} = 0$.

Podemos então supor que $g(x, y)$ é um dos seguintes polinômios:

(i) $g(x, y) = (y - \alpha x)^2(y - \beta x)(y - \gamma x)$,

(ii) $g(x, y) = (y - \alpha x)^2(y - \beta x)^2$,

(iii) $g(x, y) = (y - \alpha x)^3(y - \beta x)$,

(iv) $g(x, y) = (y - \alpha x)^4$,

onde α, β, γ são elementos mutuamente distintos e diferentes de zero.

Usando a Afirmação 2, vamos encontrar os pontos singulares de \mathcal{C} em cada caso:

(i) $g(x, y) = (y - \alpha x)^2(y - \beta x)(y - \gamma x)$

$$\frac{\partial g}{\partial x} = -(y - \alpha x)(2\alpha(y - \beta x)(y - \gamma x) + \beta(y - \alpha x)(y - \gamma x) + \gamma(y - \alpha x)(y - \beta x));$$

$$\frac{\partial g}{\partial y} = (y - \alpha x)(2(y - \beta x)(y - \gamma x) + (y - \alpha x)(2y - (\beta + \gamma)x));$$

Logo, $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y} = 0 \Leftrightarrow y - \alpha x = 0$.

Portanto, o único ponto singular de \mathcal{C} é $(1 : \alpha : 0)$.

Desomogeneizando $F(x, y, z)$ em relação a x , temos

$$G_{(i)}(y, z) = yz^3 + (y - \alpha)^2(y - \beta)(y - \gamma).$$

Fazendo a mudança de coordenadas $\mathbf{u} = \mathbf{y} - \alpha$, temos

$$\begin{aligned} G_{(i)}(\mathbf{u}, z) &= (\mathbf{u} + \alpha)z^3 + \mathbf{u}^2(\mathbf{u} + \alpha - \beta)(\mathbf{u} + \alpha - \gamma) \\ &= (\alpha - \beta)(\alpha - \gamma)\mathbf{u}^2 + \alpha z^3 + (2\alpha - \beta - \gamma)\mathbf{u}^3 + \mathbf{u}z^3 + \mathbf{u}^4. \end{aligned}$$

Portanto, $(1 : \alpha : 0)$ é uma cúspide simples de multiplicidade dois.

$$(ii) \quad g(\mathbf{x}, \mathbf{y}) = (\mathbf{y} - \alpha\mathbf{x})^2(\mathbf{y} - \beta\mathbf{x})^2$$

$$\frac{\partial g}{\partial \mathbf{x}} = -2(\mathbf{y} - \alpha\mathbf{x})(\mathbf{y} - \beta\mathbf{x})(\alpha(\mathbf{y} - \beta\mathbf{x}) + \beta(\mathbf{y} - \alpha\mathbf{x}));$$

$$\frac{\partial g}{\partial \mathbf{y}} = 2(\mathbf{y} - \alpha\mathbf{x})(\mathbf{y} - \beta\mathbf{x})(2\mathbf{y} - (\alpha + \beta)\mathbf{x}).$$

Logo, $\frac{\partial g}{\partial \mathbf{x}} = \frac{\partial g}{\partial \mathbf{y}} = 0 \Leftrightarrow (\mathbf{y} - \alpha\mathbf{x})(\mathbf{y} - \beta\mathbf{x}) = 0$, isto é, $\mathbf{y} - \alpha\mathbf{x} = 0$ ou $\mathbf{y} - \beta\mathbf{x} = 0$.

Portanto, os únicos pontos singulares de \mathcal{C} são $(1 : \alpha : 0)$ e $(1 : \beta : 0)$.

Desomogeneizando $F(\mathbf{x}, \mathbf{y}, z)$ em relação a \mathbf{x} , temos

$$G_{(ii)}(\mathbf{y}, z) = \mathbf{y}z^3 + (\mathbf{y} - \alpha)^2(\mathbf{y} - \beta)^2.$$

Fazendo a mudança de coordenadas $\mathbf{u} = \mathbf{y} - \alpha$, temos

$$\begin{aligned} G_{(ii)}(\mathbf{u}, z) &= (\mathbf{u} + \alpha)z^3 + \mathbf{u}^2(\mathbf{u} + \alpha - \beta)^2 \\ &= (\alpha - \beta)^2\mathbf{u}^2 + \alpha z^3 + 2(\alpha - \beta)\mathbf{u}^3 + \mathbf{u}z^3 + \mathbf{u}^4. \end{aligned}$$

Portanto, $(1 : \alpha : 0)$ é uma cúspide simples de multiplicidade dois. Analogamente, $(1 : \beta : 0)$ também o é.

$$(iii) \quad g(\mathbf{x}, \mathbf{y}) = (\mathbf{y} - \alpha\mathbf{x})^3(\mathbf{y} - \beta\mathbf{x})$$

$$\frac{\partial g}{\partial \mathbf{x}} = -(\mathbf{y} - \alpha\mathbf{x})^2(3\alpha(\mathbf{y} - \beta\mathbf{x}) + \beta(\mathbf{y} - \alpha\mathbf{x}));$$

$$\frac{\partial g}{\partial \mathbf{y}} = (\mathbf{y} - \alpha\mathbf{x})^2(4\mathbf{y} - (\alpha + 3\beta)\mathbf{x}).$$

Logo, $\frac{\partial g}{\partial \mathbf{x}} = \frac{\partial g}{\partial \mathbf{y}} = 0 \Leftrightarrow \mathbf{y} - \alpha\mathbf{x} = 0$.

Portanto, o único ponto singular de \mathcal{C} é $(1 : \alpha : 0)$.

Desomogeneizando $F(\mathbf{x}, \mathbf{y}, z)$ em relação a \mathbf{x} , temos

$$G_{(iii)}(\mathbf{y}, z) = \mathbf{y}z^3 + (\mathbf{y} + \alpha)^3(\mathbf{y} - \beta).$$

Fazendo a mudança de coordenadas $\mathbf{u} = \mathbf{y} - \alpha$, temos

$$\begin{aligned} G_{(iii)}(\mathbf{u}, z) &= (\mathbf{u} + \alpha)z^3 + \mathbf{u}^3(\mathbf{u} + \alpha - \beta) \\ &= \alpha z^3 + (\alpha - \beta)\mathbf{u}^3 + \mathbf{u}z^3 + \mathbf{u}^4. \end{aligned}$$

Portanto, $(1 : \alpha : 0)$ é um ponto triplo ordinário.

$$(iv) \quad g(\mathbf{x}, \mathbf{y}) = (\mathbf{y} - \alpha\mathbf{x})^4$$

$$\frac{\partial g}{\partial \mathbf{x}} = -4\alpha(\mathbf{y} - \alpha\mathbf{x})^3;$$

$$\frac{\partial g}{\partial \mathbf{y}} = 4(\mathbf{y} - \alpha\mathbf{x})^3.$$

$$\text{Logo, } \frac{\partial g}{\partial \mathbf{x}} = \frac{\partial g}{\partial \mathbf{y}} = 0 \Leftrightarrow \mathbf{y} - \alpha\mathbf{x} = 0.$$

Portanto, o único ponto singular de \mathcal{C} é $(1 : \alpha : 0)$.

Desomogeneizando $F(\mathbf{x}, \mathbf{y}, z)$ em relação a \mathbf{x} , temos

$$G_{(iv)}(\mathbf{y}, z) = \mathbf{y}z^3 + (\mathbf{y} + \alpha)^4.$$

Fazendo a mudança de coordenadas $\mathbf{u} = \mathbf{y} - \alpha$, temos

$$\begin{aligned} G_{(iv)}(\mathbf{u}, z) &= (\mathbf{u} + \alpha)z^3 + \mathbf{u}^4 \\ &= \alpha z^3 + \mathbf{u}z^3 + \mathbf{u}^4. \end{aligned}$$

Portanto, $(1 : \alpha : 0)$ é uma cúspide simples de multiplicidade três.

Agora vamos descrever a ramificação de π_P .

Para o caso (i), a equação da parte afim de \mathcal{C} , ou seja, a equação de $\hat{\mathcal{C}}$, é dada por

$$\hat{f}(\mathbf{x}, \mathbf{t}) = \mathbf{t} + (\mathbf{t} - \alpha)^2(\mathbf{t} - \beta)(\mathbf{t} - \gamma)\mathbf{x}^3.$$

Assim, $\varphi_4 = (\mathbf{t} - \alpha)^2(\mathbf{t} - \beta)(\mathbf{t} - \gamma)$; $\varphi_3 = \varphi_2 = 0$ e $\varphi_1 = \mathbf{t}$.

Logo, o discriminante de $\hat{f}(\mathbf{x}, \mathbf{t})$ é dado por $\Psi(\mathbf{t}) = -27\mathbf{t}^2(\mathbf{t} - \alpha)^4(\mathbf{t} - \beta)^2(\mathbf{t} - \gamma)^2$.

Como \mathbf{t}^2 , $(\mathbf{t} - \beta)^2$ e $(\mathbf{t} - \gamma)^2$ são fatores da parte suave de $\Psi(\mathbf{t})$, segue do Lema 3.1 que o ponto $P = (0, 0)$ é um ponto de inflexão de ordem dois e $(1 : \beta : 0)$ e $(1 : \gamma : 0)$ são pontos de inflexão de ordem um. Como $(\mathbf{t} - \alpha)^4$ é um fator da parte singular de $\Psi(\mathbf{t})$, segue do Lema 3.2 que a reta $\mathbf{y} = \alpha\mathbf{x}$ passa pelo ponto $(1 : \alpha : 0)$. Observando a equação do discriminante $\Psi(\mathbf{t})$, conclui-se que o índice de ramificação de π_P em $\mathbf{t} = \beta$, $\mathbf{t} = \gamma$ e $\mathbf{t} = 0$ é três.

Agora vamos calcular o índice de ramificação de π_P em $t = \alpha$, de acordo com a Afirmação 3.2. Para isto, considere F a equação de \mathcal{C} , L a da reta tangente a \mathcal{C} em $t = \alpha$ e $Q = (1 : \alpha : 0)$.

$$\begin{aligned}
I_Q(F, L) &= I_Q(yz^3 + g(x, y), y - \alpha x) \\
&= I_Q(yz^3 + (y - \alpha x)^2(y - \beta x)(y - \gamma x), y - \alpha x) \\
&= I_Q(yz^3, y - \alpha x) \\
&= I_Q(y, y - \alpha x) + I_Q(z^3, y - \alpha x) \\
&= 0 + 3 \cdot I_Q(z, y - \alpha x) = 3 \cdot 1 = 3.
\end{aligned}$$

Portanto, o tipo de ramificação de π_P é $(3, 3, 3, 3)$.

No caso (ii), a equação da parte afim de \mathcal{C} é dada por $\hat{f}(x, t) = t + (t - \alpha)^2(t - \beta)^2x^3$.

Assim, $\varphi_4 = (t - \alpha)^2(t - \beta)^2$; $\varphi_3 = \varphi_2 = 0$ e $\varphi_1 = t$. Logo, $\Psi(t) = -27t^2(t - \alpha)^4(t - \beta)^4$. Pelo lema 3.1, o ponto $P = (0, 0)$ é de inflexão de ordem dois. Basta olhar a equação de $\Psi(t)$ para concluir que o índice de ramificação de π_P em $t = 0$ é três.

Analogamente ao caso (i), o índice de ramificação de π_P em $t = \alpha$ e em $t = \beta$ é três.

Portanto, o tipo de ramificação de π_P é $(3, 3, 3)$.

Em particular, nos casos (i) e (ii), não há outros pontos suaves de Galois. De fato, dados qualquer outro ponto $Q \in \mathcal{C}$, tal que ($Q \neq P$) e uma reta l_λ passando por Q e $(1 : \alpha : 0)$, vemos que l_λ encontra \mathcal{C} em $(1 : \alpha : 0)$ com número de interseção dois, isto é, $I_{(1:\alpha:0)}(\mathcal{C}, l_\lambda) = 2$, pois $m_{(1:\alpha:0)} = 2$. Pelo Teorema de Bézout, existe apenas mais um ponto, digamos Q' , em $\mathcal{C} \cap l_\lambda$. E l_λ intersecta \mathcal{C} transversalmente em Q' . Então $\pi_Q^{-1}(\lambda) = \{(1 : \alpha : 0), Q'\}$, ou seja, Q é um ponto duplo. Pela Observação 3.5, Q não é ponto de Galois.

No caso (iii), a equação de $\hat{\mathcal{C}}$ é dada por $\hat{f}(x, y) = t + (t - \alpha)^3(t - \beta)x^3$.

Então $\varphi_4 = (y - \alpha)^3(t - \beta)$; $\varphi_3 = \varphi_2 = 0$ e $\varphi_1 = t$.

Assim, $\Psi(t) = -27t^2(t - \alpha)^6(t - \beta)^2$. Pelo Lema 3.1, o ponto P é um ponto de inflexão de ordem dois e o ponto $(1 : \beta : 0)$ é um ponto de inflexão de ordem um. O índice de ramificação de π_P em $t = 0$ é três. Analogamente ao item (i), o índice de ramificação de π_P em $t = \alpha$ é três. Portanto, o tipo de ramificação de π_P é $(3, 3)$.

Definição 3.3. Denotamos por $W(\mathcal{C})$ a quantidade de pontos de inflexão de uma curva plana projetiva \mathcal{C} , contando as multiplicidades. Este número pode ser calculado da seguinte maneira:

$W(\mathcal{C}) := \sum_{Q \in \mathcal{C}} \{I_Q(\mathcal{C}, T_Q) - 2\}$, onde T_Q é a reta tangente a \mathcal{C} em Q .

No caso (iv), $\hat{f}(x, y) = t + (t - \alpha)^4x^3$.

Logo, $\varphi_4 = (t - \alpha)^4$; $\varphi_3 = \varphi_2 = 0$ e $\varphi_1 = t$. Então $\Psi(t) = -27t^2(t - \alpha)^8$. Pelo lema 3.1, P é um ponto de inflexão de ordem dois. O índice de ramificação de π_P em $t = 0$ é três.

Analogamente ao item (i), o índice de ramificação de π_P em $t = \alpha$ é três. Portanto, o tipo de ramificação de π_P é $(3, 3)$.

A quantidade de pontos de inflexão de \mathcal{C} é dada por

$$W(\mathcal{C}) = I_P(\mathcal{C}, T_P) - 2 = 4 - 2 = 2.$$

Como $P = (0, 0)$ é um ponto de inflexão de ordem dois, não há mais pontos de inflexão. Para cada ponto P de Galois de \mathcal{C} , temos $2 = W(\mathcal{C}) = \delta(\mathcal{C})(I_P(\mathcal{C}, Y) - 2) = 2\delta(\mathcal{C})$. Portanto, $\delta(\mathcal{C}) = 1$, isto é, P é o único ponto de Galois suave de \mathcal{C} .

Portanto, $\delta(\mathcal{C}) = 1$ nos casos (i), (ii) e (iv).

3.2 Pontos de Galois externos

Nesta seção vamos considerar uma quártica singular \mathcal{C} e vamos estudar o caso em que o centro de projeção é o ponto $P \notin \mathcal{C}$.

Denotaremos por G_P o grupo de Galois $\text{Gal}(L_P | K_P)$.

Teorema 3.5. *Sejam \mathcal{C} uma curva quártica plana qualquer e $P \in \mathbb{P}^2$, o centro de projeção. Então G_P é isomorfo a um dos seguintes grupos:*

1. O grupo simétrico de quatro letras, S_4 ;
2. O subgrupo A_4 de S_4 das permutações pares;
3. O grupo diedral D_4 de ordem oito;
4. O grupo cíclico \mathbb{Z}_4 de ordem quatro;
5. O grupo V_4 de Klein.

Além disso, se \mathcal{C} não tem cúspide simples de multiplicidade três, então $G_P \simeq S_4$ e

$$g(\tilde{\mathcal{C}}_P) = 12g(\mathcal{X}) + 13.$$

Demonstração: Fazendo uma mudança projetiva de coordenadas, se necessário, podemos supor que:

1. $P = (0, 0) \notin \mathcal{C}$;
2. os pontos singulares de \mathcal{C} não estão sobre a reta $X = 0$.
3. a curva \mathcal{C} intercecta o eixo $X = 0$ transversalmente.

Para cada $t \in k$ considere a reta afim $l_t : y = tx$. Podemos então supor que a projeção π_P está sendo feita sobre \mathbb{A}^1 e é definida por $\pi_P(\mathcal{C} \cap l_t) = t$.

No plano afim $(x, t) \in \mathbb{A}^2$, seja $\check{\mathcal{C}}$ a curva definida por

$$\check{f}(x, t) = f(x, tx) = \varphi_4(t)x^4 + \varphi_3(t)x^3 + \varphi_2(t)x^2 + \varphi_1(t)x + c,$$

onde $\varphi_i(t) = f_i(1, t)$, $(1 \leq i \leq 4)$ e $c \in k - \{0\}$. Então $K = k(x, t)$, $K_P = k(t)$ e a extensão $K | K_P$ é obtida através de $\check{f}(x, t) = 0$.

Lema 3.6. *Suponha que \mathcal{C} não tenha cúspide simples de multiplicidade três. Se P for um ponto qualquer, então π_P tem $2g(\mathcal{X}) + 6$ pontos de ramificação, e seus índices de ramificação são dois.*

Demonstração: Seja P um ponto qualquer e l uma reta passando por P . Então vale uma das seguintes afirmações:

1. A reta l intersecta a curva \mathcal{C} transversalmente em todos os pontos de interseção, isto é, se Q for um ponto de interseção entre l e \mathcal{C} , então $I_Q(l, \mathcal{C}) = 1$.
2. A reta l tangencia \mathcal{C} em um ponto Q_1 , tal que $I_{Q_1}(l, \mathcal{C}) = 2$ e intersecta \mathcal{C} transversalmente nos outros pontos.
3. A reta l não é tangente a \mathcal{C} em pontos singulares.

Pelo Lema 2 de [11], página 39, o discriminante $\Psi(t)$ possui apenas fatores simples. Logo, os índices de ramificação dos pontos de ramificação são dois.

Aplicando a fórmula de Riemann-Hurwitz para $\pi_P : \mathcal{X} \rightarrow \mathbb{P}^1$, temos

$$2g(\mathcal{X}) - 2 = \text{gr}(\pi_P)(2g(l) - 2) + \sum_{P \in \mathcal{X}} (e_P - 1).$$

Como l é uma reta, $g(l) = 0$ e como $P \notin \mathcal{C}$, $\text{gr}(\pi_P) = 4$.

Substituindo esses valores na fórmula obtemos que o número de pontos de ramificação de π_P é $2g(\mathcal{X}) + 6$. ■

Considere $\theta_P : \tilde{\mathcal{C}}_P \rightarrow \mathbb{P}^1$ o recobrimento de Galois. Se $R \in \tilde{\mathcal{C}}_P$ for um ponto de ramificação, então podemos concluir pelo Lema 3.6 que o índice de ramificação de θ_P em R é dois. Como θ_P não é ramificado em $t = \infty$ e o grupo inercial no ponto de ramificação é gerado por uma transposição, segue das Proposições 1 e 2 de [11], página 24, que $G_P \simeq S_4$.

Como $[L_P : K_P] = \text{gr}(\theta_P) = 24$ e $[K(\mathcal{C}) : K_P] = \text{gr}(\pi_P) = 4$, segue que $[L_P : K(\mathcal{C})] = 6$. Então, pelo Lema 3.6, o número de pontos de ramificação com índice de ramificação dois é igual a $2[L_P : K(\mathcal{C})](2g(\mathcal{X}) + 6)$. Usando agora a fórmula de Riemann-Hurwitz para θ_P , obtemos:

$$2g(\tilde{\mathcal{C}}_P) - 2 = [\tilde{\mathcal{C}}_P : \mathbb{P}^1](2 \cdot 0 - 2) + 2 \cdot [L_P : K(\mathcal{C})] \cdot (2g(\mathcal{X}) + 6).$$

Substituindo os valores encontrados, temos

$$2\mathfrak{g}(\tilde{\mathcal{C}}_P) - 2 = 24(-2) + 2 \cdot 6 \cdot (2\mathfrak{g}(\mathcal{X}) + 6).$$

Resolvendo, chegamos à expressão $\mathfrak{g}(\tilde{\mathcal{C}}_P) = 12\mathfrak{g}(\mathcal{X}) + 13$.

Segundo o artigo [6], página 134, definimos a cúbica resolvente $\tilde{\mathfrak{g}}(z)$ de $\check{f}(x, t) = 0$:

$$\tilde{\mathfrak{g}}(z) = z^3 - \frac{\varphi_2}{\varphi_4}z^2 + \frac{\varphi_1\varphi_3 - 4c\varphi_4}{\varphi_4^2}z + \frac{4c\varphi_2\varphi_4 - c\varphi_3^2 - \varphi_1^2\varphi_4}{\varphi_4^3},$$

onde $\varphi_i(t)$, ($1 \leq i \leq 4$).

Segue de [6], página 134, que as expressões das raízes de $\tilde{\mathfrak{g}}(z)$ são dadas por:

$$t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad t_2 = \alpha_1\alpha - 3 + \alpha_2\alpha_4 \quad \text{e} \quad t_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3,$$

onde os α_i 's geram L_P sobre K . Logo, o corpo de fatoração de $\tilde{\mathfrak{g}}(z)$ está contido em L_P . Assim, claramente, $\tilde{\mathfrak{g}}(z) \in k(t)[z]$. Seja M o corpo de fatoração de $\tilde{\mathfrak{g}}(z) = 0$ sobre $k(t)$. Aplicando o Teorema 1 de [6], obtemos:

1. $G_P \simeq S_4 \Leftrightarrow \tilde{\mathfrak{g}}(z)$ é irredutível sobre $k(t)$ e $\sqrt{\Psi(t)} \notin k(t)$.
2. $G_P \simeq A_4 \Leftrightarrow \tilde{\mathfrak{g}}(z)$ é irredutível sobre $k(t)$ e $\sqrt{\Psi(t)} \in k(t)$.
3. $G_P \simeq V_4 \Leftrightarrow \tilde{\mathfrak{g}}(z)$ decompõe-se em fatores lineares sobre $k(t)$.
4. $G_P \simeq \mathbb{Z}_4 \Leftrightarrow \tilde{\mathfrak{g}}(z)$ possui exatamente uma raiz α em $k(t)$ e

$$h(x) := \left(x^2 - \alpha x + \frac{c}{\varphi_4}\right) \left(x^2 + \frac{\varphi_3}{\varphi_4}x + \frac{\varphi_2}{\varphi_4} - \alpha\right)$$

fatora-se sobre M .

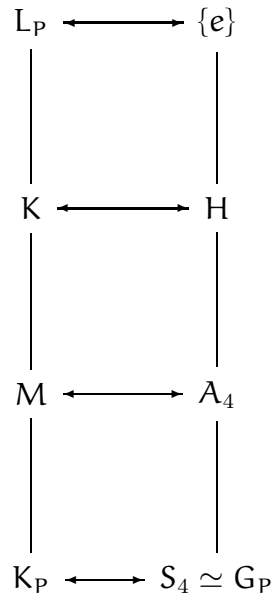
5. $G_P \simeq D_4 \Leftrightarrow \tilde{\mathfrak{g}}(z)$ possui exatamente uma raiz α em $k(t)$ e $h(x)$ não se fatora em M .

■

Corolário 3.1. *Se $P \in \mathbb{P}^2$ for um ponto qualquer, então não existe corpo intermediário entre K e K_P .*

Demonstração: Se \mathcal{C} tiver cúspide simples de multiplicidade três, então seu gênero é zero, e o caso é trivial. Se não tiver, segue do Teorema 3.5 que G_P é isomorfo a S_4 . Suponhamos que exista um corpo intermediário entre K e K_P , digamos, M . Como a extensão $K | K_P$ tem grau

quatro, as extensões $M | K_p$ e $K | M$ teriam grau dois. Como o único subgrupo de S_4 de ordem doze é A_4 , teríamos o seguinte diagrama da correspondência de Galois:



Logo, o índice do subgrupo H em A_4 seria dois. Mas A_4 não possui subgrupo de ordem seis. Portanto, não existe corpo intermediário entre K e K_p . ■

Agora vamos caracterizar as equações que definem uma curva \mathcal{C} através da estrutura de G_p . Mas antes disso, precisamos enunciar alguns resultados da teoria de corpos.

Resultado 3.1. *Se G_p for isomorfo a A_4 , então não existe corpo intermediário entre K e K_p .*

Para justificar esse resultado, basta usar o mesmo argumento da demonstração do Corolário 3.1.

Nos casos em que $G_p \simeq V_4, \mathbb{Z}_4$ ou D_4 , pode-se encontrar subcorpos entre K e K_p considerando os subgrupos de G_p .

Lema 3.7. *As afirmações abaixo são equivalentes:*

1. K contém um corpo intermediário K' com $[K' : K_p] = 2$.
2. K é expresso como $K = K_p(\xi)$, onde ξ é raiz de um polinômio irredutível $X^4 + aX^2 + b \in K_p[x]$.

Demonstração: Veja [11], página 43. ■

Proposição 3.2. *O grupo G_p é isomorfo a V_4, \mathbb{Z}_4 ou D_4 se, e somente se, uma equação que define \mathcal{C} puder ser escrita como*

$$f(x, y) = f_4(x, y) + f_2(x, y) = c,$$

sendo $f_4(x, y)$ e $f_2(x, y)$ polinômios homogêneos de graus quatro e dois, respectivamente, e $c \in k - \{0\}$.

Demonstração: Veja [8], página 292. ■

Observação 3.7.

No caso da Proposição 3.2, temos $\check{f}(x, t) = \varphi_4(t)x^4 + \varphi_2(t)x^2 + c$. Logo,

$$\tilde{g}(z) = z^3 - \frac{\varphi_2}{\varphi_4}z^2 - \frac{4c}{\varphi_4}z + \frac{4c\varphi_2}{\varphi_4^2} = \left(z - \frac{\varphi_2}{\varphi_4}\right) \left(z^2 - \frac{4c}{\varphi_4}\right).$$

E aplicando o Teorema 1 de [6], página 134, obtemos o seguinte:

1. $G_P \simeq V_4 \Leftrightarrow \sqrt{\frac{c}{\varphi_4}} \in k(t)$;
2. $G_P \simeq Z_4 \Leftrightarrow \sqrt{\frac{c}{\varphi_4} \left(\frac{\varphi_2^2}{\varphi_4^2} - \frac{4c}{\varphi_4}\right)} \in k(t)$;
3. $G_P \simeq D_4 \Leftrightarrow$ os dois casos anteriores não acontecem.

Observação 3.8. *Toda curva plana projetiva redutível tem um ponto singular.*

Demonstração: Sejam \mathcal{C} uma curva plana projetiva redutível e F um polinômio que a define.

Então podemos escrever

$$F = F_1 \cdot F_2,$$

onde F_1 e F_2 são os fatores de F .

Pelo Teorema de Bézout, $F_1 \cap F_2 \neq \emptyset$, isto é, existe $P \in F_1 \cap F_2$.

Seja l uma reta que passa por P . Assim,

$$\begin{aligned} I_P(F, l) &= I_P(F_1 \cdot F_2, l) \\ &= I_P(F_1, l) + I_P(F_2, l) \geq 1 + 1 = 2. \end{aligned}$$

Portanto P é ponto singular de \mathcal{C} . ■

Exemplos

Exemplo 3.1. *Sejam \mathcal{C} a curva definida por $f(x, y) = x^4 - 2x^2y^2 + y^4 + x^2 + y^2 + 1 = 0$ e $P = (0, 0)$. Então $G_P \simeq V_4$ e $g(\mathcal{X}) = 1$.*

De fato, temos:

$$\check{f}(x, t) = f(x, tx) = (t^4 - 2t^2 + 1)x^4 + (t^2 + 1)x^2 + 1;$$

Como $\sqrt{\frac{1}{t^4 - 2t^2 + 1}} = \frac{1}{t^2 - 1} \in k(t)$, segue da Observação 3.7 que $G_P \simeq V_4$. Além disso, temos

$$\begin{aligned}\tilde{g}(z) &= \left(z - \frac{t^2 + 1}{t^4 - 2t^2 + 1}\right) \left(z^2 - \frac{4}{t^4 - 2t^2 + 1}\right) \\ &= \left(z - \frac{t^2 + 1}{(t^2 - 1)^2}\right) \left(z - \frac{2}{t^2 - 1}\right) \left(z + \frac{2}{t^2 - 1}\right);\end{aligned}$$

Para obter $\Psi(t)$, precisamos calcular a resultante entre $\check{f}(x, t)$ e $\frac{\partial \check{f}}{\partial x}$, que, segundo a referência [3], página 75, é dada pelo determinante da matriz $D(t)$:

$$\begin{bmatrix} \varphi_4(t) & \varphi_3(t) & \varphi_2(t) & \varphi_1(t) & c & 0 & 0 \\ 0 & \varphi_4(t) & \varphi_3(t) & \varphi_2(t) & \varphi_1(t) & c & 0 \\ 0 & 0 & \varphi_4(t) & \varphi_3(t) & \varphi_2(t) & \varphi_1(t) & c \\ 4\varphi_4(t) & 3\varphi_3(t) & 2\varphi_2(t) & \varphi_1(t) & 0 & 0 & 0 \\ 0 & 4\varphi_4(t) & 3\varphi_3(t) & 2\varphi_2(t) & \varphi_1(t) & 0 & 0 \\ 0 & 0 & 4\varphi_4(t) & 3\varphi_3(t) & 2\varphi_2(t) & \varphi_1(t) & 0 \\ 0 & 0 & 0 & 4\varphi_4(t) & 3\varphi_3(t) & 2\varphi_2(t) & \varphi_1(t) \end{bmatrix}.$$

Calculando-o, obtemos

$$\begin{aligned}\det D(t) &= \\ &- \varphi_4(t)(4\varphi_1(t)^2\varphi_2(t)^3\varphi_4(t) + 128c^2\varphi_2(t)^2\varphi_4(t)^2 + 27\varphi_1(t)^4\varphi_4(t)^2 + 4\varphi_1(t)^3\varphi_3(t)^3 \\ &\quad + 80c\varphi_1(t)\varphi_2(t)^2\varphi_3(t)\varphi_4(t) - 18c\varphi_1(t)\varphi_2(t)\varphi_3(t)^3 - 144c\varphi_1(t)^2\varphi_2(t)\varphi_4(t)^2 \\ &\quad + 6c\varphi_1(t)^2\varphi_3(t)^2\varphi_4(t) - 18\varphi_1(t)^3\varphi_2(t)\varphi_3(t)\varphi_4(t) + 192c^2\varphi_1(t)\varphi_3(t)\varphi_4(t)^2 \\ &\quad - \varphi_1(t)^2\varphi_2(t)^2\varphi_3(t)^2 + 4c\varphi_2(t)^3\varphi_3(t)^2 - 144c^2\varphi_2(t)\varphi_3(t)^2\varphi_4(t) + 27c^2\varphi_3(t)^4 \\ &\quad - 16c\varphi_2(t)^4\varphi_4(t) - 256c^3\varphi_4(t)^3).\end{aligned}$$

Logo, o discriminante de $\check{f}(x, t)$ é $\Psi(t) = \frac{D(t)}{-\varphi_4(t)}$.

Neste exemplo,

$$\begin{aligned}\Psi(t) &= 128(t^2 + 1)^2(t^2 - 1)^4 - 16(t^2 + 1)^4(t^2 - 1)^2 - 256(t^2 - 1)^6 \\ &= 16(t^2 - 1)^2(8(t^2 + 1)^2(t^2 - 1)^2 - (t^2 + 1)^4 - 16(t^2 - 1)^4) \\ &= 16(t + 1)^2(t - 1)^2(t^2 - 3)^2(3t^2 - 1)^2.\end{aligned}$$

A equação homogênea de \mathcal{C} é dada por $F(x, y, z) = x^4 - 2x^2y^2 + y^4 + x^2z^2 + y^2z^2 + z^4 = 0$, onde x, y, z são as coordenadas homogêneas de \mathbb{P}^2 .

Vamos agora encontrar os pontos singulares de \mathcal{C} . Temos

$$\frac{\partial F}{\partial x} = 0 \Leftrightarrow x = 0 \text{ ou } 2x^2 - 2y^2 + z^2 = 0,$$

$$\frac{\partial F}{\partial y} = 0 \Leftrightarrow y = 0 \text{ ou } -2x^2 + 2y^2 + z^2 = 0,$$

$$\frac{\partial F}{\partial z} = 0 \Leftrightarrow z = 0 \text{ ou } x^2 + y^2 + 2z^2 = 0.$$

Assim, $\frac{\partial F}{\partial x} = \frac{\partial F}{\partial y} = \frac{\partial F}{\partial z} = 0 \Leftrightarrow z = 0$ e $y = \pm x$, com $y \neq 0$, pois $P = (0, 0) \notin \mathcal{C}$.

Portanto os pontos singulares de \mathcal{C} são $(1 : -1 : 0)$ e $(1 : 1 : 0)$.

Desomogeneizando a equação $F(x, y, z)$ em relação a x , temos

$$F(y, z) = 1 - 2y^2 + y^4 + z^2 + y^2z^2 + z^4.$$

Queremos analisar o ponto singular $Q = (1 : -1 : 0)$. Então faremos uma mudança de coordenadas para trabalharmos na origem.

Seja $u = y + 1$.

Assim,

$$\begin{aligned} F(u, z) &= 1 - 2(u - 1)^2 + (u - 1)^4 + z^2 + (u - 1)^2z^2 + z^4 \\ &= 4u^2 + 2z^2 - 4u^3 - 2uz^2 + u^4 + u^2z^2 + z^4. \end{aligned}$$

Como o grau da forma de menor grau é dois e \mathcal{C} tem duas tangentes distintas em Q , este ponto é um nó. De maneira similar, concluímos que o ponto singular $R = (1 : 1 : 0)$ também é um nó.

Pela Proposição 2.2, $\delta_P = \delta_R = \frac{2(2-1)}{2} = 1$. Pela fórmula do gênero (Teorema 2.4), $g(\mathcal{X}) = 3 - (1 + 1) = 1$.

Como as retas $y = \pm x$ não são tangentes nestes nós, π_P não é ramificado em $t = \pm 1$.

De fato, considere $Q = (1 : 1 : 0)$ e L a reta tangente a F em Q . Então

$$\begin{aligned} I_Q(F, L) &= I_Q(x^4 - 2x^2y^2 + y^4 + x^2z^2 + y^2z^2 + z^4, y - x) \\ &= I_Q((y^3 + xy^2 + (z^2 - x^2)(y + x))(y - x) + z^2(2x^2 + z^2), y - x) \\ &= I_Q(z^2(2x^2 + z^2), y - x) \\ &= I_Q(z^2, y - x) + I_Q(2x^2 + z^2, y - x) \\ &= 2 \cdot I_Q(z, y - x) + I_Q((\sqrt{2}x + iz)(\sqrt{2}x - iz), y - x) \\ &= 2 \cdot 1 + I_Q(\sqrt{2}x + iz, y - x) + I_Q(\sqrt{2}x - iz, y - x) \\ &= 2 + 0 + 0 = 2 = m_Q(F). \end{aligned}$$

Segue da Afirmação 3.2 que L não é tangente a F em Q . Logo, π_P não é ramificado em $t = 1$.

Analogamente, π_P não é ramificado em $t = -1$.

Além disso, a reta $r : y = \pm \alpha x$, onde α satisfaz $(\alpha^2 - 3)^2(3\alpha^2 - 1)^2 = 0$, é uma reta bitangente de \mathcal{C} . Isto segue do Lema 4.1 de [8], página 290.

Sejam $R \in r \cap \mathcal{C}$ e $G = y - \alpha x$.

$$\begin{aligned} I_R(\mathcal{C}, r) &= I_R(F, G) \\ &= I_R(F'G + z^4 + (\alpha^2 + 1)x^2z^2 + (\alpha^2 - 1)^2x^4, G) \\ &= I_R(z^4 + (\alpha^2 + 1)x^2z^2 + (\alpha^2 - 1)^2x^4, G). \end{aligned}$$

Procuramos escrever $z^4 + (\alpha^2 + 1)x^2z^2 + (\alpha^2 - 1)^2x^4$ como produto de fatores lineares. Para isto resolveremos a equação biquadrada $z^4 + (\alpha^2 + 1)x^2z^2 + (\alpha^2 - 1)^2x^4 = 0$. Assim,

$$\frac{z^4}{x^4} + (\alpha^2 + 1)\frac{z^2}{x^2} + (\alpha^2 - 1)^2 = 0 \Leftrightarrow \frac{z^2}{x^2} = \frac{-(\alpha^2 + 1) \pm \sqrt{-3\alpha^4 + 10\alpha^2 - 3}}{2}.$$

Para obtermos fatores lineares basta tomar α satisfazendo a equação $-3\alpha^4 + 10\alpha^2 - 3 = 0$.

Logo, $\frac{z^2}{x^2} = \frac{-(\alpha^2 + 1)}{2}$.

Sejam F_1 e F_2 os fatores lineares encontrados. Então

$$I_R(z^4 + (\alpha^2 + 1)x^2z^2 + (\alpha^2 - 1)^2x^4, G) = I_R(F_1 \cdot F_2, G) = I_R(F_1, G) + I_R(F_2, G).$$

Como $F_1 \cap F_2 = \emptyset$, quando $R \in F_1$, temos $I_R(F_1, G) = 1$ e quando $R \in F_2$, $I_R(F_2, G) = 1$.

Segue então da Relação de Nöether que o tipo de ramificação de π_P é $(2, 2, 2, 2)$.

Resolvendo a equação $\check{f}(x, t) = 0$, obtemos

$$x^2 = \frac{-(t^2 + 1) \pm \sqrt{(3t^2 - 1)(-t^2 + 3)}}{2(t^2 - 1)^2}.$$

Logo, $K = k(x, t) = k(t, \sqrt{t^2 - 3}, \sqrt{1 - 3t^2})$.

Assim, obtemos três corpos intermediários entre K e K_P , considerando os subgrupos de V_4 .

De fato, temos:

$$K_1 = k(t, \sqrt{1 - 3t^2}); K_2 = k(t, \sqrt{t^2 - 3}); K_3 = k(t, \sqrt{1 - 3t^2}\sqrt{t^2 - 3}) = k(t, \sqrt{-3 + 10t^2 - 3t^4}).$$

Seja \mathcal{C}_i a curva definida por K_i ($1 \leq i \leq 3$).

Então K_1 é o corpo de funções da curva plana suave \mathcal{C}_1 , cuja equação afim é $y^2 = 1 - 3t^2$.

Como \mathcal{C}_1 não tem ponto singular, seu gênero é dado por

$$g(\mathcal{C}_1) = \frac{(2-1)(2-2)}{2} = 0.$$

Analogamente, $g(\mathcal{C}_2) = 0$.

Para encontrar o gênero de \mathcal{C}_3 , vamos aplicar a fórmula de Riemann-Hurwitz às curvas \mathcal{C}_3 e a curva que define K_P , digamos \mathcal{C}' :

$$2g(\mathcal{C}_3) - 2 = (2g(\mathcal{C}') - 2) \cdot \text{gr}(K_3 | K_P) + \sum_{P \in \mathcal{C}_3} (e_P - 1)$$

$$2g(\mathcal{C}_3) - 2 = (2 \cdot 0 - 2) \cdot 2 + 4 = 0$$

Logo, $g(\mathcal{C}_3) = 1$.

Exemplo 3.2. *Sejam \mathcal{C} a curva definida pela equação $y^4 - xy^3 + x^2 + 1 = 0$ e $P = (0, 0)$. Então $G_P \simeq D_4$ e $g(\mathcal{X}) = 2$.*

De fato, temos

$$\tilde{f}(x, t) = (t^4 - t^3)x^4 + x^2 + 1;$$

Usando a Observação 3.7, vamos verificar que $G_P \simeq D_4$.

Com efeito, $\sqrt{\frac{1}{t^4 - t^3}} = \frac{1}{t} \sqrt{\frac{1}{t(t-1)}} \notin k(t)$ e

$$\sqrt{\frac{1}{t^4 - t^3} \cdot \left(\frac{1}{(t^4 - t^3)^2} - \frac{4}{t^4 - t^3} \right)} = \frac{1}{t^4 - t^3} \sqrt{\frac{1 - 4t^4 + 4t^3}{t^4 - t^3}} \notin k(t).$$

Além disso, $\tilde{g}(z) = \left(z - \frac{1}{t^4 - t^3} \right) \left(z^2 - \frac{4}{t^4 - t^3} \right)$ e

$$\begin{aligned} \Psi(t) &= 128(t^4 - t^3)^2 - 16(t^4 - t^3) - 256(t^4 - t^3)^3 = 16(t^4 - t^3)(8(t^4 - t^3) - 1 - 16(t^4 - t^3)^2) \\ &= 16t^3(t-1)(-16t^8 + 32t^7 - 16t^6 + 8t^4 - 8t^3 - 1) = 16t^3(t-1)(4t^4 - 4t^3 - 1)^2. \end{aligned}$$

A fim de encontrar os pontos singulares de \mathcal{C} , cuja equação homogênea é dada por

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

resolveremos as seguintes equações:

$$\frac{\partial F}{\partial x} = 0 \Leftrightarrow -y^3 + 2xz^2 = 0;$$

$$\frac{\partial F}{\partial y} = 0 \Leftrightarrow y^2(4y - 3x) = 0;$$

$$\frac{\partial F}{\partial z} = 0 \Leftrightarrow 2z(x^2 + 2z^2) = 0.$$

Assim, o único ponto singular de \mathcal{C} é $(1 : 0 : 0)$.

Desomogeneizando $F(x, y, z)$ em relação a x , obtemos $F(y, z) = z^2 - y^3 + y^4 + z^4$. Logo, o ponto singular $Q = (1 : 0 : 0)$ é uma cúspide simples de multiplicidade dois. Pelo Corolário 2.1, $\delta_Q = 1$. Logo, $g(\mathcal{X}) = 3 - 1 = 2$.

Observe que a reta $r : y = \alpha x$, é uma reta bitangente de \mathcal{C} , onde α satisfaz

$$4\alpha^4 - 4\alpha^3 - 1 = 0.$$

Isto segue novamente do Lema 4.1 de [8], página 290.

Resolvendo a equação $\check{f}(x, y) = 0$, temos que

$$x^2 = \frac{-1 \pm \sqrt{1 - 4t^4 + 4t^3}}{2t^4 - 2t^3}.$$

Além disso, sendo x_i ($1 \leq i \leq 4$) as raízes da equação $\check{f}(x, y) = 0$, temos o seguinte diagrama da correspondência de Galois:

$$\begin{array}{ccc}
 L_{\mathbb{P}} & \longleftrightarrow & (1) \\
 \downarrow & & \downarrow \\
 K = k(t, x_1) & \longleftrightarrow & \langle (34) \rangle = \{(1), (34)\} \\
 \downarrow & & \downarrow \\
 k(t, x_1^2) & \longleftrightarrow & \langle (12), (34) \rangle = \{(1), (12), (34), (12)(34)\} \\
 \downarrow & & \downarrow \\
 K_{\mathbb{P}} = k(t) & \longleftrightarrow & D_4 = \langle (1324), (12) \rangle
 \end{array}$$

Seja \mathcal{C}' a curva suave definida por $k(t, x_1^2)$. Então o recobrimento duplo $\mathcal{C}' \rightarrow \mathbb{P}^1$ ramifica-se em quatro pontos satisfazendo $4t^4 - 4t^3 - 1 = 0$, onde o índice de ramificação de $\theta_{\mathbb{P}}$ é dois.

Aplicando a fórmula de Riemann-Hurwitz à curva \mathcal{C}' e à curva que define $K_{\mathbb{P}}$, digamos \mathcal{C}'' , temos:

$$2g(\mathcal{C}') - 2 = (2g(\mathcal{C}'') - 2) \cdot \text{gr}(k(t, x_1^2) | K_{\mathbb{P}}) + \sum_{p \in \mathcal{C}'} (e_p - 1)$$

$$2g(\mathcal{C}') - 2 = (2 \cdot 0 - 2) \cdot 2 + 4 = 0$$

Logo, $g(\mathcal{C}') = 1$.

Agora vamos calcular o índice de ramificação de θ_P em $t = 0$ e em $t = 1$. Para isto, sejam $Q = (1 : 0 : 0)$, $R = (1 : 1 : 0)$ e r (respectivamente s) a reta tangente a F em Q (respectivamente em R), passando por $P = (0 : 0 : 1) \notin \mathcal{C}$. Assim,

$$\begin{aligned} I_Q(F, r) &= I_Q(y^4 - xy^3 + x^2z^2 + z^4, y) \\ &= I_Q(x^2z^2 + z^4, y) \\ &= 2 \cdot 1 + I_Q(x + iz, y) + I_Q(x - iz, y) \\ &= 2 + 0 + 0 = 2. \end{aligned}$$

$$\begin{aligned} I_R(F, s) &= I_R(y^4 - xy^3 + x^2z^2 + z^4, y - x) \\ &= I_R(y^3(y - x) + x^2z^2 + z^4, y - x) \\ &= I_R(z^2, y - x) + I_R(x^2 + z^2, y - x) \\ &= 2 \cdot 1 + I_R(x + iz, y - x) + I_R(x - iz, y - x) \\ &= 2 + 0 + 0 = 2. \end{aligned}$$

Como o corpo de funções L_P é isomorfo a $k(t, x_1, \sqrt{\Psi(t)})$, vemos que $\theta_P : \tilde{\mathcal{C}}_P \rightarrow \mathbb{P}^1$ possui tipo de ramificação $(2, 2, 2, 2, 2, 2)$. Além disso, aplicando a Fórmula de Riemann-Hurwitz a $\tilde{\mathcal{C}}_P$ e a \mathcal{X} (veja o diagrama), temos:

$$2g(\tilde{\mathcal{C}}_P) - 2 = [L_P : K](2g(\mathcal{X}) - 2) + 6 = 2(2 \cdot 2 - 2) + 6.$$

Logo, $g(\tilde{\mathcal{C}}_P) = 6$.

Agora apresentaremos um exemplo de uma curva \mathcal{C} satisfazendo $G_P \simeq A_4$ para algum $P \notin \mathcal{C}$.

Observação 3.9. *O grupo G_P é isomorfo a A_4 se, e somente se, a extensão de corpos $M | k(t)$ for uma extensão cúbica de Galois.*

De fato, pelo Teorema 1 de [6], G_P é isomorfo a A_4 se, e somente se, $\tilde{g}(z)$ é irredutível sobre $k(t)$ e $\sqrt{\Psi(t)} \in k(t)$. Como $\tilde{g}(z)$ tem grau três, a extensão $M | k(t)$ é cúbica. E como esta extensão é normal, ela é galoisiana.

Exemplo 3.3. *Sejam \mathcal{C} a curva definida pela equação*

$$x^4 + x^3y + xy^3 + y^4 + 2x^3 + 2y^3 + 2x + 2y + 1 = 0$$

e $P = (0, 0)$. Então $G_P \simeq A_4$ e $g(\mathcal{X}) = 2$.

De fato, $\check{f}(x, t) = (t^4 + t^3 + t + 1)x^4 + (2t^3 + 2)x^3 + (2 + 2t)x + 1$;

$$\begin{aligned}\tilde{g}(z) &= z^3 + \frac{(2 + 2t)(2t^3 + 2) - 4(t^4 + t^3 + t + 1)}{(t^4 + t^3 + t + 1)^2}z - \frac{(2t^3 + 2)^2 + (2 + 2t)^2(t^4 + t^3 + t + 1)}{(t^4 + t^3 + t + 1)^3} \\ &= z^3 - \frac{4(2t^2 + t + 2)}{(t^4 + t^3 + t + 1)^2};\end{aligned}$$

$$\begin{aligned}\Psi(t) &= 27(2 + 2t)^4(t^4 + t^3 + t + 1)^2 + 4(2 + 2t)^3(2t^3 + 2)^3 \\ &\quad + 6(2 + 2t)^2(2 + 2t^3)^2(t^4 + t^3 + t + 1) + 192(2 + 2t)(2 + 2t^3)(t^4 + t^3 + t + 1)^2 \\ &\quad + 27(2 + 2t^3)^4 - 256(t^4 + t^3 + t + 1)^3 \\ &= -432(t + 1)^4(4t^8 - 4t^7 + 13t^6 - 10t^5 + 19t^4 - 10t^3 + 13t^2 - 4t + 4) \\ &= -432(t + 1)^4(t^2 - t + 1)^2(2t^2 + t + 2)^2.\end{aligned}$$

A equação homogênea da curva \mathcal{C} é dada por

$$F(x, y, z) = x^4 + x^3y + xy^3 + y^4 + 2x^3z + 2y^3z + 2xz^3 + 2yz^3 + z^4 = 0.$$

Para encontrar os pontos singulares de \mathcal{C} , vamos resolver as seguintes equações:

$$\frac{\partial F}{\partial x} = 0 \Leftrightarrow 4x^3 + 3x^2y + y^3 + 6x^2z + 2z^3 = 0;$$

$$\frac{\partial F}{\partial y} = 0 \Leftrightarrow x^3 + 3xy^2 + 4y^3 + 6y^2z + 2z^3 = 0;$$

$$\frac{\partial F}{\partial z} = 0 \Leftrightarrow 2x^3 + 2y^3 + 6xz^2 + 6yz^2 + 4z^3 = 0.$$

O ponto $(1 : -1 : 0)$ é o único ponto singular.

Desomogeneizando $F(x, y, z)$ em relação a x , obtemos

$$F(y, z) = 1 + y + y^3 + y^4 + 2z + 2y^3z + 2z^3 + 2yz^3 + z^4.$$

Fazendo a mudança de coordenadas $u = y + 1 \Rightarrow y = u - 1$, temos:

$$\begin{aligned}F(u, z) &= 3u^2 + 6uz - 3u^3 - 6u^2z + u^4 + 2uz^3 + z^4 + 2u^3z \\ &= 3u(u + 2z) - 3u^2(u + 2z) + u^4 + 2uz^3 + z^4 + 2u^3z\end{aligned}$$

Como a forma de menor grau tem grau dois e \mathcal{C} tem duas tangentes distintas no ponto singular, a saber, u e $u + 2z$, segue que ele é um nó. Logo, $\delta_Q = 1$, onde Q é o ponto singular. Segue da fórmula do gênero que $g(\mathcal{X}) = 3 - \delta_P = 2$.

Seja $P = (0, 0)$. Então

$$\begin{aligned}I_P(\mathcal{C}, u) &= I_P(3u(u + 2z) - 3u^2(u + 2z) + u^4 + 2uz^3 + z^4 + 2u^3z, u) \\ &= I_P(z^4, u) = 4.\end{aligned}$$

$$\begin{aligned}
I_{\mathbb{P}}(\mathcal{C}, \mathbf{u} + 2\mathbf{z}) &= I_{\mathbb{P}}(3\mathbf{u}(\mathbf{u} + 2\mathbf{z}) - 3\mathbf{u}^2(\mathbf{u} + 2\mathbf{z}) + \mathbf{u}^4 + 2\mathbf{u}\mathbf{z}^3 + \mathbf{z}^4 + 2\mathbf{u}^3\mathbf{z}, \mathbf{u} + 2\mathbf{z}) \\
&= I_{\mathbb{P}}((\mathbf{u} + 2\mathbf{z})(3\mathbf{u} - 3\mathbf{u}^2 + \mathbf{u}^3) + 2\mathbf{u}\mathbf{z}^3 + \mathbf{z}^4, \mathbf{u} + 2\mathbf{z}) \\
&= I_{\mathbb{P}}(2\mathbf{u}\mathbf{z}^3 + \mathbf{z}^4, \mathbf{u} + 2\mathbf{z}) = I_{\mathbb{P}}(\mathbf{z}^3(2\mathbf{u} + \mathbf{z}), \mathbf{u} + 2\mathbf{z}).
\end{aligned}$$

Como as tangentes de $\mathbf{z}^3(2\mathbf{u} + \mathbf{z})$ em \mathbb{P} são distintas das de $\mathbf{u} + 2\mathbf{z}$ em \mathbb{P} , vale

$$I_{\mathbb{P}}(\mathbf{z}^3(2\mathbf{u} + \mathbf{z}), \mathbf{u} + 2\mathbf{z}) \geq m_{\mathbb{P}}(\mathbf{z}^3(2\mathbf{u} + \mathbf{z})) \cdot m_{\mathbb{P}}(\mathbf{u} + 2\mathbf{z}) = 4.$$

Portanto o nó $(1 : -1 : 0)$ é bi-inflexional.

Pelo Lema 3.1, a reta $\mathbf{y} = \alpha\mathbf{x}$ que satisfaz

$$(\alpha^2 - \alpha + 1)^2(2\alpha^2 + \alpha + 2)^2 = 0,$$

é uma tangente 1-inflexional de \mathcal{C} . E pelo Lema 3.2, a reta $\mathbf{y} = -\mathbf{x}$ passa pelo ponto singular. Além disso, é tangente à curva nele. De fato, sejam $\mathbf{Q} = (1 : -1 : 0)$ e r a reta definida pela equação $\mathbf{y} = -\mathbf{x}$. Então

$$\begin{aligned}
I_{\mathbf{Q}}(\mathbb{F}, r) &= I_{\mathbf{Q}}(\mathbf{y}^4 + (\mathbf{x} + 2\mathbf{z})\mathbf{y}^3 + (\mathbf{x}^3 + 2\mathbf{z}^3)\mathbf{y} + \mathbf{z}^4 + 2\mathbf{x}\mathbf{z}^3 + 2\mathbf{x}^3\mathbf{z} + \mathbf{x}^4, \mathbf{y} + \mathbf{x}) \\
&= I_{\mathbf{Q}}((\mathbf{y}^3 + 2\mathbf{z}\mathbf{y}^2 - 2\mathbf{x}\mathbf{z}\mathbf{y} + \mathbf{x}^3 + 2\mathbf{z}^3 + 2\mathbf{x}^2\mathbf{z})(\mathbf{y} + \mathbf{x}) + \mathbf{z}^4, \mathbf{y} + \mathbf{x}) \\
&= I_{\mathbf{Q}}(\mathbf{z}^4, \mathbf{y} + \mathbf{x}) = 4 > m_{\mathbf{Q}}(\mathbb{F}).
\end{aligned}$$

Assim, o número de pontos de ramificação de $\pi_{\mathbb{P}}$ é cinco, e seus índices de ramificação são três.

Além disso, a extensão de corpos $\mathbb{M} | \mathbb{k}(t)$ é uma extensão galoisiana dada por

$$z^3 = \frac{4(2t^2 + t + 2)}{(t^4 + t^3 + t + 1)^2}.$$

Pela Observação 3.9, $G_{\mathbb{P}} \simeq A_4$.

Obtemos um recobrimento triplo $R_{\mathbb{P}} \rightarrow \mathbb{P}^1$, cujo tipo de ramificação é $(3, 3, 3, 3, 3)$. Da consideração acima, vemos que $\theta_{\mathbb{P}} : \tilde{\mathcal{C}} \rightarrow \mathbb{P}^1$ possui tipo de ramificação $(3, 3, 3, 3, 3)$, então $g(\tilde{\mathcal{C}}_{\mathbb{P}}) = 9$. De fato, observe o seguinte diagrama:

$$\begin{array}{c}
L_{\mathbb{P}} \\
| \\
\mathbb{K} \\
| \\
K_{\mathbb{P}}
\end{array}$$

Aplicando a Fórmula de Riemann-Hurwitz a $\tilde{\mathcal{C}}_{\mathbb{P}}$ e à curva suave definida por \mathbb{K} , temos:

$$2g(\tilde{\mathcal{C}}_{\mathbb{P}}) - 2 = [L_{\mathbb{P}} : \mathbb{K}](2g(\mathcal{X}) - 2) + 5(3 - 1) = 3(2 \cdot 2 - 2) + 10.$$

Logo, $g(\tilde{\mathcal{C}}_{\mathbb{P}}) = 9$.

3.3 O caso das quárticas de gênero dois

Encerramos este capítulo estudando as quárticas de gênero dois. Vamos mostrar que, neste caso, não há pontos de Galois associados a ela.

Precisaremos do seguinte resultado:

Observação 3.10. *Se o recobrimento $\pi_P : \mathcal{X} \rightarrow \mathbb{P}^1$ for galoisiano com $G_P \simeq \mathbb{Z}_4$, então a curva quártica \mathcal{C} é birracionalmente equivalente à curva definida por*

$$g(x, y) + c = 0,$$

onde $g(x, y)$ é um polinômio homogêneo de grau quatro e c é um elemento não nulo de k .

Demonstração: Como $K | K_P$ é uma extensão galoisiana, seu grupo de Galois é isomorfo ao grupo cíclico de ordem quatro, isto é, \mathbb{Z}_4 . Assim, K pode ser expresso como $K(x, t)$, onde

$$x^4 = \frac{a(t)}{b(t)} \in k(t) = K_P.$$

Fazendo $y = tx$, temos

$$b\left(\frac{y}{x}\right) x^4 = a\left(\frac{y}{x}\right).$$

Para obter uma equação quártica, o grau de $a(t)$ deve ser zero.

Portanto, a equação de \mathcal{C} pode ser escrita como $g(x, y) + c = 0$, onde $g(x, y)$ é um polinômio homogêneo de grau quatro e $c \in k \setminus \{0\}$. ■

Teorema 3.6. *Se \mathcal{C} for uma curva quártica plana de gênero dois, então não existe ponto $P \in \mathbb{P}^2 \setminus \mathcal{C}$ que satisfaz $G_P \simeq \mathbb{Z}_4$.*

Demonstração: Suponhamos que exista algum ponto $P \in \mathbb{P}^2 \setminus \mathcal{C}$ tal que $G_P \simeq \mathbb{Z}_4$. Pela Observação 3.10, a curva \mathcal{C} é definida por $g(x, y) + c = 0$, onde $g(x, y)$ é um polinômio homogêneo de grau quatro e $c \in k - \{0\}$. A equação homogênea da curva é

$$F(x, y, z) = cz^4 + g(x, y) = 0,$$

onde x, y, z , são as coordenadas homogêneas de \mathbb{P}^2 . Então $g(x, y)$ é de uma das formas:

- (i) $g(x, y) = (y - \alpha x)^2(y - \beta x)(y - \gamma x)$,
- (ii) $g(x, y) = (y - \alpha x)^2(y - \beta x)^2$,
- (iii) $g(x, y) = (y - \alpha x)^3(y - \beta x)$,
- (iv) $g(x, y) = (y - \alpha x)^4$,

onde α , β e γ são elementos mutuamente distintos de k . Assim, os pontos singulares de \mathcal{C} são os mesmos do caso $P \in \mathcal{C}$. Como $F(x, y, z)$ não é irredutível nos casos (ii) e (iv), basta considerar os casos (i) e (iii).

No caso (i), a equação homogênea de \mathcal{C} é

$$F(x, y, z) = cz^4 + (y - \alpha x)^2(y - \beta x)(y - \gamma x).$$

Vamos olhar \mathcal{C} no plano afim $X = 1$. Assim,

$$F(1, y, z) = cz^4 + (y - \alpha)^2(y - \beta)(y - \gamma).$$

Para transladar o ponto singular $Q = (1 : \alpha : 0)$ para a origem, façamos a seguinte mudança de coordenadas:

$$u = y - \alpha.$$

Assim, a nova equação de \mathcal{C} é dada por $h(u, z) = cz^4 + u^2(u - \alpha - \beta)(u - \alpha - \gamma)$.

Como $(u - \alpha - \beta)$ e $(u - \alpha - \gamma)$ são inversíveis em $\left(\frac{k[u, z]}{(h(u, z))}\right)_{(u, z)}$, segue que o ponto singular é localmente definido por $u^2 = z^4$. Logo, o índice de ramificação de π_P em $t = \alpha$ é dois. Agora vamos calcular o gênero de \mathcal{X} .

Primeiramente observamos que a curva possui dois ramos, a saber, $f_1 = u - z^2$ e $f_2 = u + z^2$. Então $\hat{f}_1(u, z) = \frac{f_1(u, z)}{z} = \frac{uz - z^2}{z} = u - z$. Analogamente, $\hat{f}_2(u, z) = u + z$.

Pela Fórmula de Noether (veja [2], página 175), $I_Q(f_1, f_2) = I_Q(\hat{f}_1, \hat{f}_2) + m_Q(f_1) \cdot m_Q(f_2) = 1 + 1 = 2$.

Logo, $\delta_Q = 2$ e $g(\mathcal{X}) = 3 - \delta_Q = 1$.

Pelo Lema 3.2, a reta $r : y = \alpha x$ passa por Q . Além disso, ela é tangente a \mathcal{C} neste ponto, pois temos

$$I_Q(F, r) = I_Q(cz^4 + (y - \alpha x)^2(y - \beta x)(y - \gamma x), y - \alpha x) = 4 > m_Q(\mathcal{C}) = 2.$$

Observe que $\check{f}(x, t) = c + x^4(t - \alpha)^2(t - \beta)(t - \gamma)$.

Assim, o discriminante é dado por $\Psi(t) = -256c^3(t - \alpha)^6(t - \beta)^3(t - \gamma)^3$.

Pelo Lema 4.1 de [8], vemos que $(1 : \beta : 0)$ e $(1 : \gamma : 0)$ são pontos de inflexão de ordem dois.

O índice de ramificação de $\pi_P : \mathcal{X} \rightarrow \mathbb{P}^1$ é quatro em $t = \beta$ e em $t = \gamma$. Logo, o tipo de ramificação de π_P é $(2, 4, 4)$.

No caso (iii), a equação homogênea de \mathcal{C} é dada por

$$F(x, y, z) = cz^4 + (y - \alpha x)^3(y - \beta x).$$

Vamos olhar \mathcal{C} no plano afim $X = 1$. Assim,

$$F(1, \mathbf{y}, z) = cz^4 + (\mathbf{y} - \alpha)^3(\mathbf{y} - \beta).$$

Para transladar o ponto singular $Q = (1 : \alpha : 0)$ para a origem, façamos a seguinte mudança de coordenadas:

$$\mathbf{u} = \mathbf{y} - \alpha.$$

Assim, a nova equação de \mathcal{C} é dada por $h(\mathbf{u}, z) = cz^4 + \mathbf{u}^3(\mathbf{u} - \alpha - \beta)$.

Como $(\mathbf{u} - \alpha - \beta)$ é inversível em $\left(\frac{k[\mathbf{u}, z]}{h(\mathbf{u}, z)}\right)_{(\mathbf{u}, z)}$, segue que o ponto singular é localmente definido por $\mathbf{u}^3 = z^4$. Então ele é uma cúspide simples de multiplicidade três. Pelo Teorema 3.1, $g(\mathcal{X}) = 0$.

Pelo Lema 3.2, a reta $r : \mathbf{y} = \alpha x$ passa por Q . Além disso, ela é tangente à curva neste ponto, pois $I_Q(F, r) = 4 > m_Q(\mathcal{C})$.

Observe que $\check{f}(x, t) = c + x^4(t - \alpha)^3(t - \beta)$.

Assim, o discriminante é dado por $\Psi(t) = -256c^3(t - \alpha)^9(t - \beta)^3$.

Pelo Lema 4.1 de [8], vemos que $(1 : \beta : 0)$ é um ponto de inflexão de ordem dois.

Portanto, o tipo de ramificação de π_P é $(4, 4)$.

Assim, em qualquer caso, o gênero de \mathcal{C} é diferente de 2. ■

Referências Bibliográficas

- [1] Fulton, W., *Geometry of projective algebraic curves*, Addison-Wesley.
- [2] Garcia, A., *Semigroups associated to singular points of plane curves*, Journal für die Reine Angewandte Mathematik, v. 336, 165-184 (1982).
- [3] Garcia, A. e Lequain, Y., *Elementos de álgebra*, Projeto Euclides, IMPA, 2003.
- [4] Gorenstein, D., *An arithmetic theory of adjoint plane curves*, Transactions of the American Mathematics Society, v. 72, 414-437 (1952).
- [5] Hefez, A., *Irreducible Plane Curve Singularities*, In Real and Complex Singularities, Lecture Notes in Pure and Applied Math. Vol. 232, Marcel Dekker, 1-120 (2003).
- [6] Kappe, L. e Warren. B., *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly 96 (1989), 133-137.
- [7] Miura, K., *Field Theory for Function Fields of Singular Plane Quartic Curves*, Bull. Austral. Math. Soc. 62 (2000), 193-204.
- [8] Miura, K. e H. Yoshihara, *Field Theory for Function Fields of Plane Quartic Curves*, Journal of Algebra 226, 283-294 (2000).
- [9] Namba, M., *Geometry of projective algebraic curves*, Marcel Dekker.
- [10] Silva, P. M., *Pontos de Galois sobre curvas quárticas projetivas não singulares*, UFES, 2009.
- [11] Souza, G. A., *O grupo de Galois do fecho normal associado a projeções centrais de curvas quárticas projetivas planas não singulares*, UFES, 2010.
- [12] Tokunaga, H., *Triple coverings of algebraic surfaces according to the Cardano formula*, J. Math. Kyoto Univ. 31-2 (1991), 359-375.

- [13] Vaisencher, I., *Introdução às Curvas Algébricas Planas*, Coleção Matemática Universitária, IMPA, 1996.