UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

GYSLANE APARECIDA ROMANO DOS SANTOS
DE LIMA

PONTOS DE GALOIS DE CURVAS PLANAS PROJETIVAS EM CARACTERÍSTICA POSITIVA

Vitória
2015

GYSLANE APARECIDA ROMANO DOS SANTOS
DE LIMA

PONTOS DE GALOIS DE CURVAS PLANAS PROJETIVAS EM CARACTERÍSTICA POSITIVA

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.
Orientador: Prof. Dr. Valmecir Antônio dos Santos Bayer

Vitória
2015

Dedicatória

À Deus, família e amigos.

Agradecimentos

Agradeço a Deus pelas oportunidades.

À minha família pelo incentivo e compreensão nos momentos em que estive ausente.

Ao professor Valmecir Antonio dos Santos Bayer pela orientação e por estar sempre a disposição.

Aos meus queridos colegas e professores do PPGMAT pelo companherismo e ensinamentos.

À secretária Jussára pela paciência e bom atendimento.

À CAPES pelo apoio financeiro.

Resumo

Nesta dissertação estudamos pontos de Galois em curvas algébricas planas não singulares $C \subset \mathbb{P}^2$ de grau $d \geq 4$ em característica positiva $p > 2$. Os resultados de H. Yoshihara foram generalizados sobre o números de pontos de Galois internos (respectivamente externos) para característica positiva sob o pressuposto que $d \not\equiv 1$ módulo p (respectivamente $d \not\equiv 0$ módulo p). Determinamos todos os pontos de Galois internos e externos, no caso em que $d = p$ e em curvas quárticas em característica três.

Abstract

In this dissertation we study Galois points in an algebraic non singular plane curve $C \subset \mathbb{P}^2$ of degree $d \geq 4$ in positive characteristic $p > 2$. The results of H. Yoshihara on the number of inner (respectively outer) Galois points are generalized in this case, under the assumption that $d \not\equiv 1$ modulo p (respectively $d \not\equiv 0$ modulo p). We determine all the number of inner and outer Galois points, in the case that $p = d$ and for quartic curves in three characteristic.

Sumário

INTRODUÇÃO

O objetivo principal desta dissertação é estudar pontos de Galois, internos e externos, de curvas planas projetivas não singulares sobre um corpo algebricamente fechado de característica positiva. Em característica zero, os pontos de Galois associados a curvas planas projetivas foram introduzidos por *Hisao Yoshihara* ([22]) em 1996 . Posteriormente, em característica positiva, o primeiro resultado foi feito por *M. Homma* ([10]) em 2006.

A noção de pontos de Galois associados a uma curva plana projetiva $C \subset \mathbb{P}^2$ surge quando consideramos uma projeção central dessa curva sobre uma reta $l \subset \mathbb{P}^2$ a partir de um ponto P fora dessa reta. Um tal ponto é denominado centro da projeção que pode ou não pertencer à curva C. Observe que essa projeção induz uma extensão finita de corpos da maneira seguinte. O corpo de funções racionais associado à reta l pode ser visto como um subcorpo do corpo de funções da curva C. Esse corpo de funções racionais não depende da escolha da reta onde se está projetando, no entanto depende do centro de projeção.

Para tornar este contexto mais claro, vamos estabelecer algumas notações. Fixemos um corpo k algebricamente fechado e de característica positiva p. Suponhamos que C seja uma curva plana projetiva não singular de grau d sobre k, considere uma reta l e um ponto P fora da reta l (no mesmo plano de C). Vamos denotar por π_P a projeção de C sobre l, com centro de projeção no ponto P. Se a extensão de corpos, $k(C) \mid k(l)$, induzida por esta projeção for galoisiana, diremos que P é *ponto de Galois* de C. No caso em que P esteja sobre a curva, o grau da extensão $k(C) \mid k(l)$ é $d-1$ e diremos que P é um *ponto de Galois interno*. Se P não pertence à curva C, o grau da extensão $k(C) \mid k(l)$ é d e, neste caso, diremos que P é um *ponto de Galois externo*.

Denotemos por $\delta(C)$ a quantidade de pontos de Galois internos e por $\delta'(C)$ a quantidade de pontos de Galois externos de C. Em característica zero os resultados obtidos por H. Yoshihara ([22]) sobre essas quantidades, para uma

curva não singular de grau $d \geq 4$, foram: $\delta(C) = 0, 1$ ou 4 e $\delta'(C) = 0, 1$ ou 3. Em característica positiva, *M. Homma* ([10]) estudou curvas Hermitianas de grau $p^e + 1$ para algum inteiro e, e descobriu que, em tais curvas, há muitos pontos de Galois internos e externos. Portanto, os resultados de Yoshihara para carcterísitca zero não são mais válidos para tais curvas. Depois disso, *S. Fukasawa* ([7], [8] e [9]) também estudou pontos de Galois em característica positiva e obteve, sob algumas hipóteses, os mesmos resultados obtidos por *H. Yoshihara* ([22]).

S. Fukasawa mostrou que, para uma curva plana projetiva não singular de grau $d \geq 4$ sobre um corpo algebricamente fechado de característica $p > 2$, sendo $d \not\equiv 1$ módulo p, vale $\delta(C) = 0, 1$ ou 4 e, além disso, se $\delta(C) = 4$, então $d = 4$ e a curva é projetivamente equivalente à curva de Fermat. Para obter esses resultados, ele observou que uma curva C tem um ponto de Galois interno se, e somente se, ela é projetivamente equivalente à curva $X^{d-1}Z + G(Y, Z)$, onde $G(Y, Z)$ é um polinômio homogêneo de grau d sem fatores múltiplos que não possui Z como fator. Se P é um ponto de Galois interno da curva C, então é também ponto de inflexão cuja reta tangente intersecta C com multiplicidade d em P, ou seja, é uma inflexão de ordem $d - 2$, e existem d inflexões de ordem $d - 3$ e, além disso, a reta tangente contém P. No caso de pontos de Galois externos, tendo como hipótese $d \not\equiv 0$ módulo p, uma curva C tem um ponto de Galois externo se e somente se C é projetivamente equivalente a $X^d + G(Y, Z)$, onde $G(Y, Z)$ é um polinômio homogêneo de grau d e não tem raizes múltiplas. Além disso, se P é um ponto de Galois externo de C, então existem d inflexões de ordem $d - 2$ e cada reta tangente inflexional contém P. Segue daí que $\delta'(C) = 0, 1$ ou 3. Se $d \equiv 1$ módulo p e C tem a aplicação dual separável, então $\delta'(C) = 0$ ou 1.

Como exemplo, encontramos os pontos de Galois em curvas de grau $p > 3$. Neste caso se a curva C tem um ponto de Galois interno, então o número de inflexões em C é $p + (p - 1)e + 1$, onde $0 \leq e \leq 2p - 3$, quando não contamos com multiplicidades. Agora se a curva tem um ponto de Galois externo, então ela é projetivamente equivalente a $X^p - XZ^{p-1} + G(Y, Z)$, onde $G(Y, Z)$ é um polinômio homogêneo de grau p e o coeficiente de $Y^{p-1}Z$ é não nulo. Neste caso, temos que o número de inflexões é $pe' + 1$, onde $1 \leq e' \leq p - 3$, quando não contamos com multiplicidades. Daí obtemos que se C é uma curva plana projetiva não singular de grau p sobre um corpo algebricamente fechado de característica $p > 3$, então $\delta(C) \leq 1$ e $\delta'(C) \leq 1$. Segue que $\delta(C) = \delta'(C) = 1$ se, e somente se, a curva é projetivamente equivalente à curva definida por $X^p - XZ^{p-1} + Y^{p-1}Z$.

O primeiro capítulo é dedicado a conceitos e propriedades básicas necessárias

para o desenvolvimento e compreensão dos resultados principais da dissertação. Além das propriedades básicas, incluimos aqui resultados de *R. Pardini* ([14]) sobre aplicações separáveis e inseparáveis.

No segundo capítulo apresentamos os resultados sobre pontos de Galois internos, externos e curvas de grau p. Finalizamos o capítulo com uma seção sobre pontos de Galois em curvas quárticas em característica 3. Ambos os resultados obtidos por *S. Fukasawa* ([6] e [7]).

Capítulo 1

PRELIMINARES

1.1 Extensões de corpos

As definições, os conceitos e resultados apresentados nessas duas primeiras seções podem ser encontrados no texto "Teoria dos Corpos" de O. Endler em [4].

Considere dois corpos K e L tais que $K \subseteq L$. Neste caso, dizemos que L é uma *extensão* de K e denotamos por $L \mid K$.

Podemos ver L como um espaço vetorial sobre K, a dimensão desse espaço vetorial é chamada de *grau* da extensão $L \mid K$ e denotada por $[L : K]$. Uma extensão $L \mid K$ é *finita* se $[L : K] = n$, para algum $n \in \mathbb{N}$, e neste caso, existe uma base $\{x_1, \ldots, x_n\}$ de $L \mid K$.

Seja $L \mid K$ uma extensão de corpos, um elemento $\alpha \in L$ é dito *algébrico* sobre K se for raiz de um polinômio não nulo $F \in K[X]$. Caso contrário, α é dito ser *transcendente* sobre K.

Dado um elemento $\alpha \in L$ é conveniente considerar o K-homomorfismo de anéis $\varphi_\alpha : K[X] \longrightarrow L$, definido por $\varphi_\alpha(F) = F(\alpha)$. É imediato verificar que a imagem de φ_α é igual a $K[\alpha]$ e que o seu núcleo $ker(\varphi_\alpha)$ é um ideal (principal) de $K[X]$. Além disso, este núcleo é diferente de zero se, e somente se, α é algébrico sobre K. Neste caso, o polinômio mônico que gera este ideal é chamado *polinômio minimal* de α sobre K.

Quando α é algébrico sobre K então $K[\alpha]$ é um corpo e $K[\alpha] \mid K$ é uma extensão finita. Neste caso, o núcleo de φ_α é um ideal maximal de $K[X]$, o polinômio minimal de α é irredutível em $K[X]$, $K[\alpha] = K(\alpha)$ e, se n é o grau do polinômio mínimo de α, então o conjunto $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forma

uma base de $K(\alpha)$ sobre K. Portanto, temos naturalmente que o grau do polinômio minimal é igual a $[K(\alpha) : K]$.

A extensão $L \mid K$ é *algébrica* quando todo $\alpha \in L$ é algébrico sobre K. Caso contrário $L \mid K$ é chamada *transcendente*. $L \mid K$ é *finitamente gerada* se existirem $\alpha_1, \ldots, \alpha_r \in L$ tais que $L = K(\alpha_1, \ldots, \alpha_r)$. Dizemos K é um corpo *algebricamente fechado* se para todo polinômio $f(x) \in K[x]$, existe $\alpha \in K$ tal que $f(\alpha) = 0$.

Considere agora $F = F(X) \in L[X]$ um polinômio não nulo, com coeficientes no corpo L e α um elemento de L . A *multiplicidade* de α como raiz de F é definida por

$$m_\alpha = m(\alpha, F) = max\{m \in \mathbb{N} \mid (X - \alpha)^m \text{ divide } F \text{ em } L[X]\}.$$

Observe que $m_\alpha = 0$ se, e somente se, α não é raiz de F. Dizemos que α é uma *raiz simples* de F se $m_\alpha = 1$. No caso em que $m_\alpha \geq 2$ dizemos que α uma *raiz múltipla* de F. Para saber se uma raiz α de F é simples ou múltipla, podemos usar a derivada. Considere o operador derivação

$$\begin{array}{rccc} D: & L[X] & \longrightarrow & L[X] \\ & \sum_{j=0}^{m} a_j X^j & \longmapsto & \sum_{j=1}^{m} j a_j X^{j-1} \end{array}$$

No caso em que $car(L) = 0$ temos que $DF(X) = 0$ (polinômio nulo) se, e somente se $F(X) \in L$. No caso em que $car(L) = p > 0$ (p primo) então $DF(X) = 0$ se, e somente se, $F(X) \in L[X^p]$.

Entre as raízes $\alpha \in L$ de um polinômio $F \in L[X]$, as simples são caracterizada pela seguinte proposição

Proposição 1.1.1 *Sejam $F(X) \in L[X]$ um polinômio não nulo e $\alpha \in L$, tal que $F(\alpha) = 0$. Então $m(\alpha, F) = 1$ se, e somente, se $DF(\alpha) \neq 0$.*

A proposição anterior é demonstrada na página 52 de O. Endler ([4]).

Diremos que um polinômio $F(X) \in L[X] \setminus \{0\}$ é *separável*, quando F e DF forem primos entre si. Isto é equivalente ao fato do discriminante de $F(X)$ ser diferente de zero, ou seja, $Res(F(X), DF(X)) \neq 0$. Um elemento $\alpha \in L$ é dito ser *separável* sobre K se for raiz de algum polinômio separável não

nulo $F(X) \in K[X]$. Caso contrário, α é dito ser *inseparável* sobre K. Além disso dizemos que uma extensão $L \mid K$ é *separável* quando todo $\alpha \in L$ é separável sobre L.

Considere Ω um corpo algebricamente fechado que contenha K. Para cada polinômio não nulo $F(X) \in K[X]$, definimos $\Re_F = \{\alpha \in \Omega \mid F(\alpha) = 0\}$ como o conjunto das raízes de $F(X)$ em Ω. A cardinalidade (que denotamos por $\#$) de $\Re_F$ é menor ou igual ao grau de F, isto é, $\#\Re_F \leq gr(F)$.

Proposição 1.1.2 *Para todo polinômio $F \in K[X]$ não nulo, temos que $\#\Re_F \leq gr(F)$ e as seguintes afirmações são equivalentes:*

(i) $\#\Re_F = gr(F)$;

(ii) $m(\alpha, F) = 1$ *para todo* $\alpha \in \Re_F$;

(iii) F *é separável.*

No caso de característica zero, todo polinômio irredutível é separável e, portanto, toda extensão de corpos algébrica $L \mid K$ é separável sobre K. No caso de característica positiva, um polinômio irredutível $f(X) = \sum_{i=0}^{d} a_i X^i \in K[X]$ é separável se, e somente se, $a_i \neq 0$ para algum $i \not\equiv 0 \bmod p$, $0 \leq i \leq d$.

Sejam $\Re_F$ o conjunto das raízes do polinômio $F(X)$ e $\Im$ um subconjunto de $K[X] \setminus \{0\}$. Coloque $\Re_\Im = \bigcup_{F \in \Im} \Re_F$. O corpo $K(\Re_\Im)$ é chamado o *corpo de raízes* de $\Im$ ou *corpo de decomposição* de $\Im$ sobre K.

Proposição 1.1.3 *Para todo subconjunto $\Im$ de $K[X] \setminus \{0\}$, $K(\Re_\Im)$ é o "menor" corpo L entre K e Ω tal que todos os polinômios $F \in \Im$ se fatoram em $L[X]$ em um produto de polinômios lineares.*

A demonstração da proposição anterior segue na página 75 de O. Endler ([4]).

Pode-se verificar facilmente que o corpo de raízes independe da escolha de Ω.

Dizemos que uma extensão algébrica $N \mid K$ é *normal* se para todo $\alpha \in N$, o seu polinômio minimal sobre K se fatora em polinômios lineares em $N[X]$.

Proposição 1.1.4 *Para toda extensão algébrica $L \mid K$, as seguintes afirmações são equivalentes:*

(i) $L \mid K$ *é normal;*

(ii) Se $\alpha \in L$ *então todas as raízes do seu polinômio minimal de* α *sobre* K *também estão em* L*;*

(iii) Para todo polinômio irredutível $P \in K[X]$, $\Re_P \cap L$ *é vazio ou* $\Re_P \subseteq L$.

A demonstração da proposição anterior segue na página 77 de O. Endler ([4]).

Dado um corpo qualquer L entre K e Ω, denotamos por $Aut(L \mid K)$ o conjunto dos K-automorfismo de L. Dada uma extensão algébrica $L \mid K$, temos que $Aut(L \mid K)$ é igual ao conjunto dos K-homomorfismo de L em Ω se, e somente se, $L \mid K$ é normal.

Proposição 1.1.5 *Seja $L \mid K$ uma extensão finita e seja m o número dos K-homomorfismo de L em Ω, então:*

(i) $\#Aut(L \mid K) \leq m \leq [L : K]$;

(ii) $\#Aut(L \mid K) = m$ *se, e somente se,* $L \mid K$ *for normal;*

(iii) $\#Aut(L \mid K) = [L : K]$ *se, e somente se,* $L \mid K$ *for normal e separável.*

A demonstração da proposição anterior segue diretamente dos resultados das páginas 52 e 81 de O. Endler ([4]).

1.2 Alguns fatos sobre a teoria de Galois

Pode-se verificar facilmente que o conjunto $Aut(L \mid K)$ é um grupo com a operação composição, tendo como elemento neutro a aplicação identidade id_L. Este é chamado *grupo de Galois* de $L \mid K$. No caso de uma extensão finita este grupo é finito. Uma extensão $L \mid K$ é dita *galoisiana* se a ordem do grupo $Aut(L \mid K)$ for igual a $[L : K]$ (grau da extensão), ou seja, se a extensão for normal e separável.

Dada uma extensão arbitrária de corpos $N \mid K$, podemos associar a cada um de seus corpos intermediários um subgrupo de $Aut(N \mid K)$ e vice-versa. O par de aplicações assim definidas é chamado uma *conexão de Galois*. Sua descrição é a seguinte.

Considere $\Gamma = Aut(N \mid K)$, κ o conjunto de todos os corpos intermediários entre K e N, $\mathcal{G}$ o conjunto de todos os subgrupos de Γ. A conexão de Galois consiste do par de aplicações

$$\begin{array}{rcl} g : \kappa & \longrightarrow & \mathcal{G} \\ L & \longmapsto & \{\sigma \in \Gamma \mid \sigma\alpha = \alpha \text{ para todo } \alpha \in L\} = Aut(N \mid L) \end{array}$$

e

$$\begin{array}{rcl} k : \mathcal{G} & \longrightarrow & \kappa \\ \Delta & \longmapsto & \{\alpha \in N \mid \sigma\alpha = \alpha \text{ para todo } \sigma \in \Delta\} = \text{ corpo fixo de } \Delta. \end{array}$$

Proposição 1.2.1 *As aplicações $g : \kappa \longrightarrow \mathcal{G}$ e $k : \mathcal{G} \longrightarrow \kappa$ invertem a inclusão e satisfazem:*

(i) $L \subseteq kg(L)$ *para todo* $L \in \kappa$;

(ii) $\Delta \subseteq gk(\Delta)$ *para todo* $\Delta \in \mathcal{G}$;

(iii) $g(K) = \Gamma$ *e* $g(N) = \{id_N\}$;

(iv) $k(\{id_N\}) = N$ *e* $k(\Gamma) \supseteq K$.

A demonstração da proposição anterior segue na página 86 de O. Endler ([4]).

Proposição 1.2.2 *Denotando por κ^* a imagem $k(\mathcal{G})$ e por $\mathcal{G}^*$ a imagem $g(\kappa)$, temos que $\kappa^* \subseteq \kappa$ e $\mathcal{G}^* \subseteq \mathcal{G}$ e podemos concluir:*

(1) $L \in \kappa^*$ *se, e somente se,* $L = kg(L)$ *e* $\Delta \in \mathcal{G}^*$ *se, e somente se* $\Delta = gk(\Delta)$.

(2) g e k induzem bijeções entre κ^* e $\mathcal{G}^*$ sendo uma a inversa da outra.

A demonstração da proposição anterior segue na página 87 de O. Endler ([4]).

Quando o par de aplicações de uma conexão de Galois forem bijetivas a chamamos de *correspondência de Galois* entre os conjuntos κ e $\mathcal{G}$, ordenados pela inclusão. Uma conexão de Galois induz uma correspondência $\kappa^* \longleftrightarrow \mathcal{G}^*$. Uma extensão galoasiana finita implica em uma correspondência de Galois.

1.3 Espaços afins e conjuntos algébricos

As definições, os conceitos e resultados apresentados nas próximas quatro seções podem ser encontrados nos textos "Introdução às Curva Algébricas Planas" de I. Vainsencher em [20] ou "Algebraic Curves" de W. Fulton em [5].

Sejam k um corpo e n um número inteiro positivo. O *espaço afim n-dimensional* ou o *n-espaço afim* sobre k é o conjunto

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

Os elementos de $\mathbb{A}^n$ são chamados *pontos*. O conjunto $\mathbb{A}^1$ é a *reta afim* e $\mathbb{A}^2$ é o *plano afim*.

Seja $F \in k[X_1, \ldots, X_n]$ um polinômio nas indeterminadas $X_1, \ldots, X_n$ sobre k. Um ponto $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ é um *zero* de F se $F(a_1, \ldots, a_n) = 0$. Se F não for um polinômio constante, o conjunto dos zeros de F é chamado de *hipersuperfície* definida F, e denotada por $V(F)$. Consideremos a partir daqui que k seja um corpo algebricamente fechado, é possível verificar que dados dois polinômios $F, G \in k[X_1, \ldots, X_n]$ que possuem os mesmos fatores irredutíveis, tem-se que $V(F) = V(G)$ se, e somente se, existe um elemento não nulo $\lambda \in k$ tal que $G = \lambda F$. Assim, uma hipersuperfície pode ser identificada como uma classe de equivalência de polinômios não constantes em $k[X_1, \ldots, X_n]$ que diz que dois polinômios F e G são equivalentes quando existe um elemento não nulo $\lambda \in k$ tal que $G = \lambda F$. Uma hipersuperfície em $\mathbb{A}^2(k)$ é chamada de *curva algébrica plana afim* ou abreviadamente *curva*. A equação da curva é qualquer um dos polinômios da classe de equivalência que a define.

Mais geralmente, suponha que S seja um conjunto qualquer de polinômios em $k[X_1, \ldots, X_n]$. O conjunto

$$V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ para todo } F \in S\},$$

é denominadado *conjunto de zeros* de S. Quando $S = \{F_1, \ldots, F_r\}$, vamos escrever $V(F_1, \ldots, F_r)$, em vez de $V(\{F_1, \ldots, F_r\})$.

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

Para um subconjunto qualquer X de $\mathbb{A}^n$, considere o conjunto dos polinômios que se anulam em X. Este conjunto forma um ideal do anel $k[X_1, \ldots, X_n]$,

que é chamado ideal de X e é denotado por I(X). Assim,

$$I(X) = \{F \in k[X_1, \ldots, X_n] \mid F(a_1, \ldots, a_n) = 0 \text{ para todo } (a_1, \ldots, a_n) \in X\}.$$

O Teorema da Base de Hilbert garante que todo ideal de $k[X_1, \ldots, X_n]$ é finitamente gerado. Com isso, os conjuntos algébricos de $\mathbb{A}^n$ são exatamente o lugar dos pontos que satisfazem um número finito de equações polinomiais em n indeterminadas sobre k.

Um conjunto algébrico pode ser a reunião de vários outros conjuntos algébricos. Dizemos que um conjunto algébrico $X \subset \mathbb{A}^n$ é *redutível* se $X = X_1 \cup X_2$, onde X_1 e X_2 são também conjuntos algébricos e diferentes de X. No caso contrário, dizemos que X *irredutível*. Um conjunto algébrico X é irredutível se, e somente se $I(X)$ é um ideal primo. Um conjunto algébrico irredutível é denominado *variedade algébrica afim* ou, simplesmente, *variedade*.

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

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

é um domínio de integridade, pois $I(V)$ é um ideal primo. Este anel é chamado *anel de coordenadas* de V. Esta nomenclatura vem do fato que $k[V]$ 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 ver isto da seguinte forma. Seja $\mathcal{F}(V, k)$ o conjunto de todas as funções de V em k. $\mathcal{F}(V, k)$ tem naturalmente uma estrutura de anel com as operações usuais de soma e produto de funções, pois k é um corpo. Uma função $\varphi \in \mathcal{F}(V, k)$ é chamada *função polinomial* quando existe um polinômio $g \in k[X_1, \ldots, X_n]$ tal que $\varphi(P) = g(P)$ para todo $P \in V$.

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

Agora considere $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ variedades. Uma aplicação $\phi : V \longrightarrow W$ é *polinomial* se existem polinômios $G_1, \ldots, G_m \in k[X_1, \ldots, X_n]$ tais que

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

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

de aneis $\tilde{\phi} : k[W] \longrightarrow k[V]$ definida por $\tilde{\phi}(\varphi) = \varphi \circ \phi$. Além disso, todo k-homomorfismo de k-álgebras $\psi : k[W] \longrightarrow k[V]$ é da forma $\psi = \tilde{\phi}$ para alguma aplicação regular $\phi : V \longrightarrow W$. Assim, há uma correspondência entre as aplicações regulares de V em W e k-homomorfismo de k-álgebras entre $k[W]$ e $k[V]$.

Como salientamos acima, sendo V uma variedade, então $k[V]$ é um domínio de integridade. Podemos então considerar o seu corpo de frações, que denominamos por *corpo de funções de* V e o representamos por $k(V)$. Assim,

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

Além disso, como no caso do anel de coordenadas, podemos ver os elementos de $k(V)$ "funções"de V em k, ressalvando agora que tais "funções"podem não estar definidas em todos os pontos de V. De fato, a princípio $\frac{g}{h} \in k(V)$ pode não ser uma função de V em k, devido aos zeros de h, no entanto está bem definida em $P \in V$ sempre que $h(P) \neq 0$. Mesmo assim, nos permitindo um abuso de linguagem e seguindo uma nomenclatura clássica, chamamos $\frac{g}{h}$ de função e a denominamos *função racional* de V em k. No caso em que $h(P) = 0$, dizemos P é *polo* da função racional $\frac{g}{h}$. Por outro lado, se $h(P) \neq 0$, para alguma tal representação, dizemos que a função é *regular* em P.

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

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

É fácil ver que $\mathcal{O}_P(V)$ é um subanel de $k(V)$ que contém $k[V]$. Assim, temos as seguintes inclusões:

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

Uma aplicação $\phi : V \dashrightarrow \mathbb{A}^n$ é *racional* se existem funções racionais $\varphi_1, \ldots, \varphi_n$ tais que $\phi(P) = (\varphi_1(P), \ldots, \varphi_n(P))$ para todo P na interseção dos domínios das funções φ_i, para $i = 1, \ldots, n.$. Uma aplicação racional $\phi : V \dashrightarrow W$ entre duas variedades $V \subset \mathbb{A}^n$ e $W \subset \mathbb{A}^m$ é uma aplicação racional $\phi : V \dashrightarrow \mathbb{A}^m$ tal que a imagem do domínio da ϕ esteja contido em W. Uma aplicação racional $\phi : V \dashrightarrow W$ é dita ser *bi-racional* se existe uma aplicação racional

$\psi : W \dashrightarrow V$ tal que $\phi \circ \psi = Id$ e $\psi \circ \phi = Id$ nos seus respectivos domínios de definição. Duas curvas são *birracionalmente equivalentes* quando existe uma aplicação bi-racional entre elas. É fácil verificar que duas curvas são birracionalmente equivalentes se, e somente se, seus corpos de funções são isomorfos.

1.4 Algumas propriedades das curvas planas

As propriedades de curvas algébricas planas que estamos interessados em estudar precisam independer do particular sistema de coordenadas cartesianas empregado para representá-las. Um *referencial* ou *sistema de coordenadas afim* no plano $\mathbb{A}^2$ consiste na escolha de um ponto $O \in \mathbb{A}^2$, chamado origem do referencial, e de uma base $\{v_1, v_2\}$ do espaço vetorial k^2. O *referencial canônico* é dado por $O = (0,0), v_1 = (1,0), v_2 = (0,1)$. O vetor coordenadas de um ponto $P \in \mathbb{A}^2$ em relação a um referencial $\mathcal{R} = \{O, \{x_1, x_2\}\}$ é o par $(P)_{\mathcal{R}} = (x_1, x_2) \in \mathbb{A}^2$ tal que $P = O + x_1 v_1 + x_2 v_2$.

Uma *transformação afim* ou *afinidade* em $\mathbb{A}^2$ é uma aplicação $T : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ dada pela composição de uma translação com um isomorfismo linear, isto é, $T(x_1, x_2) = (y_1, y_2)$, onde

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

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

Seja $f \in k[x, y]$ uma equação afim para a curva C e seja P um ponto de C. Sem perda de generalidade (considerando mudanças afins de coordenadas) podemos supor $P = (0,0)$. Podemos escrever $f = f_m + f_{m+1} + \cdots + f_d$, onde cada f_i é um polinômio homogêneo de grau i para $m \leqslant i \leqslant d$ e $f_m \neq 0$. O inteiro m é a *multiplicidade* do ponto P na curva C ou a *multiplicidade* de C em P. Se $P \notin C$, então $m = 0$, se $P = (a, b) \in C$, escrevemos

$$f(X + a, Y + b) = f_m(X, Y) + (\textit{termos de grau} > m).$$

O polinômio homogêneo $f_m(X, Y)$ pode ser decomposto de maneira única,

$$f_m = \prod (a_i(X - a) + b_i(Y - b))^{n_i},$$

onde os fatores lineares $a_i X + b_i Y$ são retas distintas. As retas $l_i = (a_i(X - a) + b_i(Y - b))$ são as *retas tangentes* a f em P. O expoente n_i é a *multiplicidade* da tangente l_i.

Um ponto $P = (a, b)$ de uma curva C é dito *ponto simples* ou *ponto não-singular* ou *ponto regular* de C se

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

Caso contrário, P é *ponto singular* ou uma *singularidade* de C. Se um ponto $P = (a, b)$ de uma curva C é um ponto regular, a única *reta tangente* a C em P é a reta dada pela equação:

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

Seja $f = f_0 + f_1 + \cdots + f_d$ um polinômio de grau d nas indeterminadas X e Y escrito como soma de componentes homogêneas, com $f_d \neq 0$. A *homogeneização* de f, isto é, o polinômio homogêneo de grau d nas indeterminadas X, Y e Z obtido a partir de f é o seguinte:

$$f^*(X, Y, Z) = \sum_{i=0}^{d} Z^{d-i} f_i(X, Y).$$

Para polinômios homogêneos as seguintes relações são satisfeitas:

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

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

1.5 Plano projetivo e curvas projetivas

A ideia de acrescentar ao plano euclidiano uma reta no infinito, construindo assim o plano projetivo, é devida a Desargues (1591-1661) que pretendia dar uma fundamentação matemática aos métodos de perspectiva empregados por pintores e arquitetos.

A concepção de Desargues do plano projetivo é considerar o plano afim mergulhado no espaço tridimensional como o plano π de equação $Z = 1$, representado na Figura 1.1. Cada ponto do plano π determina uma reta passando pela origem e pelo dado ponto. Cada reta de π determina um plano pela origem.

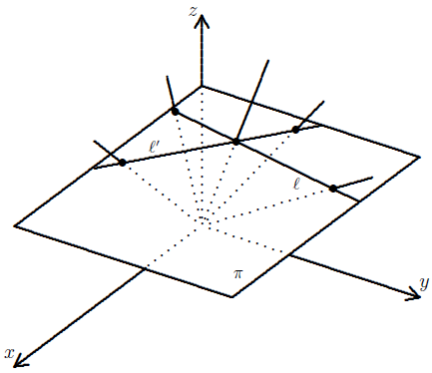

Figura 1.1: Representação do Plano projetivo. Fonte: ([20]).

O *plano projetivo* $\mathbb{P}^2$ é o conjunto das retas do espaço tridimensional que passam pela origem. O plano π se identifica como um subconjunto de $\mathbb{P}^2$. Os pontos de $\mathbb{P}^2 - \pi$ são chamados de *pontos no infinito*.

Denotamos por $(x : y : z)$ o ponto de $\mathbb{P}^2$ que representa a reta ligando a origem O a um ponto $(x, y, z) \neq O$. Naturalmente, qualquer ponto dessa reta que não seja a origem, pode ser tomado para representá-la em $\mathbb{P}^2$, pois, $(x : y : z) = (x' : y' : z')$ se, e somente se, existe constante não nula $\lambda \in k$ tal que $(x, y, z) = \lambda(x', y', z')$. Como veremos mais geralmente logo abaixo, isto define uma relação de equivalência em $\mathbb{A}^3 \setminus \{0, 0, 0\}$, cujo conjunto de classes é $\mathbb{P}^2$ e (x, y, z) é apenas um representante de sua classe. Dizemos que x, y, z são as *coordenadas homogêneas* do ponto $(x : y : z)$ relativas à base canônica $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. Em geral, fixada uma base qualquer no espaço tridimensional, as coordenadas de um ponto diferente de zero relativas a essa base são também chamadas de coordenadas homogêneas do ponto correspondente de $\mathbb{P}^2$. E estas só estão bem definidas a menos de um fator escalar diferente de zero. Além disso, vamos considerar os *pontos do infinito* de $\mathbb{P}^2$ como sendo os pontos $P = (x : y : z)$ tais que $z = 0$ e os pontos finitos são tais que $z \neq 0$.

Em geral, o *espaço projetivo n-dimensional* $\mathbb{P}^n(k)$ é obtido através da relação de equivalência $\sim$ definida no espaço afim $(n+1)-$dimensional, como segue. Dados os pontos $(a_0, a_1, \ldots, a_n), (b_0, b_1, \ldots, b_n)$ em $\mathbb{A}^{n+1} \setminus \{0, \ldots, 0\}$, dizemos que $(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n)$, se, e somente se, existe λ não nulo em k, tal que $b_i = \lambda a_i$ para $0 \leq i \leq n$. A classe de equivalência de $(a_0, a_1, \ldots, a_n)$ é representada por $(a_0 : a_1 : \ldots : a_n)$. O espaço projetivo n-dimensional é o conjunto $\mathbb{P}^n = \mathbb{P}^n(k) = \{(a_0 : a_1 : \ldots : a_n) \mid a_i \in k$, não todos nulos$\}$.

Uma *curva algébrica plana projetiva* é o conjunto algébrico projetivo de $\mathbb{P}^2$ definido por um polinômio homogêneo não constante em três indeterminadas, que denotaremos, neste caso, por X, Y, Z. Como no caso afim, considerando k um corpo algebricamente e utilizando o teorema dos zeros de Hilbert, podemos verificar que dois polinômios definem a mesma curva quando diferem apenas pela multiplicação por uma constante não nula de k. O *grau* de uma curva projetiva é o grau de um polinômio homogêneo que a define. Seja C uma curva plana projetiva definida pelo polinômio homogêneo $F = F(X, Y, Z)$. A parte afim de C é a curva algébrica afim definida pela desomogeneização de F em relação à variável Z, isto é, $F_*(X, Y) = F(X, Y, 1)$. (A escolha da indeterminada Z é arbitrária).

O estudo da teoria local das curvas projetivas planas recai no caso 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 associado a P é o conjunto $\mathcal{O}_P(\mathbb{P}^2)$ definido por:

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

Verifica-se facilmente que $\mathcal{O}_P(\mathbb{P}^2)$ 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 contém P.

Seja C uma curva projetiva definida pelo polinômio homogêneo F. Um ponto $P = (a : b : c) \in C$ é um *ponto regular* ou *não singular* de C se ao menos uma das derivadas parciais de F em relação as variáveis X, Y e Z não se anula no ponto P. Caso contrário P é dito *ponto singular* ou uma *singularidade*.

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

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

Seja $T : k^3 \longrightarrow k^3$ um isomorfismo linear. Visto que uma tal aplicação preserva retas de k^3 passando pela origem, temos definida uma bijeção natural, que, por abuso de linguagem também denotamos por $T : \mathbb{P}^2 \longrightarrow \mathbb{P}^2$ e a chamamos de *projetividade* ou *mudança projetiva de coordenadas* em $\mathbb{P}^2$.

Além disso, T também induz um k-isomorfismo de anéis em $k[X, Y, Z]$, a saber,

$$T_\bullet : k[X, Y, Z] \longrightarrow k[X, Y, Z]$$

tal que, para todo $(x, y, z) \in k^3$ e todo polinômio $f \in k[X, Y, Z]$, por avaliação, tem-se

$$(T_\bullet f)(x, y, z) = f(T^{-1}(x, y, z)).$$

Escrevendo $X = X_1$, $Y = X_2$ e $Z = X_3$ e designando por (a_{ij}) a matriz de T^{-1} relativa a base canônica de k^3, temos

$$(T_\bullet f)(X_1, X_2, X_3) = f(\Sigma a_{1j}X_j, \Sigma a_{2j}X_j, \Sigma a_{3j}X_j).$$

A imagem de uma curva projetiva F por uma projetividade T é a curva definida por $T_\bullet F$. As curvas F e $T_\bullet F$ são ditas congruentes. Propriedade como o grau, a colinearidade de pontos e redutibilidade de uma curva são invariantes por projetividade.

Precisaremos utilizar o resultado seguinte. Um automorfismo de uma curva não singular de grau $d \geq 4$ em $\mathbb{P}^2$ pode ser estendido a uma transformação projetiva de $\mathbb{P}^2$. Isto pode ser encontrado em Arbarello et. al. ([1], Apêndice A, 17 e 18) e Chang ([3]).

1.6 Multiplicidade de interseção

Uma das motivações da introdução do plano projetivo foi a intenção de resolver a questão da não intersecção de retas. Em $\mathbb{P}^2$, duas retas sempre se intersectam. Na realidade em $\mathbb{P}^2$ duas curvas projetivas planas quaisquer sempre se intersectam. Mais que isso, é possível contar o número dessas intersecções utilizando a multiplicidade ou índice de interseção entre elas em cada ponto.

A *multiplicidade* ou *índice de interseção* de duas curvas projetivas num ponto qualquer do plano projetivo pode ser definidas de duas formas clássicas. A primeira é via a codimensão do ideal gerado pelas equações das duas curvas no anel de polinômios localizado no ponto em estudo. Dessa forma é definida em ([5]). A segunda utiliza a resultante dos dois polinômios. Essa abordagem é encontrada em ([20]).

Ambas definições satisfazem naturamente os axiomas que determinam unicamente a multiplicidade de interseção de curvas planas projetivas que, na verdade, fornecem um algorítimo efetivo para sua determinação. Esses axiomas serão listados a seguir.

Dadas duas curvas planas projetivas F e G, dizemos que elas se intesectam 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 dessas duas curvas no ponto P, que denotaremos por $I_P(F,G)$, satisfaz as seguintes propriedades:

(1) $I_P(F,G) = I_P(G,F) \in \mathbb{N} \cup \{\infty\}$.

(2) $I_P(F,G) = 0$ se, e somente se, $P \notin F \cap G$.

(3) $I_P(F,G) = \infty$ se, e somente se, P está em uma componente comum de F e G.

(4) Se $T : \mathbb{P}^2 \longrightarrow \mathbb{P}^2$ é uma mudança projetiva de coordenadas então $I_P(F,G) = I_{T(P)}(F^T, G^T)$, onde F^T e G^T são as respectivas equações das curvas transformadas por T.

(5) Se X e Y denotam os eixos coordenados afins $I_P(X,Y) = 1$, onde $P = (0:0:1)$.

(6) $I_P(F,(G+AF)) = I_P(F,G)$ para todo $A \in k[X,Y,Z]$ homogêneo com $grA = grG - grF$.

(7) $I_P(F,(G_1G_2)) = I_P(F,G_1) + I_P(F,G_2)$.

Dados uma curva plana projetiva C definida pelo polinômio F e um ponto P não singular de C, a reta tangente T_P é a única reta de $\mathbb{P}^2$ que tem multiplicidade de interseção maior do que um com C em P, ou seja, $I_P(C,T_P) \geq 2$. No caso em que $I_P(C,T_P) \geq 3$, dizemos que P é um *ponto de inflexão* de C, e neste caso, dizemos que T_P é uma *reta tangente inflexi-onal*. No caso em que $I_P(C,T_P) = 3$ dizemos que P é um *ponto de inflexão ordinário*. Mais geralmente, se $I_P(C,T_P) = m \geq 3$, diremos que P é um *ponto de inflexão de ordem* $m-2$.

Exemplo 1.6.1

Sejam $F = X^3Y - XYZ^2 + Y^3Z + Z^4$ o polinômio que define a curva C, $P = (1:0:0)$ e $Q = (0:1:0)$. Iremos calcular $I_P(C,T_P)$ e $I_Q(C,T_Q)$.
Temos que $T_P = Y$ e $T_Q = Z$, seguem que

$$I_P(C,T_P) = I_P(X^3Y - XYZ^2 + Y^3Z + Z^4, Y) = I_P(Z^4,Y) = 4I_P(Z,Y) = 4,$$

$$I_Q(C,T_Q) = I_Q(X^3Y - XYZ^2 + Y^3Z + Z^4, Z) = I_Q(X^3Y,Z) = I_Q(X^3,Z) + I_Q(Y,Z) = 3.$$

Logo P é uma inflexão de ordem 2 e Q é uma inflexão de ordem 1.

No contexto do cálculo diferencial e integral ($k = \mathbb{R}$), os pontos de inflexão de uma curva que é gráfico de uma função são aqueles pontos onde a segunda derivada muda de sinal. No contexto das curvas algébricas (em característica zero), os pontos de inflexão de curvas dadas por gráficos de funções são pontos onde a segunda derivada se anula.

No caso de característica positiva $p \neq 2$ temos o seguinte critério para que um ponto P seja um ponto de inflexão. Seja $f(x, y) = F(x, y, 1)$ uma equação afim para C. Um ponto não singular (finito) $P \in C$ é um ponto de inflexão de C se, e somente se, a matriz

$$h(f) = \begin{bmatrix} f_{xx} & f_{xy} & f_x \\ f_{xy} & f_{yy} & f_y \\ f_x & f_y & 0 \end{bmatrix},$$

tem posto menor que 3 no ponto P.

Podemos estimar o número máximo de pontos de inflexão da curva C de grau d da forma seguinte. Defina

$$W(C) := \sum_{Q \in C} (I_Q(C, T_Q) - 2).$$

O lema seguinte nos dá a estimativa.

Lema 1.6.2 *Suponha que* $\dfrac{d^2y}{dx^2}$ *não seja identicamente nulo. Então*

$$W(C) \leq 3d(d-2).$$

O lema segue de alguns resultados sobre pontos de inflexão, encontrados em ([11],p.294). Esses resultados podem ser vistos como generalizações das fórmulas clássicas de Plucker.

O teorema de Bézout é um resultado central na teoria das curvas planas projetivas. Afirma que o número de pontos de intersecção, contados com multiplicidades, de duas curvas planas projetivas sem componentes comuns, é igual ao produto de seus graus:

Teorema 1.6.3 *Sejam F e G duas curvas planas projetivas sem componentes em comum de graus d_F e d_G respectivamente. Então,*

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

1.7 Aplicações separáveis e inseparáveis

Os resultados desta secção estão essencialmente em R.Pardini ([14]). Como antes, sejam k um corpo algebricamente fechado e $C \subseteq \mathbb{P}^2$ uma curva plana projetiva irredutível de grau d e F uma equação homogênea para C.

Denotemos por F_i a derivada parcial de F em relação à i-ésima indeterminada $(0 \leq i \leq 2)$ e $\mathbb{P}^{2^*}$ o plano projetivo dual associado a $\mathbb{P}^2$. A aplicação racional

$$\begin{array}{rcl} \varphi : C & \longrightarrow & \mathbb{P}^{2^*} \\ P & \longmapsto & (F_0(P), F_1(P), F_2(P)) \end{array}$$

é chamada *aplicação dual*. Essa aplicação associa cada ponto regular de C à sua reta tangente. O fecho projetivo de $\varphi(C)$ em $\mathbb{P}^{2^*}$, que denotamos por C^*, é chamada *curva dual* de C. No caso em que C é não singular claramente φ é uma aplicação regular.

Quando um corpo tem característica zero, a aplicação $\varphi : C \longrightarrow C^{**}$ é birracional. Isto não é sempre verdade para corpos de característica finita. Neste caso temos a seguinte definição:

Sejam $\varphi : C \longrightarrow C^*$ e $\phi : C^* \longrightarrow C^{**}$ aplicações dual. Dizemos que C é *reflexiva* se

(a) $C^{**} = C$;

(b) $\phi \cdot \varphi = id_C$.

Temos os seguintes resultados

Proposição 1.7.1 *C é reflexiva se, e somente se, φ é separável.*

Corolário 1.7.2 *Se a característica de k é zero, então C é reflexiva.*

Proposição 1.7.3 *Sejam k corpo de característica p, com $p \neq 2$ e $\varphi : C \longrightarrow C^*$ aplicação dual. Então,*

(a) φ é inseparável se, e somente se, C tem infinitas inflexões.

(b) Se φ é separável então C tem quantidade finita de bitangentes, isto é, há uma quantidade finita de retas tangentes à C em mais de um ponto.

A demonstração da proposição anterior segue na página 5 de R.Pardini ([14]).

A próxima proposição fornece uma relação entre os pontos de inflexão de C com a matriz Hessiana do polinômio que representa a curva C.

Proposição 1.7.4 *Se $cark = 0$ ou $cark = p$, tal que $p \neq 2$, onde p não divide $(d-1)$, então um ponto regular P de C é uma inflexão se, e somente se, a matriz hessiana de C em P é zero.*

A demonstração da proposição anterior segue em R.Pardini ([14]) na página 6 .

Teorema 1.7.5 *Se a $cark = p$, tal que $p \geq 3$ e se C é uma curva plana não singular com infintos pontos de inflexão, então $F_{ij} = 0$ para $i, j = 0, 1, 2$.*

A demonstração do teorema anterior segue na página 7 de R.Pardini ([14]).

Corolário 1.7.6 *Seja a característica de k igual a p, com $p \geq 3$. Se C é uma curva não singular de grau d, com infinitos pontos de inflexão, então $p \mid (d-1)$.*

A demonstração do corolário anterior segue na página 8 de R.Pardini ([14]).

Proposição 1.7.7 *Se $cark = p$, $p \neq 2$. Seja C uma curva plana não singular de grau $p+1$ com infinitos pontos de inflexão. Então C é projetivamente equivalente a curva dada pela equação*

$$XY^p + YZ^p + ZX^p = 0.$$

A demonstração da proposição anterior segue na página 13 de R.Pardini ([14]).

Capítulo 2

PONTOS DE GALOIS

2.1 Contextualização

Queremos estudar pontos de Galois em curvas planas projetivas em característica positiva. Para isto, precisamos conhecer propriedades de uma projeção de uma curva no plano projetivo $\mathbb{P}^2(k)$ sobre uma reta a partir de um ponto denominado centro de projeção. Este ponto pode estar (ponto interno) ou não (ponto externo) na curva. Vamos começar ilustrando a situação através de dois exemplos típicos.

Exemplo 2.1.1

Seja C a cúbica não singular definida pela equação

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

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

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

Podemos ver a aplicação π da seguinte forma: Considere a reta $L'_{(a:c)}$ que passa por P e $(a : 0 : c)$, a saber, $L'_{(a:c)} : cX - aZ = 0$. Então

$$\pi(a : b : c) = L \cap L'_{(a:c)} = (a : 0 : c).$$

Em coordenadas afins, π é a projeção vertical de $C_* = \{(a, b) \mid b^2 = a^3 - 1\}$ sobre o eixo x, isto é $\pi(a, b) = a$. Naturalmente para $(a : c) \in \mathbb{P}^1$ genérico, existem dois pontos Q, $R \in C$ tais que $\pi(Q) = \pi(R) = (a : c)$, a saber,

$Q = (a : b_1 : c)$ e $R = (a : b_2 : c)$, onde b_1 e b_2 são as duas raízes da equação $y^2c - a^3 + c^3 = 0$. Se $(a : c)$ é um ponto finito, isto é, $c \neq 0$, então podemos supor $c = 1$ e neste caso b_1 e b_2 são as duas raízes da equação $y^2 = a^3 - 1$. Quando $a^3 = 1$, esta equação se reduz $y^2 = 0$, portanto ela possui apenas uma solução (dupla). Esta é uma situação que, na linguagem clássica, a aplicação π é chamada de um *recobrimento duplo* de $\mathbb{P}^1$. Isto significa que C "recobre"a reta projetiva $\mathbb{P}^1$ duas vezes no sentido que , para $(a : b) \notin \{(1 : 1), (w : 1), (w^2 : 1)\}$, com $w^3 = 1$ e $w \neq 1$, tem-se que $\pi^{-1}(a : b)$ são dois pontos distintos de C. Essa é a situação geométrica. Do ponto de vista algébrico, temos que π induz uma inclusão de corpos de funções de $\mathbb{P}^1$ no corpo de funções de C, isto é, $k(\mathbb{P}^1) \subset k(C)$. Ora $k(\mathbb{P}^1) = k(x)$ e $k(C) = k(x, y) = k(x)[y]$, onde $y^2 = x^3 - 1$. Assim, $k(C) \mid k(\mathbb{P}^1)$ é a extensão de corpos $k(x)[y] \mid k(x)$ de grau 2. Portanto informações geométricas da projeção π podem ser obtidas da extensão $k(x)[y] \mid k(x)$.

Exemplo 2.1.2

Vamos apresentar um exemplo que apresenta pontos de Galois externos. Considere a quártica de Fermat C, que pode ser dada pela equação obtida do polinômio

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

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

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

Seja $L'_{(b:c)}$ a reta que passa por P e $(0 : b : c)$, a saber, $L'_{(b:c)} : cY - bZ = 0$. Temos que $\pi(a : b : c) = L \cap L'_{(b:c)} = \{(0 : b : c)\}$. 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 quarto 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 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 a sua imagem inversa $\pi^{-1}(b : c)$ é constituída de, no máximo, quatro pontos na curva C. Do ponto de vista algébrico, temos que π induz uma inclusão do corpo de funções de $\mathbb{P}^1$ no corpo de funções de C, isto é, $k(\mathbb{P}^1) \subset k(C)$. Podemos escrever $k(\mathbb{P}^1) = k(y)$

e $k(C) = k(x, y) = k(y)[x]$, onde $x^4 = 1 - y^4$, logo $k(C) \mid k(\mathbb{P}^1))$ é a extensão de corpos de grau 4 : $k(x, y) \mid k(y)$.

Em geral, seja dada uma curva projetiva não singular C de grau d e uma projeção π_P de C sobre uma reta l com centro de projeção no ponto P. Esta projeção induz uma extensão de corpos $k(C) \mid k(l)$. Se P é um ponto sobre a curva temos que o grau da extensão $k(C) \mid k(l)$ é igual a $d - 1$ e se P é um ponto fora da curva então o grau dessa extensão é igual a d. Este é o contexto que nos encontramos para estudar os pontos de Galois associados à curva C.

Definição 2.1.3 *Seja $C \subset \mathbb{P}^2$ uma curva plana projetiva não singular de grau $d \geqslant 4$. Um ponto $P \in \mathbb{P}^2$ é um ponto de Galois associado a C se a projeção $\pi_P : C \longrightarrow \mathbb{P}^1$ com centro P induz uma extensão de Galois $k(\mathbb{P}^1) \subset k(C)$ em seus corpos de funções. Chamamos $P \in \mathbb{P}^2$ de ponto de Galois inteno (respectivamente externo) de C se $P \in C$ (respectivamente $P \notin C$). Denotamos por $\delta(C)$ (respectivamente $\delta'(C)$) o número de pontos de Galois internos (respectivamente externos) de C.*

Em característica zero $d \geqslant 4$, Yoshihara (veja [22]) provou que o número de pontos de Galois internos pode ser igual a zero, um ou quatro e o número de pontos de Galois externos igual a zero, um ou três. O objetivo dessa dissertação é estudar o número de pontos de Galois internos e externos de uma curva plana regular em característica positiva.

As próximas três seções foram baseadas em ([7]) e ([8]) e a última em ([6]).

2.2 Pontos de Galois internos

Nesta seção, vamos considerar corpos de característica $p > 2$ e a curva C de grau $d \geq 4$ tal que $d \not\equiv 1$ módulo p. No que segue, por simplicidade de escrita, vamos identificar transformações projetivas de $\mathbb{P}^2$ com as matrizes que representam os correspondentes isomorfismos lineares de k^3.

Precisaremos do lema seguinte:

Lema 2.2.1 *Seja $\sigma : \mathbb{P}^2 \to \mathbb{P}^2$ um automorfismo não trivial tal que $\sigma^3 = I_{\mathbb{P}^2}$. Suponhamos que σ estabiliza as retas passando pelo ponto $(0 : 0 : 1)$. Então existe um automorfismo $\tau : \mathbb{P}^2 \to \mathbb{P}^2$ estabilizando as retas passando por $(0 : 0 : 1)$ tal que*

$$\tau^{-1}\sigma\tau = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta \end{bmatrix},$$

onde ζ é uma raiz cúbica primitiva da unidade.

Demonstração. Suponha que σ seja representado por uma matriz da seguinte forma

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & \zeta \end{bmatrix}.$$

Como a reta X é estável temos que $b = c = 0$. Da mesma forma, como a reta Y fica estável por σ então $d = f = 0$. Além disso, σ também estabiliza $X - Y$, portanto, $a = e$. Logo σ possui um representação da forma

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ g & h & \zeta \end{bmatrix}.$$

Por outro lado como $\sigma^3 = I_{\mathbb{P}^2}$, temos

$$A^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ g(1+\zeta)+g\zeta^2 & h(1+\zeta)+h\zeta^2 & \zeta^3 \end{bmatrix} = I_3,$$

onde I_3 é a matriz identidade 3×3. Como σ não é o automorfismo identidade, segue $\zeta \neq 1$. Então ζ é uma raíz cúbica primitiva da unidade. Observe que $(A - I)(A - \zeta I) = 0$, o que significa que o polinômio mínimo de A só possui raízes simples e, portanto, A é diagonalizável. A forma diagonal de A é $J = diag(1, 1, \zeta)$ e verifica-se facilmente que a matriz que realiza a diagonalização é

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{g\zeta}{\zeta-1} & \frac{h\zeta}{\zeta-1} & \zeta \end{bmatrix}.$$

Naturalmente, temos que $A = B^{-1}JB$. ■

Proposição 2.2.2 *Seja C uma curva algébrica plana projetiva sobre um corpo algebricamente fechado de característica $p > 2$ de grau $d \geq 4$, sendo $d \not\equiv 1$ módulo p. Então C possui um ponto de Galois interno P se, e somente se, é projetivamente equivalente à curva definida por*

$$X^{d-1}Z + G(Y, Z) \tag{2.1}$$

onde G é um polinômio homogêneo de grau d em Y e Z, sem raízes múltiplas e não divisível por Z.

Demonstração. Se necessário, após uma mudança projetiva de coordenadas, podemos supor que $P = (1 : 0 : 0) \in C$. Já que, $\pi_P(X, Y, Z) = (Y : Z)$, temos que $\pi_P(x, y, 1) = (y : 1)$ na parte afim $Z \neq 0$, onde $x = \dfrac{X}{Z}$ e $y = \dfrac{Y}{Z}$. Assim, obtemos a extensão finita de corpos $k(x, y)|k(y)$. Admita que P seja um ponto de Galois interno. Então essa extensão (galoisiana) tem grau $d-1$. Denote por G_P o seu grupo de Galois, que é cíclico de ordem $d-1$. Dado um elemento $\sigma \in G_P$, fica associado a ele um automorfisno $\phi : C \to C$ de tal forma que $\phi(x, y, 1) = (\sigma(x), \sigma(y), 1)$. A inclusão de uma curva não singular de grau $d \geq 4$ em $\mathbb{P}^2$ é uma imersão canônica, portanto, os automorfismos de C podem ser estendidos a uma transformação projetiva de $\mathbb{P}^2$. Assim, por um abuso de linguagem, podemos dizer que ϕ é uma transformação projetiva de $\mathbb{P}^2$. Seja $A_\sigma = (a_{ij})$ uma matriz 3×3 que representa ϕ, digamos:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} \sigma(x) \\ \sigma(y) \\ 1 \end{bmatrix}.$$

Como $\sigma(y) = y$, temos

$$\begin{aligned} a_{11}x + a_{12}y + a_{13} &= \sigma(x) \\ a_{21}x + a_{22}y + a_{23} &= \sigma(y) = y \\ a_{31}x + a_{32}y + a_{33} &= 1, \end{aligned}$$

e $f := (a_{21}x + a_{22}y + a_{23}) - (a_{31}x + a_{32}y + a_{33})y$ é nulo sobre C. Já que $gr(C) > 2$, necessariamente f é o polinômio nulo. Isto acarreta $a_{21} = a_{23} = a_{31} = a_{32} = 0$ e $a_{22} = a_{33}$. Podemos assumir $a_{22} = a_{33} = 1$. Se $a_{11} = 1$, então $a_{12} = a_{13} = 0$, pois os elementos $(1, 2)$ e $(1, 3)$ de A_σ^{d-1} são $(d-1)a_{12}$ e $(d-1)a_{13}$, respectivamente, e $d - 1 \not\equiv 0$ módulo p por hipótese. Considere o homomorfismo injetivo de grupo, $det : G_P \to k - \{0\}$. Como G_P é cíclico de ordem $d-1$, assumindo que σ seja um gerador, então temos $a_{11} = \zeta$ que é uma raíz $(d-1)$-ésima primitiva da unidade. Assim, A_σ tem autovalores ζ e 1, e é diagonalizável. Portanto, existe uma matriz inversível Q, tal que

$$QA_\sigma Q^{-1} = \begin{bmatrix} \zeta & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Consequentemente podemos assumir $\sigma(x) = \zeta x$ e temos que $\sigma(x^{d-1}) = \sigma(x)^{d-1} = \zeta^{d-1}x^{d-1} = x^{d-1}$. Então $x^{d-1} \in k(y)$, daí podemos escrever $x^{d-1} + g(y) = 0$, onde g é um polinômio de grau d. Ao homogenizar temos, $X^{d-1}Z + G(Y, Z)$ e obtemos o resultado. ■

Corolário 2.2.3 *Sob as mesmas hipóteses da proposição 2.2.2, se C possui um ponto de Galois interno P, então este ponto é uma inflexão de ordem $(d-2)$ e há d inflexões de ordem $(d-3)$ e, além disso, a reta tangente em cada uma dessas inflexões contém P.*

Demonstração. Suponha que C possua um ponto de Galois interno. Então, pela proposição anterior, C é projetivamente equivalente à curva definida por $F = F(X,Y,Z) = X^{d-1}Z + G(Y,Z)$. A reta tangente a (F) num ponto R é dada por

$$T_R : X((d-1)X^{d-2}Z) + YG_Y(Y,Z) + Z(G_Z(Y,Z) + X^{d-1}).$$

Assim, a reta $Z = 0$ é a reta tangente no ponto de Galois $P = (1:0:0)$ e intercecta C somente em P, uma vez que

$$I_P(X^{d-1}Z + G(Y,Z), Z) = I_P(G(Y,Z), Z) = d.$$

Portanto P é uma inflexão de ordem $d-2$. Agora vamos encontrar as demais inflexões de C (que estão na parte afim, isto é, $Z \neq 0$). Considere as deshomogenizações $f(x,y) = F(x,y,1)$ e $g(y) = G(y,1)$. A matriz hessiana de f é dada por

$$\begin{aligned} h(f) &= \begin{bmatrix} f_{xx} & f_{xy} & f_x \\ f_{xy} & f_{yy} & f_y \\ f_x & f_y & 0 \end{bmatrix} \\ &= \begin{bmatrix} (d-1)(d-2)x^{d-3} & 0 & (d-1)x^{d-2} \\ 0 & g"(y) & g'(y) \\ (d-1)x^{d-2} & g'(y) & 0 \end{bmatrix} \end{aligned}$$

Segue que

$$det(h(f)) = -(d-1)x^{d-3}[(d-2)(g'(y))^2 + (d-1)x^{d-1}g"(y)]$$

Um ponto finito de C é uma inflexão se, e somente se, o posto de $h(f)$ é estritamente menor que 3 nesse ponto. Se $x = 0$ então $g(y) = 0$ e, como $g(y)$ tem grau d e é um polinômio separável, então essa equação tem d raízes distintas. Seja $Q \in C$ um ponto situado na reta $X = 0$. Podemos assumir que G não tem o termo Z^d e $Q = (0:0:1)$. Então a reta tangente T_Q em Q é $T_Q = YG_Y(Y,Z)$, ou seja, $Y = 0$, assim $C \bigcap T_Q = \{Q, P\}$. Pela razão de T_Q não ser tangente a C em P, temos que $I_Q(C, T_Q) = d-1$, logo o ponto Q é uma inflexão de ordem $d-3$. Assim provamos que a reta tangente em Q contém P e o ponto Q é uma inflexão de ordem $d-3$. ■

Teorema 2.2.4 *Seja $C \subset \mathbb{P}^2$ uma curva não singular de grau $d \geq 4$ sobre um corpo algebricamente fechado de característica $p > 2$, onde $d \not\equiv 1$ módulo p. Então $\delta(C) = 0, 1$ ou 4. Se $\delta(C) = 4$, então $d = 4$. Além disso, para um ponto P de Galois interno, o grupo de Galois G_P é um grupo cíclico de ordem $d - 1$.*

Demonstração. O Corolário *2.2.3* afirma que para cada ponto de Galois interno em C existem d inflexões de ordem $d - 3$ e o ponto de Galois é uma inflexão de ordem $d - 2$. Ainda pelo Corolário *2.2.3* e Lema *1.6.2*, obtemos a seguinte desigualdade:

$$\delta(C)((d-2) + d(d-3)) \leq 3d(d-2).$$

Suponha que $\delta(C) \geq 2$ e seja Q outro ponto de Galois. Seja σ um gerador de G_P e $\phi_\sigma : C \to C$ o automorfismo correspondente a σ. Se $\phi_\sigma(Q) = Q$ então Q deve estar situado na reta $X = 0$ (pela forma da matriz representando σ como na prova da Proposição 2.1), ou seja $\sigma(y) = y$, os pontos que ficam fixos. Então Q não é um ponto de Galois, pois os pontos de C em $X = 0$ são inflexões da ordem $(d - 3)$. Portanto temos que $\phi_\sigma(Q) \neq Q$. Então $Q_2 = \phi_\sigma(Q)$ é também um ponto de Galois em C, pois a imagem de um ponto de Galois por uma transformação projetiva é também um ponto de Galois e assim $\phi_\sigma(C) = C$. Notemos que $\phi_\tau(Q) \neq Q$ para algum elemento $\tau \in G_P$ diferente da identidade, por isso $\phi_\sigma(\alpha, \beta) = (\zeta\alpha, \beta)$ se $Q = (\alpha, \beta)$ (como na prova da Proposição 2.1). Desta forma obtemos d pontos de Galois. Pela desigualdade $d \leq 4$ e por hipótese $d \geq 4$, logo $d = 4$ e $\delta(C) = 4$. Daí temos que cada ponto de Galois determina quatro pontos de inflexões ordinários, segue que $\delta(C) \cdot 6 \leq 24$, portanto $\delta(C) \leq 4$. Se C é uma quártica genérica, então $\delta(C) = 0$, pois não possui pontos P tais que $I_P(C, T_P) = 4$. ■

A demonstração do lema seguinte pode ser encontrado em H. Yoshihara ([22]).

Lema 2.2.5 *Sob as mesmas condições acima, um ponto $Q = (a, b) \in C$ é um ponto de Galois se, e somente se, $g_2^2 = 3g_1g_2$, onde g_i é a parte homogênea de $g(x, y) = f(x + a, y + b)$ de grau i.*

Proposição 2.2.6 *Seja C uma curva plana não singular de grau $d = 4$ sobre um corpo algebricamente fechado de caracteristica $p \geq 5$. Então $\delta(C) = 4$ se, e somente se, C é projetivamente equivalente a curva dada por $X^3Z+Y^4+Z^4$.*

Demonstração. Seja $S(X, Y) = Z^3Y + S_4(X, Y)$ a forma padrão, onde $S_4(X, Y)$ é um polinômio homogêneo de grau 4. Seja $\tau = [c_{ij}]$ uma transformação projetiva satisfazendo $\lambda S^\tau = G$ onde

$$G = G(X, Y, Z) = Z^3g_1 + Z^2g_2 + Zg_3 + g_4$$

e λ uma constante não nula. Escreva

$$\tau(X,Y,Z) = [c_{ij}] = \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} X' \\ Y' \\ Z' \end{bmatrix}.$$

isto é,

$$\begin{aligned} X' &= c_{11}X + c_{12}Y + c_{13}Z, \\ Y' &= c_{21}X + c_{22}Y + c_{23}Z, \\ Z' &= c_{31}X + c_{32}Y + c_{33}Z. \end{aligned}$$

Assim,

$$\begin{aligned} \lambda S^{\tau}(X,Y,Z) &= \lambda S(\tau(X,Y,Z)) = \lambda S(X',Y',Z') = \\ &= \lambda[(c_{31}X + c_{32}Y + c_{33}Z)^3(c_{21}X + c_{22}Y + c_{23}Z) + S_4(X',Y')]. \end{aligned}$$

Observe que como τ fixa o ponto $(0,0)$ temos que $c_{13} = c_{23} = 0$. Para encurtar as expressões vamos escrever $W = c_{31}X + c_{32}Y$ e $U = c_{21}X + c_{22}Y$. Assim,

$$\begin{aligned} \lambda S^{\tau}(X,Y,Z) &= \lambda[(W + c_{33}Z)^3U + S_4(X',Y')] = \\ &= \lambda[(W^3 + 3c_{33}W^2Z + 3c_{33}^2WZ^2 + c_{33}^3Z^3)U + S_4(X',Y')] = \\ &= \lambda(c_{33}^3UZ^3 + 3c_{33}^2WUZ^2 + 3c_{33}W^2UZ + W^3U + S_4(X',Y')). \end{aligned}$$

Seguem as seguintes igualdades:

$$\begin{aligned} g_0 &= 0 \\ g_1 &= \lambda c_{33}^3(c_{21}X + c_{22}Y) \\ g_2 &= 3\lambda c_{33}^2(c_{21}X + c_{22}Y)(c_{31}X + c_{32}Y) \\ g_3 &= 3\lambda c_{33}(c_{21}X + c_{22}Y)(c_{31}X + c_{32}Y)^2 \end{aligned}$$

Daqui obtemos que $g_2^2 = 3g_1g_3$ e

$$\begin{aligned} g_4 &= X'^4 + X'^3Y' + X'^2Y'^2 + X'Y'^3 + Y^4 = \\ &= c_{11}^4X^4 + c_{11}^3c_{22}X^3Y + c_{11}^2c_{22}^2X^2Y^2 + c_{11}c_{22}^3XY^3 + c_{22}^4Y^4 = \\ &= c_{11}^4X^4 + XY(c_{11}^3c_{22}X^2 + c_{11}^2c_{22}^2XY + c_{11}c_{22}Y^2) + c_{22}^4Y^4 = \\ &= c_{11}^4X^4 + XYg_2 + c_{22}^4Y^4. \end{aligned}$$

Tomando (c_{ij}) a matriz identidade, $g_1 = Y$, $g_2 = 0$, $g_3 = 0$ e $g_4 = X^4 + Y^4$. Substituindo em $G(X, Y, Z) = Z^3 g_1 + Z^2 g_2 + Z g_3 + g_4 = Z^3 Y + X^4 + Y^4$. ■

Exemplo 2.2.7 *Seja C uma quártica definida sobre um corpo algebricamente fechado e de característica $p > 3$ dada pela equação*

$$ZX^3 + a_4Y^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3 = 0.$$

Vamos determinar os seus pontos de Galois.

Observe que a reta tangente a C no ponto $P = (1 : 0 : 0) \in C$ é a reta do infinito $Z = 0$ e $I_P(ZX^3 + a_4Y^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3, Z) = 4$. Assim, P é o único ponto dessa reta tangente que está em C e, naturalmente é uma inflexão de ordem 2. Agora, para $Z \neq 0$, isto é, na parte finita de C, podemos considerar a sua equação afim, a saber, $f(x, y) = x^3 + a_4y^4 + a_3y^3 + a_2y^2 + a_1y = 0$. O determinante da matriz hessiana é

$$det(h(f)) = -9x^4(12a_4y^2 + 6a_3y + 2a_2)^2 - 6x(4a_4y^3 + 3a_3y^2 + 2a_2y + a_1).$$

Se $x = 0$ então $f(0, y) = a_4y^4 + a_3y^3 + a_2y^2 + a_1y$ tem quatro raízes distintas e cada uma delas é uma inflexão de ordem 1. Logo, o único ponto de Galois é o ponto do infinito $P = (1 : 0 : 0)$.

Observação 2.2.8

Se a característica do corpo for 3 então $det(h(f)) = 0$ é identicamente nulo. Isto significa que a aplicação dual é inseparável.

2.3 Pontos de Galois externo

Nesta seção, vamos supor que C seja uma curva plana algébrica projetiva não singular de grau $d \geq 4$ sobre um corpo algebricamente fechado de característica $p > 2$ e que $d \not\equiv 0$ módulo p.

Proposição 2.3.1 *Nas condições acima, a curva C tem um ponto de Galois externo se, e somente se, ela é projetivamente equivalente à curva dada por*

$$F(X, Y, Z) = X^d + G(Y, Z), \tag{2.2}$$

onde G é um polinômio homogêneo de grau d em Y, Z sem raízes múltiplas.

Demonstração. A prova segue o mesmo roteiro do caso anterior de pontos de Galois internos. Se necessário, após uma mudança projetiva de coordenadas, podemos supor que o ponto $P = (1 : 0 : 0) \notin C$. Considere a projeção $\pi_P(X, Y, Z) = (Y : Z)$, que na parte afim pode ser vista como $\pi_P(x, y, 1) = (y : 1)$, onde $x = \dfrac{X}{Z}$ e $y = \dfrac{Y}{Z}$. Então temos a extensão finita corpos $k(x, y) \mid k(y)$. Suponhamos que P seja um ponto de Galois externo de C. Então a extensão $k(x, y) \mid k(y)$ é galoisiana de grau d. Como antes, vamos denotar por G_P o seu grupo de Galois, que é cíclico de ordem d. Cada elemento $\sigma \in G_P$ determina o automorfismo $\phi : C \to C$ tal que $\phi = (\sigma(x) : \sigma(y) : 1)$. Novamente, como a inclusão de uma curva não singular de grau $d \geq 4$ em $\mathbb{P}^2$ é uma imersão canônica, o automorfismo de C pode ser estendido a uma transformação projetiva de $\mathbb{P}^2$, que a denotamos ainda por ϕ. Seja $A_\sigma = (a_{ij})$ uma matriz 3×3 que representa ϕ. Como $\sigma(y) = y$ segue que $\alpha := (a_{21}x + a_{22}y + a_{23}) - (a_{31}x + a_{32}y + a_{33})y$ é nulo sobre C. Como $gr(C) > 2$, necessariamente α é o polinômio nulo. Isto acarreta $a_{21} = a_{23} = a_{31} = a_{32} = 0$ e $a_{22} = a_{33}$. Sem perda de generalidade, podemos assumir $a_{22} = a_{33} = 1$. Se $a_{11} = 1$, então $a_{12} = a_{13} = 0$, pois os elementos de A_σ^d nas posições $(1, 2)$ e $(1, 3)$ são respectivamente da_{12} e da_{13}, e $d \not\equiv 0$ módulo p por hipótese. Considere o homomorfismo injetivo de grupos, $det : G_P \to k - \{0\}$ (lembre-se que G_P é cíclico de ordem d). Assuma que $\sigma \in G_P$ seja um gerador, então temos que $a_{11} = \zeta$ que é uma raíz d-ésima primitiva da unidade. Assim A_σ tem autovalores ζ e 1, e é diagonalizável. Portanto, existe uma matriz Q, tal que

$$QA_\sigma Q^{-1} = \begin{bmatrix} \zeta & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Consequentemente podemos assumir $\sigma(x) = \zeta x$ e temos que

$$\sigma(x^d) = \sigma(x)^d = \zeta^d x^d = x^d.$$

Então $x^d \in k(y)$, pode ser escrito como $x^d + g = 0$, onde g é um polinômio em y de grau $\leq d$. Ao homogenizar temos, $X^d + G(Y, Z)$ e obtemos o resultado que queremos. ■

Corolário 2.3.2 *Com as mesmas hipóteses acima, se a curva C (de grau d) tem um ponto de Galois externo, então existem d inflexões de ordem $d-2$ e cada uma das retas tangentes (inflexionais) contém este ponto.*

Demonstração. Se C possui um ponto de Galois externo, pela proposição anterior ela é projetivamente equivalente à curva definida pelo polinômio

dado em *(2.2)*. Pelo teorema de Bézout e por este polinômio possuir apenas raízes simples, a reta $X = 0$ intersecta C em exatamente d pontos. Seja $Q \in C$ um ponto posicionado na reta $X = 0$. Após uma possível mudança projetiva de coordenadas, podemos assumir que G contém o termo Z^d e que $Q = (0 : 0 : 1)$. Segue que a reta tangente a C em Q é

$$T_Q = X(dX^{d-1}) + Y(G_Y(Y, Z)) + Z(G_Z(Y, Z)),$$

isto é, T_Q é a reta Z, uma vez que $G_Z(Y, Z) \neq 0$. Segue que

$$I_Q(X^d + G(Y, Z), Z) = I_Q(X^d + Y^d, Z) = d, .$$

Logo a reta $Z = 0$ intersecta C somente em Q e, além disso, contém o ponto de Galois externo (infinito). ■

Teorema 2.3.3 *Seja $C \subset \mathbb{P}^2$ uma curva plana algébrica projetiva não singular de grau $d \geq 4$ sobre um corpo algebricamente fechado de característica $p > 2$, onde $d \not\equiv 0$ módulo p. Seja ainda $\delta'(C)$ a quantidade de pontos de Galois externos de C. Tem-se*

(1) Se $d \not\equiv 1$ módulo p então $\delta'(C) = 0, 1$ ou 3.

(2) Se $d \equiv 1$ módulo p e C tem um a aplicação dual separável então $\delta'(C) = 0$ ou 1.

(3) Para um ponto P de Galois externo, o grupo de Galois G_P induzido pelo ponto de Galois P é um grupo cíclico de ordem d.

Demonstração. O Corolário *(2.3.2)* afirma que para cada ponto de Galois externo P, temos d inflexões da ordem $d-2$. Também pelo Corolário *(2.3.2)* e Lema *(1.6.2)*, obtemos a desigualdade seguinte

$$\delta'(C)((d-2) + (d-1)(d-2)) \leq 3d(d-2), \text{ isto é, } \delta'(C) \leq 3.$$

Suponha $\delta'(C) \geq 2$ e seja Q outro ponto de Galois externo (além de P). Seja σ um gerador do grupo de Galois G_P e $\phi_\sigma : C \to C$ o automorfismo correspondente a σ. Podemos assumir que $\phi_\sigma(Q) \neq Q$. Então $\phi_\sigma(Q)$ é também um ponto de Galois para C, pois a imagem de um ponto de Galois por uma transformação projetiva é também um ponto de Galois e assim $\phi_\sigma(C) = C$. Deste modo, obtemos $(d + 1)$ pontos de Galois, que posiciona em uma reta comum.

Isto contradiz a condição que $d \geq 4$. Portanto $\phi_\sigma(Q) = Q$, com isso Q deve posicionar na reta $X = 0$.

Se $d \not\equiv 1$ módulo p, então C é uma curva regular com finitos pontos de inflexão, logo pela desigualdade acima $\delta'(C) \leq 3$. Segue que $\delta'(C) = 0, 1$ ou 3. Se $d \equiv 1$ módulo p e C tem uma aplicação dual separável, então $\delta'(C) \leq 1$, logo $\delta'(C) = 0$ ou 1. ■

Exemplo 2.3.4 *Seja $C \subset \mathbb{P}^2$ uma quártica não singular sobre um corpo algebricamente fechado de característica 3. Estudaremos os seus pontos de Galois externos.*

De acordo com as hipóteses desta seção $p > 2$, $d \geq 4$ e $d \not\equiv 0$ módulo p, dada uma curva C projetivamente equivalente a curva determinada por

$$X^4 + a_4Y^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3 + a_0Z^4,$$

Após uma mudança conveniente de coordenadas, podemos re-escrever este polinômio sob a forma

$$X^4 + b_3Y^3Z + b_2Y^2Z^2 + b_1YZ^3.$$

Como C é não singular, necessariamnte b_1 ou b_3 são não nulos. Então, novamente mudando coordenadas podemos supor que a equação de C é da forma

$$X^4 + Y^3Z + aY^2Z^2 + YZ^3, \text{ com } a \in k.$$

Esta equação apresenta uma simetria nas indeterminadas Y e Z. Então podemos pensar nas duas equações afins: $f(x, y) = x^4 + y^3 + ay^2 + y$ e $\tilde{f}(x, z) = x^4 + z + az^2 + z^3$. Vamos obter os resultados para o polinômio $f(x, y)$. Resultados análogos podem ser obtidos para $\tilde{f}(x, y)$.

$$h(f(x,y)) = \begin{bmatrix} 0 & 0 & x^3 \\ 0 & 2a & 2ay+1 \\ x^3 & 2ay+1 & 0 \end{bmatrix},$$

Então $det(h(f(x, y))) = -ax^6$, que é identicamente zero quando $a = 0$. Neste caso, a aplicação dual é inseparável. No outro caso a curva C tem a aplicação dual separável. Vamos calcular os pontos de inflexões em $Z \neq 0$ neste caso. Para $x = 0$ temos $f(0, y) = y^3 + ay^2 + y$ que apresenta tres raízes distintas: $y_1 = 0$, $y_2 = \alpha$ e $y_3 = \beta$. Temos então os 4 pontos de inflexão $Q_1 = (0 : 0 : 1)$, $Q_2 = (0 : \alpha : 1)$, $Q_3 = (0 : \beta : 1)$ e $Q_4 = (0 : 1 : 0)$ sobre a reta $X = 0$, sendo Q_4 um ponto no infinito. Para calcular a ordem dessas inflexões, podemos calcular as multiplicidades de intersecção da curva com a reta tangente em cada ponto. Efetuando os cálculos, utilizando as propriedades do índice de intersecção obtemos que cada reta tangente inflexional em cada ponto desses intersecta C com multiplicidade 4. Assim a ordem de cada uma dessas inflexões é 2.

2.4 Pontos de Galois para curvas de grau p

Vamos estudar, nesta seção, os pontos de Galois de uma curva algébrica plana projetiva não singular C de grau p sobre um corpo algebricamente fechado de característica $p > 3$.

Proposição 2.4.1 *Seja C uma curva algébrica plana projetiva não singular de grau p e suponha que ela possua um ponto de Galois interno. Então o número de inflexões internas de C é $p + (p-1)e + 1$, com $0 \leq e \leq 2p-3$ (não contando com multiplicidades).*

Demonstração. De acordo com a equação *(2.1)* na Proposição *2.2.2*, considere $F = X^{p-1}Z + G(Y,Z)$ $(d = p)$, existe inflexão em C com $Z \neq 0$. Sejam $f(x,y) = F(x,y,1)$ e $g(y) = G(y,1)$. Temos que

$$h(f(x,y)) = \begin{bmatrix} (p-1)(p-2)x^{p-3} & 0 & (p-1)x^{p-2} \\ 0 & g''(y) & g'(y) \\ (p-1)x^{p-2} & g'(y) & 0 \end{bmatrix}.$$

Assim $det(h(f(x,y))) = -x^{p-3}(2(g')^2 + x^{p-1}g'')$.

Se $x = 0$, pela equação da curva, temos que $g(y) = 0$, que possui p raízes.

Se $x = 0$ e $(2(g')^2 + x^{p-1}g'') = 0$ então $g = g' = 0$ e, como a curva é regular, então não há raízes neste caso.

No caso em que $x \neq 0$ e $(2(g')^2 + x^{p-1}g'') = 0$, utilizando a equação da curva, obtemos $2(g')^2 - gg'' = 0$. Para cada raiz da equação, temos $p-1$ inflexões com $x^{p-1} + g = 0$. Seja e o número de raízes de $2(g')^2 - gg'' = 0$ e escreva $g(y) = a_p y^p + a_{p-1}y^{p-1} + \cdots + a_0$, daí temos

$$\begin{aligned} g'(y) &= pa_p y^{p-1} + (p-1)a_{p-1}y^{p-2} + \cdots + a_1 = \\ &= (p-1)a_{p-1}y^{p-2} + \cdots + a_1 \\ g''(y) &= (p-1)(p-2)a_{p-1}y^{p-3} + \cdots + 2a_2. \end{aligned}$$

Como $gr(g') \leq p-2$ e $gr(gg'') \leq 2p-3$, temos que $0 \leq e \leq 2p-3$.

Agora, no caso em que $Z = 0$, temos que $F(X,Y,Z) = G(Y,0) = 0$. Escrevendo, $G(Y,Z) = a_p Z^p + a_{p-1}Z^{p-1}Y + \cdots + a_0 Y^p$, temos que $G(Y,0) = a_0 Y^p = 0$, o que acarreta $Y = 0$. A multiplicidade de interseção entre F e Z no ponto $P = (1:0:0)$ é $I_P(X^{p-1}Z + G(Y,Z), Z) = I_P(G(Y,Z),Z) = p$. Logo a quantidade de inflexões em $Z = 0$ é igual a 1.

Finalmente, efetuando a contagem da quantidade de inflexões em C temos $\delta(C) = p + (p-1)e + 1$, onde $0 \leq e \leq 2p-3$ e obtemos o resultado que queríamos. ■

Proposição 2.4.2 *Uma curva plana algébrica projetiva não singular C de grau p sobre um corpo de característica p tem um ponto de Galois externo se, e somente se, ela é projetivamente equivalente à curva dada por*

$$X^p - XZ^{p-1} + G(Y,Z) \tag{2.3}$$

onde G é um polinômio homogêneo de grau p tal que o monômio $Y^{p-1}Z$ ocorre efetivamente.

Demonstração. Podemos supor que o ponto $P = (1:0:0)$ não esteja sobre C. Desde que $\pi_P(x,y,1) = (y,1)$ na parte afim $Z \neq 0$, onde $x = \dfrac{X}{Z}$ e $y = \dfrac{Y}{Z}$. Vamos assumir que P seja um ponto de Galois externo. Então temos a extensão de Galois $k(x,y)\,|\,k(y)$ de grau p. Seja G_p o grupo de Galois dessa extensão. Dado um automorfismo $\sigma \in G_P$, temos o automorfismo $\phi : C \to C$ tal que $\phi = (\sigma(x) : \sigma(y) : 1)$. Como antes, seja $A_\sigma = (a_{ij})$ uma matriz que representa ϕ, da seguinte forma:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} \sigma(x) \\ \sigma(y) \\ 1 \end{bmatrix}.$$

Como $\sigma(y) = y$, temos

$$\begin{aligned} a_{11}x + a_{12}y + a_{13} &= \sigma(x) \\ a_{21}x + a_{22}y + a_{23} &= \sigma(y) = y \\ a_{31}x + a_{32}y + a_{33} &= 1, \end{aligned}$$

e temos que $\alpha := (a_{21}x + a_{22}y + a_{23}) - (a_{31}x + a_{32}y + a_{33})y$ é zero sobre C. Novamente, isto acarreta que $a_{21} = a_{23} = a_{31} = a_{32} = 0$ e $a_{22} = a_{33}$. Podemos assumir $a_{22} = a_{33} = 1$. Já que A_σ^p é a matriz identidade, temos $a_{11} = 1$. Denote $a_{12} = a$ e $a_{13} = b$. Dada a transformação projetiva ψ tal que $\psi(X,Y,Z) = (X : Z : aY + bZ)$ se $a \neq 0$ ou $\psi = (X : Y : aY + bZ)$ se $b \neq 0$. Então $\psi(P) = P$ e

$$\psi\sigma\psi^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Daí temos que $\sigma(x) = x + 1$. Então

$$\sigma(x^p) = \sigma(x)^p = (x+1)^p = x^p + 1, \quad \text{e} \quad \sigma(x^p - x) = x^p - x \in k(y)$$

Logo, podemos escrever $x^p - x = g(y)$ para algum polinômio $g(y)$ de grau menor ou igual a p. Assim, C é projetivamente equivalente à curva,

$$X^p - XZ^{p-1} + G(Y, Z),$$

onde $G(Y, Z)$ é um polinômio homogêneo de grau p.

Para finalizar devemos concluir que o coeficiente de $Y^{p-1}Z$ é não nulo. Escreva $G(Y,Z) = a_pY^p + a_{p-1}Y^{p-1}Z + a_{p-2}Y^{p-2}Z^2 + \cdots + a_2Y^2Z^{p-2} + a_1YZ^{p-1} + a_0Z^p$. Calculando as derivadas parciais de F, temos

$$\begin{aligned} F_X &= -Z^{p-1}, \\ F_Y &= a_{p-1}(p-1)Y^{p-2}Z + a_{p-2}(p-2)Y^{p-3}Z^2 + \cdots + 2a_2YZ^{p-2} + a_1Z^{p-1}, \\ F_Z &= XZ^{p-2} + a_{p-1}Y^{p-1} + 2a_{p-2}Y^{p-2}Z + \cdots + a_2(p-2)Y^2Z^{p-3} + a_1(p-1)YZ^{p-2}. \end{aligned}$$

Pela suavidade de C o coeficiente de $Y^{p-1}Z$ não é zero. ■

Corolário 2.4.3 *Seja C uma curva algébrica plana projetiva não singular de grau p sobre um corpo algebricamente fechado de característica p. Se C possui um único ponto de Galois externo, então o número de inflexões em C é igual a $pe' + 1$ onde $1 \leq e' \leq p-3$ (quando não contamos multiplicidades).*

Demonstração. De acordo com a equação *(2.3)* na proposição *(2.4.2)*, considere o polinômio $F = X^p - XZ^{p-1} + G(Y, Z)$ que define C, após uma eventual mudança projetiva de coordenadas. Note que a reta $Z = 0$ intersecta C somente em um ponto Q, pois $I_Q(F, Z) = p$. Logo temos uma inflexão em Q de ordem $p-2$. Seja $f(x, y) = F(x, y, 1)$ e $g(y) = G(y, 1)$. Vamos determinar as inflexões de C com $Z \neq 0$.

$$h(f(x,y)) = \begin{bmatrix} p(p-2)x^{p-2} & 0 & px^{p-1} - 1 \\ 0 & g''(y) & g'(y) \\ px^{p-1} - 1 & g'(y) & 0 \end{bmatrix}.$$

Segue que $det(h(f(x, y))) = g''(y)$. Seja e' o grau de $det(h(f(x, y)))$. Então $0 \leq e' \leq p-3$. Se $e' = 0$ então $g''(y)$ é uma constante e portanto o coeficiente de y^{p-1} é nulo em $g(y)$, e neste caso C tem um ponto singular, o que é uma contradição. Então $1 \leq e' \leq p-3$. Para cada raiz y da equação $g''(y)$ temos

p inflexões com $x^p - x + g(y) = 0$. Logo o número de inflexões em C é $pe' + 1$, onde $1 \leq e' \leq p - 3$.

Vamos mostrar agora que $\delta'(C) = 1$. Para o ponto de Galois externo P, existem e' retas que contém P e p inflexões em C. Isto mostra que $\delta'(C) = 1$ se $e' > 1$. Se $e' = 1$ então podemos assumir $g'' = y^l$ para algum $1 \leq l \leq p - 3$. Pela suavidade de C, l deve ser $p - 3$. Daí temos que $G(\widehat{Y}, \widehat{Z}) = \widehat{Y}^p + a_1\widehat{Y}^{p-1}\widehat{Z} + a_2\widehat{Y}\widehat{Z}^{p-1} + a_3\widehat{Z}^p$, ao fatorar $G(\widehat{Y}, \widehat{Z})$ em fatores lineares e fazendo $Y = \widehat{Y} - b_1 Z$ e $Z = Y + c_1\widehat{Z}$, a equação *(2.3)* torna-se $X^p - XZ^{p-1} + Y^{p-1}Z + aYZ^{p-1}$, com $a \in k$. O ponto de Galois $P = (1 : 0 : 0)$ é a interseção das retas $Z = 0$ e $Y = 0$, sendo $Z = 0$ a reta tangente em $Q = (0 : 1 : 0)$ e a reta $Y = 0$ contém p inflexões. Portanto, $\delta'(C)$ precisa ser 1. ■

Teorema 2.4.4 *Seja $C \subset \mathbb{P}^2$ uma curva não singular de grau p sobre um corpo algebricamente fechado de característica $p > 3$. Então*

$$\delta(C) \leq 1 \quad e \quad \delta'(C) \leq 1.$$

Além disso, $\delta(C) = \delta'(C) = 1$ se, e somente se, C é projetivamente equivalente à curva dada por $X^p - XZ^{p-1} + Y^{p-1}Z$.

Demonstração. Pelo Teorema *2.2.4* temos que $\delta(C) = 0, 1$ ou 4, e $\delta(C) = 4$ se e, somente se, $d = 4$. Como o grau de C é um primo p, então $\delta(C) \leqslant 1$. Segue diretamente do Corolário *2.4.3* que $\delta'(C) \leqslant 1$.

Suponha $\delta(C) = \delta'(C) = 1$ e queremos mostar que C é projetivamente equivalente à curva definida por $X^p - XZ^{p-1} + Y^{p-1}Z$. Pela Proposição *(2.4)* e Corolário *(2.3)*, temos que, $p + (p-1)e + 1 = pe' + 1$, isto é, $p(1+e) - e = pe'$. Logo $e = 0$ e $e' = 1$ e daí segue que C tem $p + 1$ inflexões e é projetivamente equivalente à curva $X^p - XZ^{p-1} + Y^{p-1}Z + aYZ^{p-1}$. Seja $Q = (a : 1 : 0)$, então a reta tangente a C em Q é $T_Q : \{Z = 0\}$. Como C tem um ponto de Galois interno, ela é projetivamente equivalente a $Y^{p-1}Z + G(X, Z)$ (após uma possível mudança projetiva de coordenadas). Daí temos que $a = 0$ e C é projetivamente equivalente a $X^p - XZ^{p-1} + Y^{p-1}Z$. ■

2.5 Pontos de Galois em curvas quárticas em característica 3

Nesta seção, vamos estudar um caso específico em característica $p = 3$, a saber, uma quártica não singular C, dentro do caso $d \equiv 1 \bmod p$.

Proposição 2.5.1 *Uma quártica não singular $C \subset \mathbb{P}^2$ sobre um corpo algebricamente fechado de característica 3 tem um ponto de Galois interno se, e somente se, ela é projetivamente equivalente a uma das curvas*

$$\begin{array}{ll} (1) & X^3Z - XZ^3 + Y^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3 \\ (2) & X^3Y - XYZ^2 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3 + Z^4, \end{array}$$

onde os a_i $(i = 1, 2, 3)$ são constantes. Na curva (2) $a_3 \neq 0$. Além disso, a aplicação dual de C é inseparável se, e somente se, $a_2 = 0$ na curva (1).

Demonstração. A prova da primeira parte é análoga à prova da proposição *2.4.2*, onde podemos escrever $\sigma(x) = x + 1$. Temos que

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

fazendo

$$\sigma(x(x + 1)(x + 2)) = \sigma(x)\sigma(x + 1)\sigma(x + 2) = x(x + 1)(x + 2) = x^3 - x.$$

Portanto $x^3 - x \in k(y)$ e, assim podemos escrever $x^3 - x = \dfrac{g(y)}{h(y)}$, onde $g(y)$ e $h(y)$ são polinômios. Como $gr(C) = 4$, necessariamente, $gr(g) \leq 4$ e $gr(h) \leq 1$. No caso em que $gr(h) = 0$ temos que a curva é projetivamente equivalente à curva definida em (1). Se $gr(h) = 1$, podemos supor $h(y) = y$ e vamos ter que C é projetivamente equivalente à curva definida em (2).

Para provar as demais afirmações considere a curva no caso (1):

$$f_1(x, y) = x^3 - x + y^4 + a_3y^3 + a_2y^2 + a_1y.$$

Para $Z \neq 0$, temos:

$$h(f_1(x, y)) = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 2a_2 & y^3 + 2a_2y + a_1 \\ -1 & y^3 + 2a_2y + a_1 & 0 \end{bmatrix}.$$

Assim temos $det(h(f_1(x, y))) = a_2$.

No caso da curva (2) temos $f_2(x, z) = x^3 - xz + a_3z + a_2z^2 + a_1z^3 + z^4$. No caso em que $Y \neq 0$, temos:

$$h(f_2(x, z)) = \begin{bmatrix} 0 & z & -1 \\ Z & x + 2a_2 & xz + a_3 + 2a_2z + z^3 \\ -z^2 & xz + a_3 + 2a_2z + z^3 & 0 \end{bmatrix}.$$

Então, $det(h(f_2(x, z))) = z^3(a_3 + z^3)$. Concluimos que $det(h(f_1(x, y))) = 0$ se, e somente se, $a_2 = 0$ e $det(h(f_2(x, z)))$ é um polinômio não nulo. ∎

Corolário 2.5.2 *Assuma as mesmas hipóteses acima. Um ponto de Galois em uma quártica C é uma inflexão de ordem 2. Além disso, se a aplicação dual de C é separável e possui um ponto de Galois interno então $\delta(C) = 1$ e o número de inflexões em C é 1 ou 5.*

Demonstração. Seja $P = (1 : 0 : 0)$. Na curva definida pela equação (1), temos que a reta tangente a C em P é $Z = 0$ e $I_P(C, Z) = 4$. Logo P é uma inflexão de ordem 2 e Z intercepta C somente em P. Se $Z \neq 0$, considere $f_1(x, y) = x^3 - x + y^4 + a_3y^3 + a_2y^2 + a_1y$. Como a aplicação dual de C é separável, temos que $det(h(f_1(x, y))) = a_2$ é não nulo. Logo não existem inflexões em C com $Z \neq 0$. Segue que C tem somente um ponto de Galois interno e uma inflexão.

No caso da curva definida pela equação (2), temos que a reta tangente a C em P é $Y = 0$, que intercecta C somente em P, que é uma inflexão de ordem 2. No caso em que $Y \neq 0$, considere $f_2(x, z) = x^3 - xz + a_3z + a_2z^2 + a_1z^3 + z^4$. Temos que $det(h(f_2)) = z^3(a_3 + z^3)$. Vamos determinar as inflexões.

No caso em que $z = 0$ temos que $f_2(x, 0) = x^3$, isto é, $x = 0$. Considere $Q = (0 : 1 : 0)$. A reta tangente em Q é $Z = 0$ e, logo Q é uma inflexão de ordem 1 que contém o ponto P.

No caso em que $z = \sqrt[3]{-a_3}$ temos que $x^3 - (\sqrt[3]{-a_3})^2x + a_2(\sqrt[3]{-a_3})^2 - a_1a_3 = 0$ tem três raízes. Logo a curva dada por (2) tem cinco inflexões. Os três pontos dados por $z = \sqrt[3]{-a_3}$ não podem ser pontos de Galois, pois para cada um desses pontos P', não existe uma inflexão na qual a reta tangente contenha P', logo a curva dada pela equação (2) tem somente um ponto de Galois. ■

Exemplo 2.5.3 *Seja $F(X, Y, Z) = X^3Y - XYZ^2 + Y^3Z + Z^4$. Podemos verificar que a curva C definida por F tem apenas um ponto de Galois e quatro inflexões de ordem 1.*

Seja $P = (1 : 0 : 0)$. A reta tangente a C em P é $Y = 0$ e, logo $I_P(F, Y) = 4$. Assim P é uma inflexão de ordem 2. Como $f(x, z) = x^3 - xz^2 + z + z^4$, temos que $det(h(x, z)) = z^3(z^3 + 1)$. Se $z = 0$ então $f(x, 0) = x^3$ e, logo, $x = 0$. Se $z = -1$, temos que $f(x, -1) = x^3 - x$ que tem três raizes. Daí temos uma inflexão de ordem 2, que é o ponto de Galois, e quatro inflexões de ordem 1.

Teorema 2.5.4 *Seja $C \subset \mathbb{P}^2$ uma curva não singular de grau 4 sobre um corpo algebricamente fechado de característica 3. Se a aplicação dual de C é separável, então*

$$\delta(C) + \delta'(C) \leq 1.$$

Demonstração. Se a aplicação dual de C é separável e C possui um ponto de Galois interno então $\delta(C) = 1$ e o número de inflexões em C é um ou cinco. Se a aplicação dual de C é separável então tem apenas quatro inflexões e $\delta'(C)$ é no máximo 1. Portanto podemos concluir o resultado. ■

Teorema 2.5.5 *Seja $C \subset \mathbb{P}^2$ uma curva não singular de grau 4 sobre um corpo algebricamente fechado de característica 3, temos que $\delta(C) + \delta'(C) \geq 1$ se, e somente se, C é projetivamente equivalente à curva de Fermat $X^4 + Y^4 + Z^4$.*

Demonstração. Primeiramente vamos mostrar que a curva definida pelo polinômio $F_1 = X^3Z - XZ^3 + Y^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3$ com $a_2 = 0$ é projetivamente equivalente à curva de Fermat. Se $a_3 = a_1 = 0$ então podemos reduzir F_1 a $X^3Z - XZ^3 + Y^4$. Caso contrário, consideremos $a_3 \neq 0$, obtemos F_1 da seguinte forma, $X^3Z - XZ^3 + Y^4 + a_3Y^3Z$. Daí, sejam $\alpha \in k$ tal que $\alpha^9 + \alpha + a_3^3 = 0$, c a raiz cúbica de α e $\beta \in k$ tal que $\beta^3 - \beta - c^4 = 0$. A mudança de indeterminadas

$$\begin{aligned} \widehat{X} &= X - (\alpha Y + \beta Z) \\ \widehat{Y} &= Y - cZ, \\ \widehat{Z} &= Z \end{aligned}$$

transforma F_1 em $\widehat{X}^3\widehat{Z} - \widehat{X}\widehat{Z}^3 + \widehat{Y}^4$. Fazendo $\widehat{X} = u_1X_1 + v_1Z_1$ e $\widehat{Z} = u_2X_1 + v_2Z_2$, obtemos que F_1 é projetivamente equivalente a curva de Fermat.

Seja $F_2 = X^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3$, com $a_2 = 0$, podemos obter que a curva é projetivamente equivalente à curva de Fermat.
Nas curvas F_1 temos um ponto de Galois interno e em F_2 um ponto de Galois externo, logo a curva de Fermat $X^4 + Y^4 + Z^4$ tem pontos de Galois interno e externo, segue que

$$\delta(C) + \delta'(C) \geq 2.$$

Então, pelo teorema *2.5.4*, a aplicação dual é inseparável. Neste caso, temos que a curva C é projetivemente equivalente à curva de Fermat. ■

Referências Bibliográficas

[1] ARBARELLO, E.; CORNALBA, M.; GRIFFITHS, P. A.; HARRIS, J. *Geometry of Algebraic Curves*. Vol. I. Grundlehren der Mathematischen Wissenschaften, 267. New York: Springer - Verlag, 1985.

[2] BUOSI, C. C. M. *Pontos singulares e pontos de Galois de quárticas planas singulares*, Dissertação de Mestrado - PPGMAT - UFES, 2011.

[3] CHANG, H. C. *On plane algebraic curves*, Chinese J. Math. 6:185-189, 1978.

[4] ENDLER, O. *Teoria dos corpos*, Publicações matemáticas, IMPA, 2007.

[5] FULTON, W. *Algebraic Curves: An Introduction to Algebraic Geometry*, Benjamin, New York, 1969.

[6] FUKASAWA, S. *Galois points on quartic curves in characteristic 3*, Nihonkai Math. J. 17:103?110, 2006.

[7] FUKASAWA, S. *On the number of Galois points for a plane curve in positive characteristic*, Commun. Algebra 36: 29-36, 2006.

[8] FUKASAWA, S. *On the number of Galois points for a plane curve in positive characteristic, II*, 2007.

[9] FUKASAWA, S. *Galois points for a plane curve in arbitrary characteristic*, Commun. Algebra 139:211-218, 2008.

[10] HOMMA, M. *Galois points for a Hermitian curve*, Comm. Algebra 34:4503-4511, 2006.

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

[12] MIURA, K.; YOSHIHARA, H. *Field theory for function fields of plane quartic curves*, J. Algebra 226:283-294, 2000.

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

[14] PARDINI, R. *Some remarks on plane curves over fields of finite characteristic*.Compositio Math. 60 (1986) 3-17.

[15] RODRIGUES, J. H. O. *Pontos de Galois em Quárticas Lisas*, Dissertação de Mestrado - PPGMAT - UFRGS, 2009.

[16] SHAFAREVICH, I. R. *Basic Algebraic Geometry*: Varieties in Projective Space. 3.ed. Springer-Verlag. Berlin, 2013.

[17] SILVA, P. M. *Pontos de Galois Sobre Curvas Quárticas Projetivas Não Singulares*, Dissertação de Mestrado - PPGMAT - UFES, 2009.

[18] SOUZA, G. A. *O grupo de Galois do fecho normal associado a projeções centrais de quárticas projetivas planas não singulares*, Dissertação de Mestrado - PPGMAT - UFES, 2010.

[19] STOHR, K. O.;VOLOCH, J. F. *Weierstrass points and curves over finite fields*. Proc. London Math. Soc. 3(52):1-19, 1986.

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

[21] WALKER, R. J. *Algebraic curves*, Princeton University Press, Princeton, 1950.

[22] YOSHIHARA, H. *Function field theory of plane curves by dual curves*, J. Algebra 239:340-355, 2001.