O grupo de Galois do fecho normal associado a projeções centrais de quárticas projetivas planas não singulares.

Guilbert de Arruda Souza

Dissertação de Mestrado em Matemática

Mestrado em Matemática

Universidade Federal do Espírito Santo

Vitória, 28 de Maio de 2010

O grupo de Galois do fecho normal associado a projeções centrais de quárticas projetivas planas não singulares.

Guilbert de Arruda Souza

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 28 de maio de 2010 por:

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

Prof. Dr. José Gilvan de Oliveira , UFES

Prof. Dr. Renato Vidal da Silva Martins, UFMG

Universidade Federal do Espírito Santo
Vitória, 28 de Maio de 2010

Souza, Guilbert de Arruda, 1985
O grupo de Galois do fecho normal associado a projeções centrais de quárticas projetivas planas não singulares. [Vitória] 2010
(UFES, M. Sc., Matemática, 2010)
Dissertação, Universidade Federal do Espírito Santo, PPGMAT.
I. Álgebra
I. PPGMAT/UFES II. Título

Dedicatória

Ao grande senhor Gilberto Vagonette de Souza.

Agradecimentos

A Deus por todas as dádivas.

À minha família pelo apoio, carinho e atenção nos momentos difíceis.

Ao meu orientador Professor Valmecir Antonio dos Santos Bayer pelo apoio desde o inicio da jornada.

Ao Professor José Gilvan de Oliveira pelas valiosas sugestões e orientações.

Ao Professor Moacir Rosado Filho por valiosos ensinamentos, aconselhamentos e apoio.

Aos amigos e companheiros mestrandos e mestres do PPGMAT pela amizade e momentos agradáveis.

Aos professores do PPGMAT pelos ensinamentos e em especial ao professor Ricardo Soares Leite pelo incentivo.

À Luana de Oliveira Justo por sugestões valiosas, apoio incondicional e por seu carinho e amor de sempre.

À FAPES (FUNDAÇÃO DE AMPARO À PESQUISA DO ESPÍRITO SANTO) pelo apoio financeiro.

Sumário

Resumo

Esta monografia trata do estudo de Pontos de Galois associados a uma curva algébrica projetiva plana de grau 4 sobre um corpo de característica zero. A noção de ponto de Galois associado a uma curva algébrica projetiva plana surge quando se projeta a curva sobre uma reta a partir de um ponto que é o centro de projeção, sendo ambos, a reta e o ponto, situados no plano da curva. Há duas situações distintas possíveis: O ponto está sobre a curva, neste caso o denominamos ponto interno. O ponto está fora da curva, neste caso o denominamos ponto externo. Um ponto (interno ou externo) é chamado ponto de Galois associado à curva se a extensão de corpos correspondente ao corpo de funções da curva sobre o corpo de funções da reta de projeção é uma extensão galoisiana. Neste trabalho, estudamos os pontos de Galois externos de uma quártica plana e o grupo de Galois associado ao fecho normal dessas extensões no caso em que elas não são galoisianas.

Abstract

This dissertation is concerned to the study of the properties of Galois points for an algebraic projective plane curve of degree 4 on zero characteristic fields. Galois points associated to algebraic projective plane curves arise from the projection of the curve over a projective line from a point which we call the center of projection, both, the line and the point, placed in the plane of the curve. There are two different possible situations: The point is on the curve, and in this case we call it an inner point. The point is outside the curve, and in this case we call it an outer point. A point (inner or outer one) is called a Galois point for the curve whenever the extension field corresponding to the function field of the curve over the function field of the projection line is a Galois extension. In this dissertation we study the outer Galois points for a quartic plane curve and the associated Galois group of the normal closure of these extensions in case they are not Galois extensions.

Introdução

Esta monografia tem como objetivo central estudar pontos de Galois externos de uma curva plana projetiva de grau 4, que denominaremos por quártica. O estudo sistemático de pontos de Galois associados a curvas algébricas projetivas, e mais geralmente, a variedades projetivas quando a situação é pertinente, começou em 1996 com Hisao Yoshihara. No caso de curvas, esta noção de ponto de Galois surge ao projetarmos uma curva plana irredutível sobre uma reta (do plano) a partir de um ponto que é denominado centro de projeção e que pode ou não estar sobre a curva. Esta projeção induz uma extensão finita de corpos, a saber, o corpo racional associado à reta é visto como um subcorpo do corpo de funções da curva. Quando esta extensão é galoisiana o centro de projeção é chamado de ponto de Galois associado à curva. Se este ponto está na curva ele é chamado ponto de Galois interno e se está fora da curva ele é chamado ponto de Galois externo. Os pontos de Galois internos de uma quártica são mais simples de serem estudados pois, neste caso, tem-se uma extensão de corpos de grau 3. Este caso foi abordado na monografia de mestrado de *P. M. Silva* em [15]. No caso de pontos externos, a extensão de corpos tem grau 4. Neste caso precisamos estudar os possíveis subgrupos do grupo de permutações S_4 que podem surgir como grupos de Galois de um polinômio irredutível de grau 4.

Para sermos mais precisos e começarmos a introduzir a linguagem, consideramos C uma curva projetiva plana não singular sobre um corpo algebricamente fechado k de característica zero. Seja d o grau de C e seja π_P uma projeção de C sobre uma reta l, com centro de projeção num ponto P. Esta projeção induz uma extensão de corpos $k(C) \mid k(l)$. No caso em que P está sobre a curva temos que o grau de $k(C)$ sobre $k(l)$ é igual a $d-1$ e se P é um ponto fora da curva então o grau dessa extensão é igual a d.

Nesta dissertação estudaremos o caso em que o grau $[k(C) : k(l)]$ é igual a 4, isto é, o caso em que C é uma quártica e P está fora de C. Quando a extensão $k(C) \mid k(l)$ for galoisiana o ponto P é chamado um ponto de Galois associado a C.

Quando $k(C) \mid k(l)$ não é galoisiana, isto é, quando o ponto P tomado para centro de projeção não é um ponto de Galois, consideramos o fecho normal L_P da extensão $k(C) \mid k(l)$ (num fecho algébrico de $k(l)$). O resultado principal da dissertação é o Teorema 7 da secção 3.2 que descreve completamente os possíveis grupos de Galois de $L_P \mid k(l)$ que ocorrem. Como o grau da extensão $k(C) \mid k(l)$ é igual a quatro os grupos de Galois de $L_P \mid k(l)$ que

podem ocorrer são subgrupos do grupo de permutações de 4 objetos S_4. O estudo explícito desses subgrupos é o objeto do capítulo 3 da dissertação e o teorema principal desse capítulo é o Teorema 5 da secção 2.1.

O capítulo 3 da dissertação está baseado no trabalho de *Miura, K. e Yoshihara, H.* de 2000, em [11], que foi o primeiro trabalho publicado introduzindo a noção de pontos de Galois. Neste trabalho é estudado o corpo de funções de uma quártica não singular em característica zero.

Posteriormente, a noção de pontos de Galois foi generalizada, também por Yosihara e outros autores, para outros contextos tais como hipersuperfícies e subespaços de Galois. Paralelamente, o assunto tem despertado interesse especialmente para o caso de corpos de característica positiva. Para citar dois exemplos:

1. No caso da curva hermitiana em característica p prima, o conjunto dos pontos de Galois internos coincide com o conjunto dos pontos racionais da curva (Veja a referência [6]). A curva hermitiana é uma curva maximal no contexto da teoria de pontos racionais pois atinge a cota de Weil para o número de pontos racionais (Veja [18]).

2. No caso de característica zero o número de pontos de Galois para curvas de grau maior ou igual a 4 é limitado por 4. No entanto, em característica positiva, este número pode ser infinito. Recentemente, *S. Fukasawa* em [3] apresentou uma classe de curvas com número infinito de pontos de Galois. Esta classe de curva é exatamente uma família de curvas estranhas racionais que foi estudada, no início da década de 1990, por *V. Bayer e A. Hefez* em [1]. Veja também a dissertação de Mestrado de *C. P. C. Chacca* em [2].

Para tornar a monografia tão auto-suficiente quanto possível a organizamos da maneira seguinte. Ela é apresentada em tres capítulos.

O primeiro capítulo é dedicado ao material básico sobre curvas algébricas projetivas planas. Essencialmente nesse capítulo apresentamos as definições iniciais, os conceitos básicos e teoremas clássicos que são utilizados na monografia. Para esse capítulo a referência básica é o livro Algebraic Curves de *W. Fulton* [4].

No segundo capítulo apresentamos um estudo dos subgrupos do grupo S_4 das permutações de 4 objetos que surgem como grupos de Galois de um polinômio irredutível de grau 4. Este assunto é clássico e já foi muito explorado há algumas décadas (Veja por exemplo *N. Jacobson* [8], *I. Kaplansky* [9] e *R. P. Stauduhar* [16]). Ele foi abandonado devido ao grande esforço computacional para manipular exemplos. No entanto, nos dias atuais, com a popularização da Computação Algébrica é possível trazê-lo de volta e, eventualmente, ser apresentado em disciplinas específicas de Álgebra. Esta é, além da necessidade natural do assunto da monografia, mais uma razão da sua apresentação de forma detalhada e justificando um capítulo no trabalho.

Os resultados apresentados no capítulo estão no trabalho de *L. C. Kappe* e *B. Warren* [10]. No final do capítulo são apresentados alguns exemplos básicos.

O capítulo 3 trata do assunto central da monografia. Nele apresentamos o teorema principal do trabalho que é o Teorema 7 que já comentamos acima. Além disso, como no capítulo 2, no final do capítulo são apresentados exemplos ilustrativos que afirmam a teoria apresentada. A referência aqui utilizada é o trabalho de *K. Miura* e *H. Yoshihara* [11] que é o trabalho inicial dessa teoria.

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. Neste contexto de curvas algébricas estaremos admitindo que o corpo de base k é algebricamente fechado e de característica zero. Os resultados apresentados aqui neste capítulo estão, essencialmente, no livro *Algebraic Curves* de *W. Fulton* [4]. Os resultados das secções 1.3 e 1.4 podem ser encontrados em *M. Namba* [12] ou em *H. Stichtenoth* [17].

1.1 Espaço projetivo e curvas projetivas

Seja k um corpo e $n \in \mathbb{N}$. O espaço afim n-dimensional ou o n-espaço afim sobre k é o conjunto

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

Naturalmente, como conjunto, $\mathbb{A}^n(k)$ é o mesmo que k^n. No entanto, de acordo com a nomenclatura clássica, no contexto dos conjuntos algébricos, não se privilegia a estrutura vetorial de k^n, e isto é feito alterando o nome e a notação desse conjunto. $\mathbb{A}^1$ é chamado de *reta afim* e $\mathbb{A}^2$ é chamado de *plano afim*.

O espaço projetivo é obtido da maneira seguinte. Defina no espaço afim $(n+1)$-dimensional a relação de equivalência seguinte: Se $P,\ Q \in \mathbb{A}^{n+1} \setminus \{0\}$, declaramos que $P \sim Q$ se existe $\lambda \in k,\ \lambda \neq 0$, tal que $Q = \lambda P$. A classe de equivalência de um elemento $P = (a_0, \ldots, a_n) \in \mathbb{A}^{n+1} \setminus \{0\}$ é representada por $\bar{P} = (a_0 : a_1 : \ldots : a_n)$.

O *Espaço Projetivo n-dimensional* é então definido como sendo o conjunto quociente dessa relação de equivalência, a saber,

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

Nos permitimos o abuso de linguagem usando a mesma notação para designar por P os pontos de $\mathbb{P}^n$, a saber, $P = (a_0 : a_1 : \ldots : a_n)$.

Para cada $i,\ 0 \leq i \leq n$, seja $U_i = \{(a_0 : \ldots : a_i : \ldots : a_n) \in \mathbb{P}^n \mid a_i = 1\}$. Então estes conjuntos U_i cobrem $\mathbb{P}^n$, isto é,

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

O conjunto $H_n = \mathbb{P}^n \setminus U_n = \{(a_0 : a_1 : \ldots : a_{n-1} : 0) \in \mathbb{P}^n\}$ é chamado de *hiperplano no infinito* e os pontos $P \in H_n$ são chamados de *pontos no infinito* do espaço projetivo $\mathbb{P}^n$.

Para cada $i,\ 0 \leq i \leq n$, a aplicação φ_i definida por

$$\begin{array}{rccccc} \varphi_i : & \mathbb{A}^n & \longrightarrow & U_i & \subset & \mathbb{P}^n \\ & (a_1, a_2, \ldots, a_n) & \mapsto & (a_0 : \ldots : a_{n-1} : 1 : a_{n+1} : \ldots : a_n) & & \end{array}$$

é bijeção e, portanto, a função φ_i fornece $n+1$ cópias de $\mathbb{A}^n$ em $\mathbb{P}^n$. Se $n = 1$ chamaremos o espaço projetivo $\mathbb{P}^1$ de *reta projetiva* e se $n = 2$ chamaremos $\mathbb{P}^2$ de *plano projetivo*. Assim $\mathbb{P}^2$ pode ser visto como o conjunto de retas do espaço afim tridimensional $\mathbb{A}^3$ que passam pela origem.

De uma maneira mais geral e completamente análoga é possível definir *o espaço projetivo associado a um espaço vetorial* V de dimensão arbitrária sobre um corpo k.

O objetivo central da Geometria Algébrica é o estudo de conjuntos de zeros de famílias de polinômios com coeficientes em k. Vamos comentar alguns conceitos e resultados neste contexto.

Uma *curva algébrica plana projetiva* é uma classe de equivalência de polinômios homogêneos não constantes do anel $k[X, Y, Z]$ que identifica dois polinômios quando um é múltiplo constante não nulo do outro. Seja

$$f = f_0 + f_1 + \cdots + f_d \in k[X, Y]$$

um polinômio de grau d nas indeterminadas X e Y sobre k, escrito como soma de componentes homogêneas, isto é, cada f_i é um polinômio homogêneo de grau i, com $f_d \neq 0$. A *homogenização* do polinômio f é o polinômio homogêneo de grau d em $k[X, Y, Z]$ obtido da seguinte forma:

$$f^*(X, Y, Z) = f_0 Z^d + f_1(X, Y) Z^{d-1} + \cdots + f_d(X, Y) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

O subconjunto $\{(a : b : c) \in \mathbb{P}^2 \mid f^*(a, b, c) = 0\}$ de $\mathbb{P}^2$ claramente contém o conjunto dos zeros de f em $\mathbb{A}^2$ quando olhamos $\mathbb{A}^2$ contido em $\mathbb{P}^2$ pela

imersão $(x, y) \hookrightarrow (x : y : 1)$. Além disso, os pontos de $\mathbb{P}^2$ que estão no conjunto de zeros de f^* e que não estão no conjunto de zeros de f são exatamente os pontos no infinito de $\mathbb{P}^2$ que são zeros de f^*.

A seguir fazemos alguns comentários sobre intersecções de curvas algébricas planas. Para definir o índice de intersecção ou a multiplicidade de intersecção de duas curvas algébricas planas temos duas formas clássicas, a primeira é via codimensão do ideal gerado pelas equações das duas curvas no anel de polinômios localizado no ponto em questão. A segunda forma utiliza a resultante de dois polinômios e, neste caso, é necessário um trabalho cuidadoso de escolha do sistema do coordenadas para perfazer a computação.

As duas definições satisfazem os axiomas que determinam unicamente o índice de intersecção de curvas planas projetivas, que de fato, fornecem um algoritmo efetivo para a sua determinação. Estes axiomas, como citado inicilmente, podem ser encontrados em [4].

Se C e D são duas curvas planas projetivas vamos denotar o índice de intersecção de C com D num ponto $P \in \mathbb{P}^2$ por $I(P, C \cdot D)$. Este índice de intersecção é um número inteiro não negativo ou ∞, sendo que

$$I(P, C \cdot D) = 0 \quad \Leftrightarrow \quad P \notin C \cap D \quad \text{e}$$

$$I(P, C \cdot D) = \infty$$
$$\Updownarrow$$
$$P \quad \text{pertence a uma componente comum de } C \text{ e } D.$$

Seja C uma curva plana projetiva e $P \in C$. A multiplicidade de P em C, que denotamos por $m_C(P)$, é definida como sendo o menor índice de intersecção obtido ao intersectar C com retas que passam por P, ou seja,

$$m_C(P) = \min\{I(P, C \cdot L) \mid L \text{ é uma reta e } P \in L\}.$$

Se $m_C(P) = 1$ dizemos que P é um *ponto simples* ou *ponto regular* ou ainda *ponto não singular* de C. Caso contrário, dizemos que P é um *ponto múltiplo* ou *ponto singular* ou ainda uma *singularidade* de C. Se $m_C(P) = 2$ dizemos que P é um *ponto duplo* de C. Se $m_C(P) = 3$ dizemos que P é um *ponto triplo* de C.

Seja $f \in k[X, Y]$ uma equação afim para a curva C. Podemos escrever, de maneira única, $f = f_m + f_{m+1} + \cdots + f_d$, onde f_i é um polinômio homogêneo em $k[X, Y]$ de grau i e $f_m \neq 0$. Neste caso é fácil verificar que m é a multiplicidade de C em $P = (0, 0)$. Assim, através de uma mudança de coordenadas, podemos ler facilmente a multiplicidade de um ponto de uma curva numa de suas equações afins. Dizemos que uma reta T é uma *reta tangente* a C em P se $I(P, C \cdot T) > m_C(P)$. Caso contrário, dizemos que T é

uma *reta transversal* a C em P. O número de retas tangentes a C em P é no máximo m e, supondo $P = (0, 0)$, as equações afins das retas tangentes a C em P são dadas pelos fatores lineares do polinômio homogêneo f_m. Assim, se P é um ponto regular então há uma única tangente a C em P. Neste caso vamos denotar esta reta tangente por T_P. Um ponto $P \in C$ é dito um *ponto múltiplo ordinário* de C se há exatamente $m = m_C(P)$ tangentes distintas a C em P. Um ponto duplo ordinário é chamado de *nó*.

Dizemos que $P \in C$ é um *ponto de inflexão* de C se P é um ponto regular de C e $I(P, C \cdot T_P) \geq 3$. Neste caso dizemos que T_P é uma *tangente inflexional* de C. No caso em que $I(P, C \cdot T_P) = 3$ dizemos que P é um *ponto de inflexão ordinário* e que T_P é uma *reta tangente inflexional ordinária*. Observe que um ponto de inflexão é um ponto não singular. Naturalmente que se $P \in C$ é um ponto singular de C então, segue da definição que, para qualquer reta L passando por P, tem-se $I(P, C \cdot L) \geq 2$.

Uma observação também interessante é que no Cálculo Diferencial usual os pontos de inflexão de uma curva dada pelo gráfico de uma função duas vezes diferenciável são aqueles pontos onde a segunda derivada muda de sinal. Geometricamente, isso significa que a concavidade da curva muda. No contexto de curvas algébricas, para curvas dadas por gráficos de funções, os pontos de inflexão são pontos onde a segunda derivada se anula. Por exemplo, $P = (0, 0)$ é um ponto de inflexão de $Y = X^3$ em ambos os contextos, mas é ponto de inflexão de $Y = X^4$ apenas no contexto de curvas algébricas. No contexto de curvas algébricas, um ponto de inflexão significa simplesmente que a reta tangente tem intersecção alta com a curva no ponto (não singular) em questão.

1.2 O corpo de funções de uma variedade

Vamos apresentar agora alguns resultados básicos sobre variedades afins e os seus morfismos. A referência básica para os fatos listados é [4].

Seja $F \in k[X_1, \ldots, X_n]$ um polinômio em n indeterminadas sobre k. Um ponto $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ é um *zero* de F se $F(P) = F(a_1, \ldots, a_n) = 0$. Se F não é constante, o conjunto de zeros de F é chamado de *hipersuperfície* definida por F, e é denotada por $V(F)$. Naturalmente uma hipersuperfície em $\mathbb{A}^2$ é uma curva plana afim. Se F é um polinômio de grau 1, $V(F)$ é chamado de *hiperplano* em $\mathbb{A}^n$.

Um conjunto $X \subset \mathbb{A}^n$ é um *conjunto algébrico afim*, ou simplesmente um *conjunto algébrico*, se $X = V(S)$ para algum $S \in k[X_1, \ldots, X_n]$. Se I é o ideal de $k[X_1, \ldots, X_n]$ gerado por S então $V(S) = V(I)$. Assim todo conjunto algébrico de $\mathbb{A}^n$ é o conjunto de zeros de um ideal. Além disso, o Teorema

da Base de Hilbert garante que todo ideal de $k[X_1, \ldots, X_n]$ é finitamente gerado. Assim, os conjuntos algébricos de $\mathbb{A}^n$ são intersecções finitas de hipersuperfícies. Os subconjuntos algébricos de $\mathbb{A}^n$ formam a coleção de conjuntos fechados de uma topologia em $\mathbb{A}^n$ que é a *topologia de Zariski*.

Por outro lado um subconjunto $X \subset \mathbb{A}^n$ define um ideal em $k[X_1, \ldots, X_n]$, a saber:

$$I(X) = \{q(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n] \mid q(P) = 0 \text{ para todo } P \in X\}.$$

Uma das formas do Teorema de Zeros de Hilbert nos diz que, se J é um ideal $k[X_1, \ldots, X_n]$ então $I(V(J)) = \sqrt{J}$, onde

$$\sqrt{J} = \{F \in k[X_1, \ldots, X_n] \mid F^n \in J \text{ para algum } n \in \mathbb{N}\}$$

é o *ideal radical* de J. Assim, há uma correspondência (bijeção) entre conjuntos algébricos de $\mathbb{A}^n$ e ideais radicais de $k[X_1, \ldots, X_n]$. Neste contexto, esta correspondência é a principal razão pela qual podemos utilizar ferramentas da álgebra para estudar objetos geométricos. Uma *variedade afim* ou simplesmente uma *variedade* em $\mathbb{A}^n$ é um conjunto algébrico *irredutível*, que é um conjunto algébrico que não pode ser união de dois de seus subconjuntos algébricos próprios. Na correspondência citada acima, variedades de $\mathbb{A}^n$ correspondem a ideais primos de $k[X_1, \ldots, X_n]$. Considere V uma variedade afim em $\mathbb{A}^n$ e I_V seu ideal primo. O anel quociente

$$\Gamma[V] = \frac{k[X_1, \ldots, X_n]}{I_V}$$

que é um domínio integral, uma vez que I_V é um ideal primo, pode ser visto de maneira natural como um "anel de funções"com domínio V e contradomínio k. Isto é visto da seguinte forma.

Uma *função polinomial em* V é uma função $\varphi : V \to k$ tal que existe um polinômio $G \in k[X_1, \ldots, X_n]$ satisfazendo

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

Se dois polinômios $F, G \in k[X_1, \ldots, X_n]$ são tais que $\varphi(P) = F(P)$ e $\varphi(P) = H(P)$ para todo $P \in V$ então $F(P) - H(P) = 0$ para todo $P \in V$ e, portanto $F - H \in I_V$. Assim, em $\Gamma[V]$ temos $\bar{F} = \bar{H}$, onde $\bar{F}$ denota a classe de equivalência de F módulo I. A partir daí é fácil verificar que há um isomorfismo de anéis entre o anel das funções polinomiais em V e $\Gamma[V]$.

Dados $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ conjuntos algébricos em $\mathbb{A}^n$ e $\mathbb{A}^m$ respectivamente dizemos que uma aplicação $\phi : V \to W$ é *polinomial* se existem m polinômios $G_1, \ldots, G_m \in k[X_1, \ldots, X_n]$ tais que

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

Neste caso dizemos também que ϕ é uma *aplicação regular* de V em W. Naturalmente uma aplicação regular $\phi : V \to W$ induz um homomorfismo de anéis $\phi^* : \Gamma[W] \to \Gamma[V]$ definido por $\phi^*(\varphi) = \varphi \circ \phi$. Na verdade, todo *k-homomorfismo* de *k-álgebra* $\Psi : \Gamma[W] \to \Gamma[V]$ é da forma $\Psi = \phi^*$ para alguma aplicação regular $\phi : V \to W$. Assim, existe uma equivalência entre aplicações regulares de V em W e *k-homomorfismos de k-álgebras entre* $\Gamma[W]$ *e* $\Gamma[V]$. Quando V é uma variedade, $\Gamma[V]$ é um domínio integral. Podemos então considerar o seu corpo de frações que neste caso o denominamos de corpo de funções, isto é, o *corpo de funções* de V é o corpo de frações de $\Gamma[V]$ que denotamos por $k(V)$, ou seja:

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

Observe que quando C é uma curva algébrica irredutível, então C é uma variedade algébrica, assim temos definido $k(C)$ como o corpo de funções de C.

Se $\varphi = \frac{g}{h} \in k(V)$, em princípio φ pode não ser uma função de V em k devido aos zeros de h. No entanto φ é bem definida em $P \in V$ sempre que $h(P) \neq 0$. Então φ está definida fora dos zeros de h que é um conjunto fechado na topologia de Zariski de V. Por abuso de linguagem e pela tradição, mesmo assim, chamamos uma tal φ de *função racional* de V em k. Na verdade, o domínio de φ é um aberto de V. Um ponto $P \in V$ onde $h(P) = 0$, para qualquer representação $\varphi = \frac{g}{h}$, é chamado de *polo* de φ. Por outro lado, se $h(P) \neq 0$, para alguma tal representação, dizemos que φ é *regular* em P.

Fixado um ponto P de V, podemos olhar para o conjunto de todas estas funções que estão definidas em P, isto é, o conjunto das funções que são regulares em P. Isto motiva a definição de anel local num ponto de uma variedade V: O *anel local* de V em $P \in V$ é o conjunto

$$\mathcal{O}_P(V) = \{\varphi \in k(V) \mid \varphi \text{ é regular em } P\}.$$

É fácil ver que $\Gamma[V] \subset \mathcal{O}_P(V) \subset k(V)$ para qualquer $P \in V$. Na verdade, vale que:

$$\Gamma[V] = \bigcap_{P \in V} \mathcal{O}_P(V).$$

O anel $\Gamma[V]$ pode também ser interpretado como um *anel de coordenadas de* V no sentido seguinte. Podemos ver $\Gamma[V]$ como sendo o anel gerado sobre k pelas funções $x_1, x_2, \ldots, x_n$ onde x_i é a classe residual de X_i em $\Gamma(V)$ e pode ser identificada com a função que associa ao ponto $P = (a_1, a_2, \ldots, a_n) \in V$ a sua i-ésima coordenada a_i.

Considere $U \subset V$ um subconjunto aberto (na topologia de Zariski) de V. O conjunto das funções regulares em todos os ponto de U também é um anel

que denominaremos de *anel das funções regulares de U* e o denotaremos por $\Gamma(U)$.

Uma aplicação $\phi : V \to \mathbb{A}^n$ é uma *aplicação racional* de V em $\mathbb{A}^n$ se $\phi(P) = (\varphi_1(P), \ldots, \varphi_n(P))$, onde $\varphi_1, ..., \varphi_n$ são funções racionais de V em k e P está na intersecção dos domínios dessas funções racionais φ_i em V para cada índice i. Mais geralmente, uma *aplicação racional* $\phi : V \to W$ entre duas variedades $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^n$ é uma aplicação racional $\phi : V \to \mathbb{A}^n$ tal que a imagem do domínio de ϕ esteja contido em W. Uma aplicação racional $\phi : V \to W$ é *bi-racional* se existe uma aplicação racional $\psi : W \to V$ tal que $\phi \circ \psi = Id$ e $\psi \circ \phi = Id$ nos seus respectivos domínios de definição. Duas curvas são birracionalmente equivalentes se, e somente se, seus corpos de funções são isomorfos. Toda curva projetiva C tem um modelo não singular $\tilde{C}$, isto é:

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

Estes fatos, como comentado inicialmente, podem ser encontrados em [4]. Precisamos estar atentos pois, mesmo sendo C uma curva plana projetiva, o seu modelo não singular $\tilde{C}$ pode não ser uma curva plana.

Fazemos agora breves comentários sobre morfismos de variedades. Sejam V e W duas variedades (não necessariamente no mesmo espaço afim). Um *morfismo* de V em W é uma aplicação $f : V \to W$ que satisfaz:

1. f é contínua (na topologia de Zariski).

2. Para cada aberto U de W, se $\varphi \in \Gamma(W)$, então

$$f^*(\varphi) = \varphi \circ f \in \Gamma(f^{-1}(U)).$$

Em palavras, f^* transforma aplicações regulares de W em aplicações regulares de V. O diagrama abaixo ilustra a condição (2) acima.

$$\begin{array}{ccc} & f & \\ V & \longrightarrow & W \\ \varphi \circ f \ \searrow & & \swarrow \ \varphi \\ & k & \end{array}$$

Seja $f : C \to D$ um morfismo não constante de curvas projetivas não singulares, correspondente a um homomorfismo de corpos (portanto injetor) f^* de $k(D)$ em $k(C)$. Portanto, podemos ver $k(D) \subset k(C)$, isto é, $k(C)$ é uma

extensão do corpo $k(D)$. O grau desta extensão, $[k(C) : k(D)]$, é denominado o *grau* do morfismo f e é denotado por $\deg(f)$, isto é, $\deg(f) = [k(C) : k(D)]$.

Sejam $P \in C$ e $Q = f(P) \in D$ pontos regulares de C e D respectivamente. Os anéis locais $\mathcal{O}_P(C)$ de C em P e $\mathcal{O}_P(D)$ de D em Q são domínios de valorizações discretas e há um homomorfismo canônico $f^* : \mathcal{O}_Q(D) \to \mathcal{O}_P(C)$ de anéis locais, induzido de forma análoga ao que ocorre no caso de anéis regulares que foi descrito acima. Sejam ν_P e ν_Q as respectivas valorizações de $\mathcal{O}_P(C)$ e $\mathcal{O}_Q(D)$. Suponha que $t \in \mathcal{O}_Q(D)$ seja um *parâmetro local* em Q, isto é, um elemento em $\mathcal{O}_Q(D)$ tal que $\nu_Q(t) = 1$. O número inteiro $e_P = \nu_P(t)$ é chamado *índice de ramificação* de f em P.

- Se $e_P > 1$, dizemos que f é *ramificado* em P.
- Se $e_P = 1$, dizemos que f é *não-ramificado* em P.

Fixe um ponto $Q \in D$. Há uma relação rígida que os índices de ramificação dos pontos $P \in C$ tais que $f(P) = Q$ satisfazem, a saber

$$\sum_{P \in f^{-1}(Q)} e_P = \deg(f).$$

Quando a extensão de corpos $k(C) \mid k(D)$ é galoisiana, com grupo de Galois G, dizemos que f é um *recobrimento galoisiano* e que o grupo G age naturalmente sobre C. Neste contexto vale o resultado seguinte.

Teorema 1 *Sejam C e D duas curvas projetivas não singulares e $f : C \to D$ um recobrimento galoisiano de grau d, com grupo de Galois G.*

1. *Para qualquer $\sigma \in G$, temos $f(\sigma(P)) = f(P)$.*
2. *Se $P \in C$ e $G(P) = \{\sigma \in G \mid \sigma(P) = P\}$ é o subgrupo de G que deixa P fixo então a ordem de $G(P)$ é igual a e_P.*
3. *Se $f(P_1) = f(P_2)$ então $e_{P_1} = e_{P_2}$.*
4. *O índice de ramificação e_P divide o grau d.*

1.3 Dois teoremas clássicos

Nesta seção vamos considerar C uma curva algébrica projetiva irredutível e $f : \tilde{C} \to C$ um morfismo birracional do modelo não singular $\tilde{C}$ em C. Então $K(C) = K(\tilde{C})$ e vamos denotá-lo por K. Como já observamos anteriormente,

se $\tilde{P} \in \tilde{C}$ então o anel local $\mathcal{O}_{\tilde{P}}$ de $\tilde{C}$ em $\tilde{P}$ é um anel de valorização discreta. Seja $\nu_{\tilde{P}}$ a sua valorização. Considere um ponto $P \in C$. A *multiplicidade* do morfismo f em P é o número inteiro não negativo

$$mult_P(f) = \nu_{\tilde{P}} f^*(t_P)$$

onde t_P é um parâmetro local de $\mathcal{O}_{\tilde{P}}$.

Um *divisor* D na curva não singular $\tilde{C}$ é uma soma formal finita

$$D = \sum_{Q \in \tilde{C}} n_Q \, Q$$

onde $n_Q \in \mathbb{Z}$ e $n_Q \neq 0$ exceto para no máximo um número finito de pontos Q.

O *grau* de um divisor é a soma dos seus coeficientes, isto é,

$$\deg \left(\sum_{Q \in \tilde{C}} n_Q \, Q \right) = \sum_{Q \in \tilde{C}} n_Q.$$

O conjunto de todos os divisores em $\tilde{C}$ formam um grupo abeliano aditivo (é exatamente o grupo abeliano livre sobre o conjunto $\tilde{C}$). O divisor $\sum_{Q \in \tilde{C}} \; n_Q \; Q$ é dito *efetivo* se $n_Q \geq 0$ para todo ponto $Q \in \tilde{C}$. Assim, em casos especiais podemos comparar divisores, a saber, escrevemos $\sum n_Q \, Q \succ \sum m_Q \, Q$ se $n_Q \geq m_Q$ para todo $Q \in \tilde{C}$.

Suponhamos que C seja uma curva plana (projetiva irredutível) de grau n. Fixe $P \in C$ e seja $Q \in \tilde{C}$ tal que $f(Q) = P$. Considere uma outra curva projetiva plana G (possivelmente redutível) que não contenha C como componente. Então a desomogenização G_* de G, pode ser vista em $\mathcal{O}_P(\mathbb{P}^2)$. Seja g a classe residual de G^* em $\mathcal{O}_P(C) \subset k(C) = k(\tilde{C})$. Definimos a *ordem de G em Q* como sendo $ord_Q(G) = \nu_Q(g)$. Neste contexto podemos definir o *divisor de G* (em $\tilde{C}$), e o denotamos por $div(G)$, a saber:

$$div(G) = \sum_{Q \in \tilde{C}} ord_Q(G) \, Q,$$

Nesta situação vale que

$$I(P, C \cdot G) = \sum_{Q \in f^{-1}(P)} ord_Q(G)$$

(Veja [4] pg. 182). Assim, podemos ver que

$$\deg(div(G)) = \sum_{P \in C} I(P, C \cdot G).$$

De maneira análoga à discussão acima, dada uma função racional não nula $z \in K$, podemos também definir o *divisor de* z, $div(z)$, como sendo

$$div(z) = \sum_{Q \in \tilde{C}} ord_Q(z)\ Q.$$

Dado $D = \sum_{Q \in \tilde{C}}\ n_Q\ Q$ em $\tilde{C}$ definimos o k-subespaço vetorial de $K = k(\tilde{C})$:

$$L(D) = \{z \in K \mid ord_Q(z) \geq -n_Q \text{ para todo } Q \in \tilde{C}\}.$$

Desta forma uma função racional z em K está em $L(D)$ se $div(z) + D \succ 0$, ou se $z \equiv 0$. Denotamos a dimensão de $L(D)$ por $\ell(D)$. Os espaços $L(D)$, quando D varia, codifica propriedades fundamentais da curva $\tilde{C}$ e o estudo dessas propriedades é um tema central na teoria de curvas algébricas. Um exemplo disso é o gênero de C que é um invariante aritmético que pode ser determinado pelos espaços $L(D)$. A dimensão $\ell(D)$ é finito e se $\deg(D) \geq 0$ então $\ell(D) \leq \deg(D) + 1$. [4]

O gênero de $\tilde{C}$ é caracterizado pelo teorema seguinte:

Teorema 2 *(Teorema de Riemann) Existe uma constante g tal que*

$$\ell(D) \geq \deg(D) + 1 - g$$

para todo divisor D. Esta constante g é um número inteiro não negativo e é chamado **gênero** *de $\tilde{C}$ (ou de K, ou de C).*

De acordo com o gênero g há três classes fundamentais de curvas, a saber:

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

É possível mostrar que existe um inteiro positivo N tal que para todo divisor D com $\deg(D) \geq N$ vale

$$\ell(D) = \deg(D) + 1 - g$$

Também é possível mostrar que se C é uma curva projetiva plana com no máximo pontos múltiplos ordinários. Então o gênero g de C pode ser calculado pela fórmula:

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in C} \frac{r_P(r_P - 1)}{2}.$$

onde n é o grau de C e $r_P = m_P(C)$ é a multiplicidade de P em C. Em particular, para toda curva projetiva plana não singular de grau n o seu gênero é

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

As retas e as cônicas irredutiveis são exemplos de curvas com gênero $g = 0$ e as cúbicas não singulares possuem gênero $g = 1$. Já as quárticas planas não singulares têm gênero $g = 3$, observe que não existe curva plana projetiva não singular com gênero $g = 2$.

Seja f uma função racional sobre a curva algébrica C. Considere a aplicação $\phi : C \longrightarrow \mathbb{P}^1$ definida por

$$\begin{array}{rcl} \phi : C & \longrightarrow & \mathbb{P}^1 \\ P & \mapsto & (1 : f(P)) \end{array}$$

Observe que se P é um pólo de f, a aplicação acima não está bem definida. No entanto, neste caso, podemos definir ϕ em P por

$$\phi(P) = \left(\frac{1}{f(P)} : 1\right) = (0 : 1) \in \mathbb{P}^1.$$

A aplicação assim definida é um morfismo e usaremos o termo **aplicação regular** em vez de morfismo algébrico.

Se conhecemos o índice de ramificação nos pontos de ramificação P e o grau $d = \sum e_P$ da aplicação ϕ, podemos obter o gênero de C. Este é o resultado apresentado no teorema a seguinte:

Teorema 3 *(Riemann-Hurwitz) Seja $\phi : C \to \mathbb{P}^1$ uma aplicação regular sobrejetiva. Sejam $d = grau(\phi)$, e_P o índice de ramificação de ϕ no ponto de ramificação P e $R = \{P \in C \mid P$ é ponto de ramificação de $\phi\}$. Então o gênero g de C satisfaz:*

$$2g - 2 = -2d + \sum_{P \in R} (e_P - 1).$$

Considere o exemplo seguinte. Seja ϕ a aplicação regular

$$\begin{array}{rcl} \phi : \mathbb{P}^1(\mathbb{C}) & \longrightarrow & \mathbb{P}^1(\mathbb{C}) \\ (a_0 : a_1) & \mapsto & (a_0^n : a_1^n) \end{array}$$

Esta é uma aplicação determinada pela função racional $x^n = (\frac{x_1}{x_0})^n$. Para distinguir as duas retas projetivas, denotemos por $(x_0 : x_1)$ as coordenadas homogêneas do $\mathbb{P}^1(\mathbb{C})$ da esquerda e por $(y_0 : y_1)$ as coordenadas homogêneas

do $\mathbb{P}^1(\mathbb{C})$ da direita. Como parâmetros locais para o ponto $(1:0)$ podemos tomar $x = \frac{x_1}{x_0}$ e $y = \frac{y_1}{y_0}$, respectivamente, e representamos ϕ por

$$y = x^n.$$

Assim $(1:0)$ é um ponto de ramificação de índice n. Para um ponto $(1:a)$, $a \neq 0$, tome b tal que $b^n = a$. Podemos usar os parâmetros locais $s = x - b$ para $(1:b)$ e $t = y - a$ para $(1:a)$. Assim, temos ϕ representada por $t = -a + (s+b)^n$ e $(1:b)$ não é um ponto de ramificação. No ponto $(1:0)$. Fixando $u = \frac{x_0}{x_1}$ e $v = \frac{y_0}{y_1}$, representamos ϕ por

$$v = u^n.$$

Isto mostra que $(0:1)$ é um ponto de ramificação de índice n. Como o grau de ϕ é n, temos assim $-2n + 2(n-1) = -2$, e portanto, a fórmula de Riemann-Hurwitz é verificada.

A fórmula de Riemann-Hurwitz generalizada é dada pelo teorema:

Teorema 4 (Generalização do Teorema de Riemann-Hurwitz) *Seja $\phi : \tilde{C} \to C$ uma aplicação regular sobrejetiva, onde $\tilde{C}$ e C são curvas algébricas de gênero $\tilde{g}$ e g respectivamente . Então*

$$2\tilde{g} - 2 = d(2g-2) + \sum(e_i - 1)$$

onde d é o grau de ϕ e cada e_i é o índice de ramificação de ϕ nos pontos de ramificação P_i de ϕ.

Além dos teoremas de Riemann e de Riemann-Hurwitz vamos precisar utilizar dois resultados que podem ser encontrados em [13]. São eles:

Proposição 1 *: Seja G um subgrupo transitivo do grupo simétrico S_n que é gerado por ciclos de ordem prima.*

1. *Se G contém uma transposição então $G = S_n$*
2. *Se G contém um 3-ciclo, então $G = A_n$ ou $G = S_n$, onde A_n é o subgrupo de S_n das permutações pares.*

Proposição 2 *: Seja $f : C \to \mathbb{P}^1$ um recobrimento galoisiano regular com grupo de Galois G, não ramificado no ∞. Então G é gerado pelos subgrupos inerciais de pontos finitos e seus conjugados.*

1.4 Projeções em espaços projetivos

Sejam E e E' dois subspaços lineares disjuntos de $\mathbb{P}^n$ de dimensões m e $n-m-1$ respectivamente. Seja $P \in \mathbb{P}^n \backslash E$ e vamos considerar o espaço linear $L = \langle E, P \rangle$ gerado por E e P. Este espaço intersecta E' em apenas um ponto, e define portanto uma aplicação racional

$$\begin{array}{rccc} \pi_E : & \mathbb{P}^n & \longrightarrow & E' \\ & P & \mapsto & L \cap E' \end{array}$$

que é regular em $\mathbb{P}^n \backslash E$. Podemos escolher, adequadamente, coordenadas em $\mathbb{P}^n$ de tal maneira que

$$\begin{array}{rccc} \pi_E : & \mathbb{P}^n & \longrightarrow & E' \\ & (P_0 : P_1 : \ldots : P_n) & \mapsto & (P_0 : \ldots : P_{n-m-1} : 0 : \ldots : 0) \end{array}$$

onde o espaço E é dado pelas equações $X_0 = X_1 = \ldots = X_{n-m-1} = 0$ e o espaço E' pelas equações $X_{n-m} = X_{n-m+1} = \ldots = X_n = 0$.

Se X é uma variedade qualquer de $\mathbb{P}^n$, que não está contida em E, a restrição de π_E a X também define uma aplicação racional $\pi : X \longrightarrow E'$. Quando $E \cap X = \emptyset$, esta aplicação é regular.

Seja C uma curva em $\mathbb{P}^n$ e P um ponto regular de C. Então o anel local $\mathcal{O}_P(C)$ é um anel de valorização discreta. Seja ν_P a sua valorização. Se L é um subespaço linear de $\mathbb{P}^n$, definido por formas lineares $l_0, l_1, \ldots, l_r$, então o índice de intersecção de C com L em P é o inteiro não negativo

$$I(P, C \cdot L) = \min\{\nu_P(l_0), \ldots, \nu_P(l_r)\}$$

Considere um subespaço linear E de $\mathbb{P}^n$, como acima, tal que $C \not\subset E$. Temos então a proposição seguinte:

Proposição 3 *Sejam P um ponto regular de C e $L = \langle E, P \rangle$. Se $P \notin E$ e e_P é o índice de ramificação de π_E em P, então*

$$e_P = I(P, C \cdot L)$$

Demonstração: Sejam $L_0, L_1, \ldots, L_{n-m-1}$ formas lineares que definem o subespaço linear L. Como $E \subset L$ e tem codimensão 1 em L, existe uma forma linear L_{n-m} tal que $L_0, \ldots, L_{n-m-1}, L_{n-m}$ definem E. Tem-se então que a projeção $\pi_E : C \to \mathbb{P}^{n-m}$ é dada por

$$\pi_E(P) = (L_0(P) : \ldots : L_{n-m-1}(P) : L_{n-m}(P))$$

e portanto $\pi_E(P) = (0 : \ldots : 0 : L_{n-m}(P))$. Defina $Y := \pi_E(C)$. Seja $a_0 X_0 + \cdots + a_{n-m-1} X_{n-m-1}$ um hiperplano genérico que passa por $\pi_E(P)$.

Sendo o hiperplano genérico, ele é transversal à curva Y em $\pi_E(P)$, e a sua imagem em $\mathcal{O}_P(\pi_E(P))$ é um parâmetro local t' de Y em $\pi_E(P)$. Seja t um parâmetro local em P e suponhamos que $P \in U \cap C$, onde U é o aberto $X_n \neq 0$. Denote por

$$x_0(t) = \frac{X_0}{X_n}, \ldots, x_n(t) = \frac{X_{n-1}}{X_n},$$

em $\mathcal{O}_P(C)$, temos

$$\begin{aligned} \pi_E^*(t') &= \pi_E^*(a_0X_0 + \cdots + a_{n-m-1}X_{n-m-1}) \\ &= a_0L_0(x_0(t), \ldots, x_{n-1}(t), 1) + \cdots + a_{n-m-1}L_{n-m-1}(x_0(t), \ldots, x_{n-m-1}(t), 1). \end{aligned}$$

Sendo o hiperplano genérico, temos que

$$\begin{aligned} e_P &= ord_t(a_0L_0(x_0(t), \ldots, x_{n-1}(t), 1) + \cdots + a_{n-m-1}L_{n-m-1}(x_0(t), \ldots, x_{n-1}(t), 1)) \\ &= \min_{i=0,\ldots,n-m-1}\{ord_i(L_i(x_0(t), \ldots, x_{n-1}(t), 1))\} \ = \ I(P, C \cdot L). \end{aligned}$$

Corolário 1 *Seja P um ponto regular de C e T_PC a reta tangente a C em P. O ponto P é ponto de ramificação de π_E se, e somente se, $T_PC \cap E \neq \emptyset$.*

Um caso especial é quando o espaço E tem dimensão $m = 0$, isto é, a projeção é centrada num ponto. Este é o caso que estamos estudando neste trabalho. Observe que qualquer projeção pode ser obtida através de uma sucessão de projeções a partir de pontos.

Capítulo 2

O Grupo de Galois

Neste capítulo vamos fazer uma descrição completa dos possíveis grupos que ocorrem como grupos de Galois para fechos normais de extensões de corpos de grau quatro em característica zero. Isto será fundamental para o estudo dos pontos de Galois externos das curvas quárticas em $\mathbb{P}^2$. Durante todo este capítulo, como antes, vamos supor K um corpo de característica zero.

A questão da determinação do grupo de Galois de um polinômio a partir de seus coeficientes é um assunto clássico e despertou interesse ao longo do século XX. Há trabalhos de matemáticos como *O. Hölder, W. Krull* e *B. L. Vander Waerden* que apresentam algorítmos para isto. Os métodos que lá aparecem são muito trabalhosos e de pouco interesse prático. No entanto, mais recentemente, com a chegada da computação algébrica este assunto tem despertado interesse.

2.1 O critério

O teste que apresentamos a seguir pode ser usado para determinar o grupo de Galois de qualquer polinômio irredutível de grau 4 sobre qualquer corpo de característica zero. Ele é baseado no mesmo método de redução para determinar o Grupo de Galois de um polinômio de grau três utilizado por I. Kaplansky [9]. No entanto evitamos a necessidade de verificar a irredutibilidade do polinômio sobre extensões do corpo de base para distinguir entre os casos dos grupos de Galois cíclicos e diedrais.

Estamos interessados em estudar o fecho normal de uma extensão de grau quatro de K, portanto, naturalmente, K não é algebricamente fechado. Outra observação que também é imediata é que os possíveis grupos de Galois que irão surgir são subgrupos de S_4, o grupo das simetrias de 4 objetos, cuja

ordem é 24.

Este assunto é antigo e pode ser encontrado em alguns textos clássicos de Álgebra. Recentemente foi publicado o artigo de *L. Kappe* e *B. Warren* [10], no qual estamos nos baseando. A razão de incluirmos este assunto na dissertação é para torná-la auto-suficiente em relação a este tópico.

Seja L uma extensão de grau 4 de K e seja M o seu fecho galoisiano (em algum corpo algebricamente fechado que contenha K). Pelo teorema do elemento primitivo, existe um elemento $\alpha \in L$, de grau quatro, tal que $L = K(\alpha)$. Seja $p(X) \in K[X]$ o polinômio mínimo de α sobre K que é naturalmente um polinômio irredutível de grau quatro. Escreva

$$p(X) = \prod_{1 \leq i \leq 4} (X - \alpha_i) = X^4 + aX^3 + bX^2 + cX + d$$

onde $a, b, c, d \in K$. Sejam $\alpha_1 = \alpha, \alpha_2, \alpha_3, \alpha_4$ as raízes de $p(X)$. Então $M = K[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$, uma vez que M é o corpo de fatoração de K.

Vamos denotar por $K^2 = \{a^2 \mid a \in K\}$ o conjunto de todos os quadrados de elementos de K. Como as raízes de $p(X)$ são distintas, o grupo de Galois $G = Gal(F|K)$ age transitivamente sobre as quatro raízes e portanto deve ser isomorfo a um dos subgrupos normais de S_4 que são um dos cinco subgrupos abaixo:

1. O grupo S_4 das permutações de 4 objetos que tem ordem 24;
2. O subgrupo A_4 das permutações pares de S_4 que tem ordem 12;
3. O subgrupo diedral D_4 das simetrias do quadrado que tem ordem 8;
4. O subgrupo de Klein V_4 que tem ordem 4 e não é cíclico;
5. O subgrupo Z_4 cíclico de ordem 4;

Considere o seguinte polinômio associado ao polinômio $p(X)$, que é o *polinômio cúbico revolvente* de $p(X)$ estudado originalmente por Lagrange:

$$r(X) = X^3 - bX^2 + (ac - 4d)X - (a^2d - 4bd + c^2) \in K[X].$$

É fácil verificar que as raízes de $r(X)$ são:

$$t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4; \quad t_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \quad \text{e} \quad t_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Seja $E = K[t_1, t_2, t_3]$ o corpo de fatoração de $r(X)$ sobre K. Naturalmente E é um subcorpo de M. Também é imediato verificar que $p(X)$ e $r(X)$ possuem o mesmo discriminante:

$$D = \prod_{1 \leq i < j \leq 4} (\alpha_i - \alpha_j)^2 = \prod_{1 \leq i < j \leq 3} (t_i - t_j)^2$$

e que $D = -4b^3A + b^2B^2 + 18dBA - B^3 - 27A^2$, onde $A = a^2d + c^2 - 4bd$ e $B = ac - 4d$. Temos então o teorema seguinte:

Teorema 5 *Mantendo as mesmas notações estabelecidas acima temos que*

1. *$Gal(M|K) \cong S_4$ se, e somente se, $r(X)$ é irredutivel sobre K e $D \notin K^2$, isto é, D não é um quadrado em K.*

2. *$Gal(M \mid K) \cong A_4$ se, e somente se, $r(X)$ é irredutivel sobre K e $D \in K^2$, isto é, D é um quadrado em K.*

3. *$Gal(M \mid K) \cong V_4$ se, e somente se, $r(X)$ se fatora em fatores lineares em $K[X]$.*

4. *$Gal(M \mid K) \cong \mathbb{Z}_4$ se, e somente se, $r(X)$ tem exatamente uma raiz β em K e o polinômio*

$$h(X) = (X^2 - \beta X + d) \cdot (X^2 + aX + (b - \beta))$$

   se fatora em $E[X]$.

5. *$Gal(M \mid K) \cong D_4$ se, e somente se, $r(X)$ possui exatamente uma raiz em K e o polinômio $h(X)$ definido em (4) não se fatora em $E[X]$.*

Demonstração: Vamos utilizar as notações usuais para escrever permutações de $\{1, 2, 3, 4\}$. Assim o grupo de Klein é escrito como

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \subset S_4$$

V_4 é o único grupo de 4 elementos em S_4 que não é cíclico, portanto ele tem que ser normal em S_4. Por outro lado, o corpo de fatoração E da cúbica resolvente $r(X)$ está contido em M. Como $p(X)$ é irredutível, portanto com raízes distintas, o seu discriminante D é não nulo. Segue que $r(X)$ também possui raízes distintas, pois o seu discriminante também é D. Além disso, uma permutação dos α_i, com $i = 1, 2, 3, 4$, fixa as três raízes t_1, t_2 e t_3 de $r(X)$ se, e somente se, ela age transitivamente nos índices $i's$ de α_i. Dessa forma $Gal(M|E) = Gal(M|K) \cap V_4$ e podemos ver que:

1. O polinômio $r(X)$ se decompõe em fatores lineares em $K[X]$ se, e somente se, $Gal(M|K) \subset V_4$.

2. O polinômio $r(X)$ é irrudutível em $K[X]$ se, e somente se,

$$|Gal(M|K)| = |Gal(M|E)| \cdot |Gal(E|K)| \text{ é múltiplo de 3.}$$

Observe que $|Gal(M|K)|$ é um múltiplo de 4, consequentemente a sua ordem é no mínimo 4. Desta forma, no primeiro caso, temos que $Gal(M|K) \cong V_4$. Isto mostra *(3)*. No segundo caso temos que $|Gal(M|K)|$ é múltiplo de 3 e 4, logo também múltiplo de 12. Assim,

$$Gal(M|K) \cong A_4 \quad \text{ou} \quad Gal(M|K) \cong S_4.$$

Olhando a expressão de D em termos das raízes α_i e lembrando que $D \in K$, segue daí que $Gal(M|E)$ será isomorfo a A_4 se, e somente se, D for uma raíz quadrada em K. Isto mostra *(1)* e *(2)*.

Suponha agora que $r(X)$ tenha exatamente uma raíz β em K. Então podemos supor que esta é a raíz $\beta = t_1 = (\alpha_1\alpha_2 + \alpha_3\alpha_4)$. Considere então o polinômio

$$h(X) = (X^2 - \beta X + d) \cdot (X^2 + aX + (b - \beta)) \quad \text{em} \quad K[X].$$

As raízes do primeiro fator $X^2 - \beta X + d$ são $\alpha_1\alpha_2$ e $\alpha_3\alpha_4$. Já as raízes do segundo fator $X^2 + aX + (b - \beta)$ são $\alpha_1 + \alpha_2$ e $\alpha_3 + \alpha_4$. Se $Gal(F \mid K) \cong \mathbb{Z}_4$ então E é a única extensão quadrática de K contida em M. Desta forma, cada um dos fatores quadráticos de $h(X)$ se decompõem em E.

Reciprocamente, suponha que $h(X)$ se decomponha completamente em $E[X]$. Então o polinômio $s(X) = X^2 - (\alpha_1 + \alpha_2)X + (\alpha_1\alpha_2)$ que tem raízes α_1 e α_2 tem coeficientes em E. Seja M_1 o corpo de fatoração de $s(X)$ sobre E. Então $E \subset M_1 \subset M$, e portanto os elementos α_1, α_2, t_1, t_2, t_3 ($t_1 = \beta$) estão em M_1. Como $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = a$, segue que $(\alpha_3 + \alpha_4) = -a - (\alpha_1 + \alpha_2)$, e portanto $(\alpha_3 + \alpha_4) \in M_1$. Como $(\alpha_1 - \alpha_2) \neq 0$ e $(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) = (t_2 - t_3)$ vemos que $(\alpha_3 - \alpha_4)$ está em M_1 e, consequentemente, α_3 e $\alpha_4 \in M_1$. Isto permite concluir que $M_1 = M$ e logo, $|Gal(M \mid M_1)| = 1$. Assim,

$$\begin{array}{rcl} |\mathbb{Z}_4| & \leq & |Gal(M \mid K)| \\ & = & |Gal(M \mid M_1)| \cdot |Gal(M_1 \mid E)| \cdot |Gal(E \mid K)| \quad \leq \quad 1 \cdot 2 \cdot 2 = 4 \\ & < & |D_4| \end{array}$$

Segue que $Gal(M|K) \cong \mathbb{Z}_4$. Isto mostra *(4)*. A condição para D_4 segue por exclusão. □

2.2 Polinômios biquadrados

Vamos aplicar o critério que acabamos de estabelecer para encontrar o grupo de Galois de um polinômio irredutível *biquadrado*, isto é, um polinômio da forma $p(X) = X^4 + bX^2 + d \in K[X]$. Primeiramente vamos estabelecer um critério de irredutibilidade para tais polinômios.

Lema 1 *Sejam* $p(X) = X^4+bX^2+d \in K[X]$ *um polinômio e* $\{\alpha,\ -\alpha,\ \beta,\ -\beta\}$ *suas raízes (em algum corpo algebricamente fechado que contenha* K*). As três condições seguintes são equivalentes.*

1. $p(X)$ *é irredutível em* $K[X]$*;*
2. $\alpha^2,\ \alpha+\beta,\ \alpha-\beta \notin K$*;*
3. $b^2-4d,\ -b+2\sqrt{d},\ -b-2\sqrt{d} \notin K^2$*.*

Demonstração: Observe que o polinômio $p(X)$ não pode ter um fator irredutível de grau 3 uma vez que $p(X)$ tem raízes simétricas. Segue que $p(X)$ se fatora em $K[X]$ se, e somente se, uma das 3 fatorações abaixo ocorre em $K[X]$:

- $p(X) = (X^2-\alpha^2)(X^2-\beta^2)$
- $p(X) = [X^2-(\alpha+\beta)X+\alpha\beta]\cdot[(X^2+(\alpha+\beta)X+\alpha\beta)]$
- $p(X) = [X^2-(\alpha-\beta)X-\alpha\beta]\cdot[(X^2+(\alpha-\beta)X-\alpha\beta)]$

Imediatamente vemos que (*2*) implica (*1*). As relações básicas entre coeficientes e raízes nos fornecem

$$\alpha^2+\beta^2 = -b \quad \text{e} \quad \alpha^2\beta^2 = d.$$

Juntando estas relações com

$$(\alpha+\beta)^2 = -b+2\alpha\beta \quad \text{e} \quad (\alpha-\beta)^2 = -b-2\alpha\beta,$$

obtemos que $\alpha^2 \in K$ se, e somente se, $\beta^2 \in K$ e se $\alpha \pm \beta \in K$ então $\alpha\beta \in K$. Portanto (*1*) implica (*2*). A equivalência entre (*2*) e (*3*) pode ser vista como segue. Como consequência das relações básicas obtemos:

1. $(\alpha+\beta)^2 = -b+2\alpha\beta \quad \text{e} \quad (\alpha-\beta)^2 = -b-2\alpha\beta,$
2. $(b+2\alpha^2)^2 = (\alpha^2-\beta^2)^2 = (\alpha+\beta)^2(\alpha-\beta)^2 = b^2-4d.$

Portanto $\alpha \pm \beta \in K$ se, e somente se, $-b \pm 2\sqrt{d} \in K^2$. Analogamente, $\alpha^2 \in K$ é equivalente a $b^2-4d \in K^2$. □

Teorema 6 *Seja* $p(X) = X^4+bX^2+d \in K[X]$ *um polinômio biquadrado e* $\{\alpha,\ -\alpha,\ \beta,\ -\beta\}$ *suas raízes (em algum corpo algebricamente fechado que contenha* K*). Se* M *é o corpo de fatoração de* $p(X)$ *sobre* K *então,*

1. $Gal(M|K) \cong V_4$ *se, e somente se,* $d \in K^2$ *se, e somente se,* $\alpha\beta \in K$*;*

2. *$Gal(M|K) \cong \mathbb{Z}_4$ se, e somente se, $d(b^2 - 4d) \in K^2$ se, e somente se, $K(\alpha\beta) = K(\alpha^2)$;*

3. *$Gal(M|K) \cong D_4$ se, e somente se, $d \notin K^2$ e $d(b^2 - 4d) \notin K^2$ se, e somente se, $\alpha\beta \notin K(\alpha^2)$;*

Demonstração: A resolvente cúbica de $p(X)$ é $r(X) = (x - b)(x^2 - 4d)$. Assim, pelo Teorema 5, o grupo de Galois $Gal(M|K)$ de $p(X)$ é isomorfo a um dos grupos D_4, $\mathbb{Z}_4$ ou V_4 e, além disso, $Gal(M|K) \cong V_4$ se, e somente se, $r(X)$ se fatora completamente em $K[X]$. Mas isto é claramente equivalente a $\sqrt{d} = \alpha\beta \in K$, o que prova o ítem *(1)*. Agora, suponha que $\sqrt{d} \notin K$. Então $r(X)$ tem apenas uma raiz, $t_1 = b$, em K e, caímos então em um dos casos *(4)* ou *(5)* do Teorema 5. O polinômio $h(X)$, que surge na prova do Teorema 5, associado ao polinômio $p(X)$ é $h(X) = (X^2 - bX + d)X^2$. As raízes não nulas de $p(X)$ são

$$u = \frac{1}{2}\left(b + \sqrt{b^2 - 4d}\right) = b + \alpha^2 \quad \text{e} \quad v = \frac{1}{2}\left(b - \sqrt{b^2 - 4d}\right) = b + \beta^2.$$

Como $p(X)$ é irredutível em $K[X]$, pelo Lema 1, u e v não estão em K uma vez que $\alpha^2 \notin K$. Pelo Teorema 5, $Gal(F \mid K) \cong \mathbb{Z}_4$ se, e somente se, $h(X)$ se fatora em $E = K(\sqrt{d})$. Mas isto é equivalente a dizer que $K(\sqrt{b^2 - 4d}) = K(\sqrt{d})$, ou equivalentemente, $K(\alpha^2) = K(\alpha\beta)$. Ora, duas extensões quadráticas de um corpo são iguais se, e somente se, o produto de seus discriminantes é um quadrado nesse corpo. Logo, a última condição é eqüivalente a $d(b^2 - 4d) \in K^2$. Isto prova o ítem *(2)*. O terceiro ítem segue por exclusão. □

2.3 Exemplos

Nos exemplos a seguir, vamos seguir as notações estabelecidas no início do capítulo. Em todos eles vamos considerar $K = \mathbb{Q}$.

Exemplo 1

Considere o polinômio $p(X) = X^4 - 4X^3 + 4X^2 + 6 \in \mathbb{Q}[X]$. Claramente $p(X)$ é irredutível em $\mathbb{Q}[X]$. A resolvente (de grau 3) associada ao polinômio $p(X)$ é $r(X) = r_p(X) = X(X^2 - 4X - 24)$ e $E = \mathbb{Q}[\sqrt{7}]$. O polinômio $h(X)$ associado ao polinômio $p(X)$ que surge na prova do Teorema (5) é $h(X) = (X-2)^2(X^2+6)$ que claramente não se fatora em E, portanto, pelo critério temos que $Gal(M|\mathbb{Q}) \cong D_4$.

Exemplo 2

O polinômio $q(X) = X^4 + 4X^3 + 4X^2 + 6 \in \mathbb{Q}[X]$ também é claramente irredutível em $\mathbb{Q}[X]$. A sua resolvente é $r(X) = X(X-2)(X-4)$. Então, segue imediatamente do critério que $Gal(M|\mathbb{Q}) \cong V_4$.

Exemplo 3

O polinômio $f(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ é irredutível em $\mathbb{Q}[X]$. Neste caso, é fácil concluir que $Gal(M|\mathbb{Q}) \cong \mathbb{Z}_4$ pois $M = \mathbb{Q}(\alpha)$ onde α é uma raiz quinta primitiva da unidade. No entanto, também podemos aplicar o critério para concluir isto. Observe que a resolvente associada ao polinômio $f(X)$ é $r(X) = X(X^2 + X - 1)$ e o polinômio $h(X)$ associado ao polinômio $f(X)$ que surge na prova do Teorema 5 é $h(X) = (X-1)^2(X^2 + X - 1)$. Então, pelo critério, $Gal(M|\mathbb{Q}) \cong \mathbb{Z}_4$ pois $r(X)$ tem apenas uma raiz em $\mathbb{Q}$ e $r(X)$ e $g(X)$ possuem o mesmo corpo de fatoração.

Exemplo 4

Seja p um número inteiro primo positivo. Vamos estudar o polinômio bi-quadrático $f(X) = X^4 + pX^2 + p \in \mathbb{Q}[X]$. Vemos imediatamente que $f(X)$ é irredutível em $\mathbb{Q}[X]$. A sua resolvente é $r(X) = X^3 - 4pX - p^2$. Como $r(X)$ é mônico ele é irredutível em $\mathbb{Q}[X]$ se, e somente se, ele não possui raízes em $\mathbb{Z}$. Assim as possíveis raízes de $r(X)$ são os divisores de p^2. Testando cada divisor vemos que $r(X)$ é irredutível em $\mathbb{Q}[X]$ se, e somente se, $p \notin \{3, 5\}$. Assim, observando que o seu discriminante é $D = -p^3(99p - 64) < 0$, pelo critério, obtemos que se $p \neq 3, 5$ então $Gal(M|\mathbb{Q}) \cong S_4$.

- No caso em que $p = 3$ então temos $r(X) = (X + 3)(X^2 - 3X - 3)$ e $E = \mathbb{Q}(\sqrt{21})$. Logo, $g(X) = (X^2 + 3X + 3)(X^2 + 3)$ não tem raízes reais, portanto não se fatora sobre E que está contido em $\mathbb{R}$. Assim, pelo critério, $Gal(M|\mathbb{Q}) \cong D_4$.

- No caso em que $p = 5$ então $r(X) = (X-3)(X^2+5X+5)$ e $E = \mathbb{Q}(\sqrt{5})$. Temos que $g(X) = (X^2 - 5X + 5)(X^2 - 5)$ se fatora em E. Segue do critério que $Gal(M|\mathbb{Q}) \cong \mathbb{Z}_4$.

Capítulo 3

Quárticas planas não singulares.

3.1 Contextualização.

O principal objetivo dessa monografia é estudar pontos de Galois externos de uma curva quártica plana projetiva não singular obtidos ao fazermos uma projeção central, a partir de um ponto fora da curva, no plano projetivo, sobre uma reta projetiva. Este processo dá origem a uma extensão de corpos cujo corpo de base é um corpo racional (corpo de funções da reta sobre a qual a curva está sendo projetada) e o corpo de cima é o corpo de funções da quártica. A quártica de Fermat é um exemplo protótipo dessa situação.

Considere a quártica de Fermat C que é uma curva não singular, cuja equação pode ser dada pelo polinômio

$$F(X,Y,Z) = X^4 + Y^4 - Z^4 \in \mathbb{C}[X,Y,Z].$$

Considere o ponto $P = (1:0:0)$ e a reta L dada por $X = 0$. Claramente $P \notin C$ e podemos identificar essa reta L com $\mathbb{P}^1$ dentro de $\mathbb{P}^2$ dado por $\mathbb{P}^1 = \{(0:b:c) \mid b,c \in \mathbb{C}, b \neq 0 \text{ ou } c \neq 0\}$. Defina então a projeção

$$\begin{array}{cccc} \pi: & C & \longrightarrow & \mathbb{P}^1 \\ . & (a:b:c) & \mapsto & (0:b:c) \end{array}$$

Seja $L'_{(b:c)}$ a reta que passa por P e $(0:b:c)$, a saber, $L'_{(b:c)} : cY - bZ = 0$, e temos $\pi(a:b:c) = L \cap L'_{(b:c)} = \{(0:b:c)\}$. Em coordenadas afins, π é a projeção de $C_* = \{(a,b) \mid b^4 = 1 - a^4\}$ sobre o eixo Y, isto é, $\pi(a,b) = b$. Para $(b:c) \in \mathbb{P}^1$ qualquer, existem no máximo quatro pontos Q_1, Q_2, Q_3 e Q_4 tais que $\pi(Q_i) = (0:b:c)$ com $i \in \{1,2,3,4\}$, a saber, $Q_i = (a_i:b:c)$, onde os a_i são as raízes da equação $x^4 + b^4 - c^4 = 0$. Se $(b:c)$ não é um

ponto no infinito de $\mathbb{P}^1$, isto é, $c \neq 0$, então podemos supor $c = 1$ e, neste caso, os a_i são as raízes da equação $x^4 = 1 - b^4$, em particular, quando $b^4 = 1$ a equação se reduz a $x^4 = 0$. Do ponto de vista geométrico isto significa que dado $(b : c) \in \mathbb{P}^1$ tem-se que $\pi^{-1}(b : c)$ são, no máximo, quatro pontos na curva C. Do ponto de vista algébrico, temos que π induz uma inclusão do corpo de funções de $\mathbb{P}^1(\mathbb{C})$ no corpo de funções de C, isto é, $k(\mathbb{P}^1(\mathbb{C})) \subset k(C)$. Veja que $k(\mathbb{P}^1(\mathbb{C})) = k(y)$ e $k(C) = k(x, y) = k(y)[x]$, onde $x^4 = 1 - y^4$, logo $k(C) \mid k(\mathbb{P}^1(\mathbb{C}))$ é a extensão de corpos $k(x, y) \mid k(y)$ de grau 4. Concluímos que informações geométricas da projeção π podem ser obtidas da extensão $k(y)[x] \mid k(y)$. Isto é o que faremos para estudar os pontos de Galois, associados a uma curva C, que definiremos a seguir. Após discutirmos a teoria voltaremos a este exemplo e vamos verificar que associados à quártica de Fermat:

1. Há 3 pontos de Galois externos, a saber $P_1 = (1 : 0 : 0)$, $P_2 = (0 : 1 : 0)$ e $P_3 = (0 : 0 : 1)$.

2. Há 12 pontos P (externos a C) cujo grupo de Galois, G_P, do fecho normal de $k(C)$ sobre o corpo racional $k(l)$ é isomorfo ao grupo diedral D_4.

3. Não há ponto P para o qual o grupo de Galois G_P seja isomorfo ao subgrupo A_4 das permutações pares de S_4.

Conseqüentemente teremos que G_P é isomorfo a S_4 exceto para 15 pontos.

Relembramos que estamos admitindo k um corpo algebricamente fechado e de característica zero. Seja $K \mid k$ um corpo de funções algébricas em uma variável sobre k.

Um subcorpo intermediário K' da extensão $K \mid k$ é chamado *subcorpo racional maximal* se K' é racional e, para qualquer subcorpo intermediário racional K'' contendo K', isto é, $K' \subseteq K'' \subseteq K$, tem-se necessariamente $K'' = K'$. Vamos fixar então um subcorpo racional maximal K_m de K. Após estudarmos os pontos de Galois associados à curva C, nosso objetivo será estudar a estrutura da extensão $K \mid K_m$, mais especificamente estamos interessados em responder à pergunta:

Se L é o fecho galoisiano de $K \mid K_m$, qual é o grupo de Galois da extensão $L \mid K_m$?

Suponha que $\deg(C) = d$ e considere uma projeção π_P de C sobre uma reta l com centro em $P \notin C$ (Ver pg 76 Namba), então temos uma extensão de corpos

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

Observe que $k(\mathbb{P}^1)$ é um subcorpo racional de $k(C)$. É fácil verificar que esta extensão de corpos independe da reta l sobre a qual estamos projetando C, no entanto depende do ponto P do qual estamos projetando a curva. Portanto denotaremos o corpo de funções $k(\mathbb{P}^1)$ por K_P e L, o fecho galoisiano de $k(C) \mid K_P$, por L_P.

Definição 1 *Na situação acima, o ponto $P \in \mathbb{P}^2$ é chamado ponto de Galois ou ponto galoisiano da curva C se $k(C) \mid K_P$ é uma extensão galoisiana, isto é, $L_P = k(C)$.*

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

3.2 Projeção de uma quártica.

Queremos estudar o grupo $G_P = Gal(L_P|K_P)$ no caso da projeção central de uma quártica projetiva plana não singular C com centro $P \in \mathbb{P}^2 \backslash C$. Então, nos concentraremos daqui por diante na prova do teorema enunciado abaixo que é o principal resultado dessa monografia. Denotaremos por $\delta(C)$ a quantidade de pontos de Galois de C e por $g(P)$ o gênero da curva $\tilde{C}_P$ ou, equivalentemente, o gênero do corpo de funções $L_P \mid k$.

Teorema 7 . *Seja C uma quártica projetiva não singular em $\mathbb{P}^2(\mathbb{C})$ e seja $P \in \mathbb{P}^2 \backslash C$. Então, $G_P = Gal(L_P|K_P)$ é isomorfo a um dos seguintes grupos:*

1. *O grupo das permutações de quatro objetos, S_4.*
2. *O subgrupo de S_4 das permutações pares, A_4.*
3. *O grupo diedral de ordem 8, D_4.*
4. *O grupo cíclico de ordem 4, $\mathbb{Z}_4$.*

Além disso, não existe ponto $P \in \mathbb{P}^2$ satisfazendo $G_P \cong V_4$ (grupo de Klein). Se $P \in \mathbb{P}^2 \backslash C$ é um ponto genérico, então $G_P \cong S_4$ e $g(P) = 49$ e não existe corpo intermediário entre $k(C)$ e K_P. Se C é uma quártica genérica então $\delta(C) = 0$.

A demonstração desse Teorema ocupará grande parte desta secção. Precisaremos de alguns lemas que serão enunciados e provados no decorrer da demonstração do Teorema devido a uma melhor contextualização de conceitos e notações que irão surgindo.

Seja então C uma quártica projetiva não singular em $\mathbb{P}^2$ e $P \in \mathbb{P}^2 \setminus C$, que será pensado como um centro de projeção. Após uma possível mudança projetiva de coordenadas, podemos supor que:

1. O centro P de projeção está na origem do sistema afim de coordenadas, isto é, $P = (0,0) \notin C$,

2. C intersecta o eixo $X = 0$ transversalmente (isto é, $X = 0$ não é tangente a C em nenhuma de suas intersecções, incluindo aí o ponto do infinito).

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

$$\pi_P(C \cap l_t) = t$$

além disso podemos supor que a equação afim de C é dada por

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

onde $c \in k \setminus \{0\}$.

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

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

Então, fazendo $K = k(x,t)$ e $K_P = k(t)$, a extensão $K \mid K_P$ é obtida através de $\hat{f}(x,t) = 0$. Assim, observando que $k(x,y) = k(x,tx) = k(x,t)$ vemos que $K = k(C) = k(\hat{C})$. Observe que para uma curva de grau d dada por uma equação do tipo acima:

$$\hat{F}(x,t) = F(x,tx) = \varphi_d(t)x^d + \varphi_{d-1}(t)x^{d-1} + \cdots + \varphi_1(t)x + c$$

o *discriminante* de $\hat{f}(x,t)$ é dado por

$$\psi(t) = (-1)^{\frac{d(d-1)}{2}} \varphi_d(t)^{2d-1} \prod_{1 \le i < j \le d} (x_i - x_j)^2,$$

onde x_i com $i = 1, ..., d$ são as raízes de $\hat{F}$ em alguma extensão normal de $k(t)$. (Veja [5]).

No nosso caso, isto é, $d = 4$, para cada $t \in k$, temos:

$$\psi(t) = \varphi_4^7(t) \prod_{1 \le i < j \le 4} (x_i - x_j)^2$$

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

Observe que como $\varphi_4(t) \neq 0$ temos que $\psi(t)=0$ se, e somente se, a equação $\hat{f}(x,t)=0$ possui raiz múltipla em $k(t)$. Estes valores de t para os quais $\hat{f}(x,t)=0$ possui raízes múltiplas são essenciais no que segue. O lema seguinte nos permitirá dar uma descrição local dos valores de t para os quais $\psi(t)=0$. Lembre-se que um ponto $Q \in C$ é chamado *1-inflexional* ou *ponto de inflexão ordinário* em C se $I(Q, C \cdot T_Q)=3$. Se $I(Q, C \cdot T_Q)=4$, dizemos que Q é *2-inflexional*. Mais geralmente, se $I(Q, C \cdot T_Q)=r \geq 3$, dizemos que Q é ponto $(r-2)$-*inflexional*.

Considere as notações fixadas acima e π_P a projeção de $\hat{C}$ sobre $\mathbb{A}^1$, onde estamos considerando t a variável de $\mathbb{A}^1$.

Lema 2 . *Suponha que* $\deg(C)=d$ *e que* $(t-\alpha)^n$ *seja um fator do discriminante* $\psi(t)$. *Então* $1 \leq n \leq d$. *Em particular, se* $d=4$, *temos que:*

1. $n=1$ *se, e somente se,* l_α *torna-se a reta tangente não inflexional de* C, *isto é, existe* $Q \in C$ *tal que* $I(Q, C \cdot T_Q)=2$ *ou* l_α *torna-se uma bitangente (não inflexional), isto é,* l_α *é tangente a* C *em dois pontos* Q_1 *e* Q_2 *distintos com* $I(Q_1, C \cdot T_{Q_1})=I(Q_2, C \cdot T_{Q_2})=2$.

2. $n=2$ *se, e somente se,* l_α *torna-se tangente inflexional ordinária de* C, *isto é, existe* $Q \in C$ *tal que* $I(Q, \cdot T_Q, Q)=3$

3. $n=3$ *se, e somente se, a reta* l_α *torna-se uma reta tangente 2-inflexional de* C, *isto é, existe* $Q \in C$ *tal que* $I(Q, C \cdot T_Q)=4$.

Demonstração: Considere a aplicação $\pi_P : C \longrightarrow \mathbb{P}^1$ de C em $\mathbb{P}^1$ definida da seguinte forma: se $Q \in C \cap l_t$ então $\pi_P(Q)=t \in \mathbb{A}^1 \subset \mathbb{P}^1$. Assim π_P induz uma imersão $\pi_P^* : \Gamma(\mathbb{P}^1) \longrightarrow \Gamma(C)$ do anel de coordenadas de $\mathbb{P}^1$ no anel de coordenadas de C. Suponha que $\alpha \in \mathbb{A}^1$ seja uma raiz de ψ. Observe que $s=t-\alpha$ é um parâmetro local em $\alpha \in \mathbb{A}^1$. Pela imersão π_P^*, podemos ver s no anel das funções regulares $\Gamma(C)$, ou ainda, no anel local $\mathcal{O}_Q(C)$. Seja u um parâmetro local em $Q \in C$. Então podemos escrever

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

onde $\lambda_i \in \mathbb{C}$ e $\lambda_m \neq 0$. Assim, após uma mudança de parâmetro local em Q, podemos supor $s=u^m$. Observe que

$$\deg(\pi_P)=\begin{cases} d & \text{se} \quad P \notin C \\ \\ d-1 & \text{se} \quad P \in C. \end{cases}$$

Assim m fica limitado superiormente por d, ou seja, $m \leq d$. Como $s-u^m = 0$ em $\mathcal{O}_Q(\hat{C})$, podemos escrever

$$s - u^m = \frac{g(x,t)}{h(x,t)},$$

onde $g(x,t), h(x,t) \in \Gamma(C)$, $g(Q) = 0$ e $h(Q) \neq 0$. Então g é um múltiplo de $\hat{f}$ em $\mathbb{C}[x,t]$ e podemos escrever $g(x,t) = g_1(x,t)\hat{f}(x,t)$ para algum $g_1(x,t) \in \mathbb{C}[x,t]$. Portanto,

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

Observe que $g_1(Q) \neq 0$ devido à ordem do zero da função $s - u^m$ em Q. Assim, $\hat{f}(x,t) = (s - u^m) \cdot \varepsilon(u)$, onde $\varepsilon(u)$ é um elemento inversível em $\mathcal{O}_P(\hat{C})$. Agora, escolha uma raiz m-ésima de s (no fecho algébrico de $k(t)$), digamos, $u_0 = \sqrt[m]{s}$ e w uma raiz m-ésima primitiva da unidade. Assim, numa vizinhança de $s = 0$, o discriminante $\psi(t)$ será

$$\begin{aligned}
\psi(t) &= (-1)^{\frac{d(d-1)}{2}}[\varepsilon(t)]^{2d-1} \prod_{1 \leq i < j \leq d} (x_i - x_j)^2 \\
&= [u_0^2]^{\frac{m(m-1)}{2}}(1-w)^2(1-w^2)^2 \cdots (w^{m-2} - w^{m-1})^2(-1)^{\frac{d(d-1)}{2}}[\varepsilon(t)]^{2d-1}.
\end{aligned}$$

Lembrando que $u_0 = \sqrt[m]{s}$, temos que $n = m - 1$. Como $m \leq d$ segue que $1 \leq m - 1 \leq d - 1$, e portanto, $1 \leq n \leq d - 1$.

Considerando $d = 3$ ou $d = 4$, temos $n \in \{1, 2, 3\}$. Sendo π_P a projeção de $\hat{C}$ sobre o eixo t e considerando $Q_i \neq Q_j$ sempre que $i \neq j$, teremos as seguintes opções para a imagem inversa de π_P em α, usando a linguagem de divisores:

1. $\pi_P^*(\alpha) = Q_1 + Q_2 + Q_3 + Q_4$ com os Q_i todos distintos $\Leftrightarrow$ $m_\alpha = 1$ $\Leftrightarrow$ $n_\alpha = 0$;

2. $\pi_P^*(\alpha) = Q_1 + Q_2 + 2\,Q_3$ com Q_1, Q_2, Q_3 distintos $\Leftrightarrow$ $m_\alpha = 2$ $\Leftrightarrow$ $n_\alpha = 1$; $\pi_P^*(\alpha) = 2\,Q_1 + 2\,Q_2$ com $Q_1 \neq Q_2$ $\Leftrightarrow$ l_α é uma bitangente $\Leftrightarrow$ $n_\alpha = 1$;

3. $\pi_P^*(\alpha) = Q_1 + 3\,Q_2$ com $Q_1 \neq Q_2$ $\Leftrightarrow$ $m_\alpha = 3$ $\Leftrightarrow$ $n_\alpha = 2$;

4. $\pi_P * (\alpha) = 4\,Q_1$ $\Leftrightarrow$ $m_\alpha = 4$ $\Leftrightarrow$ $n_\alpha = 3$.

Fixado $t \in k$, se x_1, x_2, x_3, x_4 são as raízes de $\hat{f}(x,t) = f(x,tx)$ então pelo Teorema de Bézout, como C tem grau 4 e l_α tem grau 1, as possibilidades dos pontos de intersecção entre essas duas curvas, levando em consideração as multiplicidades, são:

- $\pi_P^*(\alpha) = Q_1 + Q_2 + Q_3 + Q_4 \Leftrightarrow l_\alpha$ intersecta C transversalmente em todos os 4 pontos de intersecção, isto é, l_α não é tangente a C. Assim, $\pi_P^*(\alpha) = Q_1 + Q_2 + Q_3 + Q_4 \Leftrightarrow n_\alpha = 0$;
- $\pi_P^*(\alpha) = Q_1 + Q_2 + 2 \cdot Q_3 \Leftrightarrow l_\alpha$ é tangente (ordinária) a C em Q_3, isto é, $I(Q_3, C \cdot l_\alpha) = 2$. Assim, $\pi_P^*(\alpha) = Q_1 + Q_2 + 2 \cdot Q_3 \Leftrightarrow n_\alpha = 1$ ou $\pi_P^*(\alpha) = 2 \cdot Q_1 + 2 \cdot Q_2 \Leftrightarrow l_\alpha$ é uma bitangente com $I(Q_1, l_\alpha \cdot C) = 2$ e $I(Q_2, l_\alpha \cdot C) = 2 \Leftrightarrow n_\alpha = 1$;
- $\pi_P^*(\alpha) = 3 \cdot Q_1 + Q_2 \Leftrightarrow l_\alpha$ é tangente inflexional (ordinária) a C em Q_1, isto é, $I(Q_1, C \cdot l_\alpha) = 3 \Leftrightarrow n_\alpha = 2$;
- $\pi_P^*(\alpha) = 4 \cdot Q_1 \Leftrightarrow l_\alpha$ é tangente 2-inflexional a C em Q_1, isto significa que $I(Q_1, C \cdot l_\alpha) = 4 \Leftrightarrow n_\alpha = 3$.

Isto conclui a demonstração do Lema 2. □

Voltemos à prova do Teorema. Pela escolha de coordenadas vemos que $t = \alpha$ é um ponto ramificado se, e somente se, l_α é uma reta tangente a C, ou equivalentemente $\psi(\alpha) = 0$. Além disso, a condição *(2)* inicial nos garante que $t = \infty$ não é um ponto ramificado. Podemos então considerar $\hat{C} \to \mathbb{A}^1$. Usando a expressão do discriminante de $f(x,tx)$ em termos dos coeficientes $\varphi_i = \varphi_i(t)$ obtemos:

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

Precisamos agora do lema seguinte:

Lema 3 *Seja P um ponto genérico em $\mathbb{P}^2$. Então $gr(\psi(t)) = 12$ e $\psi(t)$ possui somente fatores simples.*

Demonstração: Se P é um ponto genérico e l é uma reta passando por P, então uma das seguintes afirmações valem:

- A reta l intersecta C transversalmente em todos os 4 pontos de intersecção.

- A reta l tangencia C em um ponto $Q_1 \in C$ com $I(Q_1, C \cdot l) = 2$ e nos outros dois pontos Q_2 e Q_3 intersecta transversalmente, isto é, $I(Q_2, C \cdot l) = I(Q_3, C \cdot l) = 1$

Sendo assim, pelo Lema 2, $\psi(t)$ possui apenas fatores simples. Como o gênero de C é $g(C) = 3$ (e o gênero da reta l é $g(l) = 0$), utilizando a fórmula de Riemann-Hurwitz para o recobrimento $\pi_P : C \to l$, temos

$$2g(C) - 2 = \deg(\pi_P)(2g(l) - 2) + \sum(m_\alpha - 1),$$

isto é, $2.3 - 2 = 4(0 - 2) + \deg(\psi(t))$, o que nos fornece, $\deg(\psi(t)) = 12$.

Isto conclui a demonstração do Lema 3. □

Seja P um ponto genérico em $\mathbb{P}^2$ e $\rho_P = \pi_P \circ \tilde{\pi}_P : \tilde{C}_P \to \mathbb{P}^1$ o recobrimento galoisiano, isto é, $\tilde{C}_P$ é uma curva não singular com corpo de funções igual a L_P que é o fecho normal de $k(C)$. Se $R \in \tilde{C}_P$ é um ponto de ramificação de ρ_P, então podemos afirmar que o índice de ramificação de ρ_P em R é igual a 2, uma vez que, pelo Lema 3, $\psi(t)$ só possui fatores simples. Já que ρ_P não é ramificado em $t = \infty$ e o grupo inercial no ponto ramificado é gerado por uma transposição. Agora usando as Proposições 1 e 2 do capítulo 1, página 24, podemos concluir que G_P é isomorfo a S_4. Agora o gênero de $\tilde{C}_P$ pode ser obtido pela aplicação da fórmula de Riemann-Hurwitz. Como $[L_P : K_P] = 24$ e $[k(C) : K_P] = 4$, segue que $[L_P : k(C)] = 6$. Então ρ_P terá $6 \cdot \deg(\psi(t)) = 6 \cdot 2 \cdot 12 = 144$ pontos de ramificação com índice 2. Então a fórmula de Riemann- Hurwitz nos fornece $2g(P) - 2 = 24(0 - 2) + 144$, e portanto $g(P) = 49$. O fato que não existe corpo intermediário entre K_P e $k(C)$ é um fato geral de teoria de Galois e da estrutura de S_4. Para concluir a prova do Teorema precisamos analisar os casos em que P não é genérico. Para isto considere a cúbica resolvente $\tilde{g}(x)$ de $\hat{f}(x, t) = 0$:

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

Segue das expressões das raízes da resolvente já explicitadas anteriormente:

$$t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad t_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad t_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3,$$

onde os α_i geram L_P sobre $K = k(t)$, que o corpo de fatoração de $\tilde{g}(x)$ está contido em L_P e naturalmente $\tilde{g}(x) \in k(t)[x]$. Então, aplicando o Teorema 5, do capítulo 2, (e seguindo as mesmas notações do Teorema) temos que

1. $G_P \cong S_4 \Leftrightarrow \tilde{g}(x)$ é irredutível sobre $k(t)$ e $\sqrt{\psi(t)} \notin k(t)$.

2. $G_P \cong A_4 \Leftrightarrow \tilde{g}(x)$ é irredutível sobre $k(t)$ e $\sqrt{\psi(t)} \in k(t)$.

3. $G_P \cong V_4 \Leftrightarrow \tilde{g}(x)$ se fatora em fatores lineares sobre $k(t)$.

4. $G_P \cong C_4 \Leftrightarrow \tilde{g}(x)$ tem exatamente uma raiz α em $k(t)$ e

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

se fatora sobre E.

5. $G_P \cong D_4 \Leftrightarrow \tilde{g}(x)$ possui exatamente uma raiz α em $k(t)$ e $h(x)$ (definido em (4)) não se fatora em E.

Isto conclui a prova do Teorema. □

Em seguida gostaríamos de caracterizar as equações que definem C pela estrutura de G_P. Para isso relembremos que se G_P é isomorfo a S_4 ou A_4 então não existem corpos intermediários entre $k(C)$ e K_P. Além disso, nos casos em que $G_P \cong V_4$, C_4 ou D_4, podemos encontrar subcorpos entre $k(C)$ e K_P considerando-se subgrupos de G_P.

Neste sentido, temos o seguinte lema.

Lema 4 *As seguintes afirmações são equivalentes:*

1. *$k(C)$ possui um corpo intermediário K' com $[K' : K_P] = 2$.*

2. *$k(C)$ pode ser expresso por $k(C) = K_P(\theta)$ onde θ é raiz do polinômio irredutível $X^4 + aX^2 + b \in K_P[X]$.*

Demonstração: Suponhamos que *(1)* seja válido. Seja $\alpha \in K'$ tal que $\alpha \notin K_P$. Então $K' = K_P(\alpha)$. Podemos supor $\alpha^2 = c \in K_P$, isto é, o polinômio mínimo de α sobre K_P é $p(X) = X^2 - c$. De modo análogo, seja $\beta \in k(C)$ tal que $\beta \notin K'$ um elemento primitivo da extensão $k(C)|K_P$. Podemos supor que $\beta^2 = d \in K'$, isto é, o polinômio mínimo de β sobre K' é $p'(X) = X^2 - d$. Observe que $\{1, \alpha\}$ é uma base de K' sobre K_P, então podemos escrever $d = a\alpha + b$ com $a, b \in K_P$, logo $\alpha = \frac{d-b}{a} = \frac{\beta^2 - b}{a}$. Sem perda de generalidade podemos tomar $\beta^2 - d = a\alpha$, assim $\beta^2 = d = a\alpha + b$. Logo $\beta^4 = a^2\alpha^2 + 2a\alpha b + b^2 = 2b\beta^2 + a^2c - b^2$, isto é, $\beta^4 - 2b\beta^2 + b^2 - a^2c = 0$ com $2b, b^2 - a^2c \in K_P$. Observe que como $\beta \notin K'$ então $\{1, \beta\}$ é uma base de $k(C)$ sobre K', portanto $\{1, \beta, \beta^2\}$ é um conjunto LD sobre K'. Temos $\{1, \alpha\}$ uma base de K' sobre K_P, $\{1, \beta\}$ uma base de $k(C)$ sobre K', portanto $\{1, \alpha, \beta, \alpha\beta\}$, é uma base de $k(C)$ sobre K_P. Como α é escrito em função de

β^2, temos que $\{1, \beta, \beta^2, \beta^3\}$ é uma base de $k(C)$ sobre K_P, concluindo assim que o polinômio mínimo de β sobre K_P é $p(X) = X^4 - 2bX^2 + b^2 - a^2c$.

Reciprocamente, suponhamos que $k(C) = K_P(\theta)$ onde o polinômio mínimo de θ sobre K_P é $p(X) = X^4 + aX^2 + b \in K_P[X]$. Tome $K' = K_P(\theta^2)$. Então $(\theta^2)^2 + a\theta^2 + b = 0$. Portanto $[K' : K_P] = 2$ e o polinômio mínimo de θ^2 sobre K_P é $q(X) = X^2 + aX + b$. □

Do Lema 4 obtemos que $k(C) = k(x, t)$, onde $x^4 + ax^2 + b = 0$. Os coeficientes a e b estão em $k(t)$, assim denotamos $a = a(t)$ e $b = b(t)$. Cancelando os denominadores, obtemos $c(t)x^4 + d(t)x^2 + e(t) = 0$ onde $c(t)$, $d(t)$ e $e(t)$ são assumidos relativamente primos. Colocando $y = tx$, obtemos

$$c\left(\frac{y}{x}\right)x^4 + d\left(\frac{y}{x}\right)x^2 + e\left(\frac{y}{x}\right) = 0.$$

Afim de se obter uma equação quártica, é preciso que $\text{grau}(e(t)) = 0$, $\text{grau}(d(t)) \leq 2$ e $\text{grau}(c(t)) \leq 4$. Daí obtemos a proposição seguinte.

Proposição 4 *O grupo G_P é isomorfo a V_4, C_4 ou D_4 se, e somente se, uma equação de C pode ser expressa como*

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

onde $f_4(x, y)$ e $f_2(x, y)$ são polinômios homogêneos de grau 4 e 2 respectivamente e c é um elemento não nulo em k. □

Assim,

$$\tilde{f}(x, t) = \varphi_4(t)x^4 + \varphi_2(t)x^2 + c \quad \text{e} \quad \tilde{g}(x) = (x - \varphi_2/\varphi_4)(x^2 - 4c/\varphi_4).$$

Aplicando o Teorema 5 do capítulo 2, obtemos neste caso:

1. $G_P \cong V_4 \Leftrightarrow \sqrt{c/\varphi_4} \in k(t)$.
2. $G_P \cong C_4 \Leftrightarrow \sqrt{(c/\varphi_4)((\varphi_2^2/\varphi_4^2) - (4c/\varphi_4))} \in k(t)$.
3. $G_P \cong D_4 \Leftrightarrow$ *(i)* e *(ii)* não ocorrem.

Com relação ao caso *(i)* temos as seguintes equivalências:

$$\sqrt{\frac{c}{\varphi_4}} \in k(t) \Leftrightarrow \sqrt{\varphi_4} \in k(t) \Leftrightarrow f_4(x, y) \text{ é um quadrado perfeito em } k[x, y].$$

Então vemos que, neste caso, C deveria ter pontos singulares, contradizendo o fato que C é não singular. Consequentemente não existe ponto P que satisfaça $G_P \cong V_4$.

Se $\varphi_2 = 0$, então (ii) é sempre satisfeito. Então consideremos o caso $\varphi_2 \neq 0$. Neste caso, a condição (ii) é equivalente a

$$\sqrt{\frac{\varphi_2^2 - 4c\varphi_4}{\varphi_4}} \in k(t).$$

Se φ_4 possui um fator múltiplo então C tem pontos singulares. Assim, a condição é equivalente a $(\varphi_2^2 - 4c\varphi_4)/\varphi_4$ ser um elemento não nulo em k. Mas neste caso então temos $\varphi_4 = c'\varphi_2^2$ para algum $c' \in k$, $c' \neq 0$. Daí vemos que C possui pontos singulares. Consequentemente se $G_P \cong \mathbb{Z}_4$, então φ_2 deve ser igual a zero, isto é, $f(x, y)$ é expresso como $f(x, y) = f_4(x, y) + c$, neste caso vemos que $\psi(t) = 256c^3\varphi_4(t)^3$. Portanto, para existir um ponto de Galois é necessário existir 4 retas tangentes 2-inflexionais. Daí podemos concluir que:

O número de pontos de Galois de uma quártica C é finito. Em particular, uma quártica qualquer não possui pontos de Galois.

3.3 Exemplos

Vamos agora apresentar alguns exemplos. O primeiro exemplo é a curva de Fermat de grau 4 que foi colocada como protótipo no início do capítulo. Assim vamos verificar as afirmações que lá foram feitas. Nos outros dois exemplos apenas citamos o que ocorre. Nos exemplos vamos supor que $k = \mathbb{C}$.

Exemplo 5

Considere C a curva de Fermat de grau 4 cuja equação em $\mathbb{P}^2$ pode ser dada pelo polinômio homogêneo $F(X, Y, Z) = X^4 + Y^4 - Z^4$. Sua equação afim é $X^4 + Y^4 = 1$. É fácil verificar que de fato C é não singular. Seja $P \notin C$. Observe que C não possui pontos 1-inflexionais pois não há pontos $Q \in C$ tais que $I(Q, C \cdot T_Q) = 3$. No entanto, C possui 12 pontos 2-inflexionais, a saber, os pontos $Q_{ij} \in C$ dados por $Q_{1j} = (0 : i^j : 1)$, $Q_{2j} = (i^j : 0 : 1)$ e $Q_{3j} = (1 : \xi_j : 0)$, onde i é uma das raízes de $w^2 + 1 = 0$, ξ é uma das raízes de $w^4 + 1 = 0$ e $0 \leq j \leq 3$. É fácil verificar que $I(Q_{ij}, C \cdot T_{Q_{ij}}) = 4$ para todos i, j tais que $1 \leq i \leq 3$.

Suponhamos que $G_P \cong \mathbb{Z}_4$. Então, pela conclusão da discussão final da secção anterior, deve existir quatro retas passando por P que são tangentes a um dos pontos 2-inflexionais de C. Por exemplo, tomando

$$Q_{10} = (0 : 1 : 1),\ Q_{11} = (0 : i : 1),\ Q_{12} = (0 : -1 : 1) \text{ e } Q_{13} = (0 : -i : 1)$$

são 4 pontos 2-inflexionais cujas retas tangentes a eles são respectivamente

$$Y - Z = 0, \quad Y - iZ = 0, \quad Y + Z = 0 \quad \text{e} \quad Y + iZ = 0.$$

Todas estas 4 retas passam pelo ponto externo $P = (1 : 0 : 0) \notin C$. Podemos verificar que $P = (1 : 0 : 0)$ é um ponto de Galois de C, cujo grupo G_P é isomorfo a $\mathbb{Z}_4$. Para isto, colocando $x = \frac{Y}{X}$, $y = \frac{Z}{X}$ e $y = tx$, sendo $f(x, y) = F(1, x, y)$, teremos que

$$\hat{f}(x, t) = f(x, tx) = 1 + x^4 - y^4 = 1 + x^4 - t^4x^4 = 1 + (1 - t^4)x^4.$$

Daí segue imediatamente que $G_P \cong \mathbb{Z}_4$. Naturalmente existe um subcorpo intermediário K' entre $k(C)$ e K_P. Podemos verificar diretamente que este subcorpo K' é isomorfo a $k(t)(\sqrt{\psi(t)}\,) = k(t, \sqrt{1 - t^4}\,)$. Isto confirma o resultado teórico. De maneira análoga, vemos que os pontos $(0 : 1 : 0)$ e $(0 : 0 : 1)$ são pontos de Galois externos de C com as mesmas características de $(1 : 0 : 0)$. Pelas condições sobre os pontos inflexionais e retas tangentes a esses pontos, vemos que não existem outros pontos de Galois em C e, Portanto o número de pontos de Galois externos a C é $\delta(C) = 3$.

Vamos agora considerar o caso em que P não é um ponto de Galois. Temos a seguinte afirmação: $G_P \cong A_4$ se, e somente se, $\sqrt{\psi(t)} \in k(t)$. Uma vez que C não possui pontos 1-inflexionais, $\sqrt{\psi(t)} \in k(t)$ se, e somente se, existem 6 retas bitangentes passando por P. Vemos facilmente que é impossível já que as possíveis retas bitangentes a C são $y = \varepsilon x + \xi$, onde ε e ξ são respectivamente raízes de $w^2 + 1 = 0$ e $w^4 + 1 = 0$. Portanto não temos solução para o sistema formado pela equação da reta tangente e a equação da curva. Concluímos assim que não existe ponto P satisfazendo $G_P \cong A_4$.

Finalmente vamos estudar a condição $G_P \cong D_4$. Suponha que a equação da curva se expressa sob a forma $f(x, y) = f_4(x, y) + f_2(x, y) + c$. Então temos que

$$\psi(t) = 16c\varphi_4(t)\left[\varphi_2(t)^2 - 4c\varphi_4(t)\right]^2.$$

Como C é uma curva não singular, $\varphi_4(t)$ não pode ter fatores múltiplos. Assim, se $G_P \cong D_4$, então deve existir quatro retas bitangentes passando por P. Todos os pontos, fora de C, que satisfazem esta condição são os 12 pontos seguintes:

$$(0 : \xi : 1),\ (\xi : 0 : 1),\ (1 : 1 : 0),\ (1 : -1 : 0),\ (1 : i : 0),\ (1 : -i : 0),$$

onde ξ é uma das raízes de $w^4 + 1 = 0$. De fato estes pontos satisfazem a condição $G_P \cong D_4$. Por exemplo, no caso em que $P = (\xi : 0 : 1)$, onde $\xi = (\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$, temos:

$$\hat{f}(x, t) = (t^4 + 1)x^4 + 4\xi x^3 + 6ix^2 + 4i\xi x - 2 \quad \text{e,}$$

$$\tilde{g}(x) = x^3 - \frac{6i}{t^4+1}x^2 + \frac{8(t^4-1)}{(t^4+1)^2}x - \frac{32it^4}{(t^4+1)^3}.$$

Além disso, $\tilde{g}(x)$ tem uma fator irredutível de grau 2 em $k(t)[x]$, a saber,

$$\tilde{g}(x) = \left(x - \frac{4i}{t^4+1}\right)\left(x^2 - \frac{2i}{t^4+1}x + \frac{8t^4}{(t^4+1)^2}\right).$$

Daí vemos que $G_P \cong \mathbb{Z}_4$ ou $G_P \cong D_4$. Pelo que sabemos dos pontos de ramificação, π_P não é um recobrimento galoisiano e, então podemos concluir que $G_P \cong D_4$.

Exemplo 6

A curva de Klein é a quártica C definida pela equação afim

$$f(x,y) = x^3y + y^3 + x = 0.$$

A sua equação projetiva é $F(X,Y,Z) = X^3Y + Y^3Z + XZ^3 = 0$. É fácil verificar que C é não singular e tem apenas pontos de inflexão ordinários. Não existem pontos de Galois associados a C, nem internos nem externos.

Exemplo 7

Considere a curva quártica C definida pela equação afim

$$f(x,y) = x^3y + y^4 + x^3 + y^3 + 4y + 1 = 0.$$

Sua equação projetiva é

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

O ponto $P = (0:0:1)$ não é ponto de Galois associado a C. No entanto é fácil verificar que G_P é isomorfo a A_4.

Referências Bibliográficas

[1] V. Bayer and A. Hefez, *Strange Curves*, Comm Algebra 19, 3041-3059, (1991).

[2] C. P. C. Chacca, *Classificação de Curvas Planas com inifinitos pontos de Galois Externos*, Dissertação de Mestrado - Instituto de Matemática - UFF (2010).

[3] S. Fukasawa and T. Hasegawa, *Singular plane curves with infinitely many Galois points*, Journal of Algebra 323, 10-13, (2010).

[4] W. Fulton, *Algebraic Curves: an Introduction to Algebraic Geometry*, Benjamin, New York, 1969.

[5] A. Garcia e Y. Lequain, *Elementos de Álgebra*, Projeto Euclides, IMPA, 2002.

[6] M. Homma, *Galois points for a Hermitian curve*, Comm. Algebra 34, 4503-4511, 2006.

[7] S. Iitaka, *Algebraic Geometry*, Graduate Texts in Math., Vol. 76 Springer-Verlag, New York/Heidelberg/Berlin, 1982.

[8] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Company, San Francisco, 1974.

[9] I. Kaplansky, *Fields and Rings*, second edition, University of Chicago Press, Chicago, 1972.

[10] L. C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly 96 (1989), 133-137.

[11] K. Miura and H. Yoshihara, *Field theory for function fields of plane quartic curves*, Journal of Algebra 226, 283-294 (2000).

[12] M. Namba., *Geometry of Projective Algebraic Curves*, Dekker, New York/Basel, 1984.

[13] J. P. Serre, Notes written by H. Darmon, *Topics in Galois Theory*, Research Notes in Math., Vol 1, Jones and Bartlett, Boston/London, (1992).

[14] V. V. Shokurov, *Riemann Surfaces and Algebraic Curves*, Vol. 23 Springer-Verlag, New York/Heidelberg/Berlin,1988.

[15] P. M. Silva , *Pontos de Galois sobre Curvas Quárticas Projetivas Não Singulares*, Dissertação de Mestrado - PPGMAT - UFES, (2009).

[16] R. P. Stauduhar, *Determination of Galois Groups*, Mathematics of Computation, 27, 981-999, (1973).

[17] H. Stichtenoth, *Algebraic Function Fields and Codes*. Universitext. Springer-Verlag, Berlin, 1993.

[18] E. Strey, *A Hipótese de Riemann para Curvas Algébricas e uma Caracterização da Curva Hermitiana*, Dissertação de Mestrado - PPGMAT - UFES, (2009).

[19] Vainsencher, I., *Introdução às Curva Algébricas Planas*, Coleção Matemática Universitária, SBM, 1996.

Livros Grátis

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

Milhares de Livros para Download:

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