Fecho Galoisiano de sub-extensões quárticas do corpo de funções racionais sobre corpos finitos

David A. Saldaña Monteza

David A. Saldaña Monteza

Fecho Galoisiano de sub-extensões quárticas do corpo de funções racionais sobre corpos finitos

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Matemática. *EXEMPLAR DE DEFESA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Março 2017

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

MC263f

Monteza, David A. Saldaña
Fecho Galoisiano de sub-extensões quárticas do corpo de funções racionais sobre corpos finitos / David A. Saldaña Monteza; orientador Herivelto Martins Borges Filho. - São Carlos - SP, 2017.
51 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2017.

1. Corpos finitos. 2. teoria de Galois. 3. corpo de funções. 4. resolvente cúbica. 5. teorema de Bézout. I. Filho, Herivelto Martins Borges, orient. II. Título.

David A. Saldaña Monteza

Galois closures of quartic sub fields of rational function fields over finite fields

Master dissertation submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP, in partial fulfillment of the requirements for the degree of the Master Program in Mathematics. *EXAMINATION BOARD PRESENTATION COPY*

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
March 2017

Dedico este trabalho:

- *a Deus, que me deu a vida e me conhece desde sempre;*
- *à minha família que é o suporte para continuar estudando cada dia;*
- *a todos os professores e amigos que apoiaram com seu conhecimentos e criticas;*
- *ao Instituto de Ciências Matemáticas e de Computação (ICMC), pelo suporte econômico neste tempo.*

AGRADECIMENTOS

Para a elaboração deste trabalho, foi de maneira muito valiosa o apoio de varias pessoas, para as quais dedico nesta página meu agradecimento

Manifesto a minha gratidão á Prof. Doutor Herivelto Martins Borges Filho, orientador desta tese, pelo seu apoio em cada parte difícil para a concretização desta tese.

Agradeço a meu amigos e professores, por seu apoio em cada etapa do trabalho desde o principio, e ate nas ultimas horas do depósito.

Agradeço a minha família por suas orações e o amino durante todo este tempo fora do Perú.

“No hay mayor fracaso que tener éxito en las cosas que no importan en la eternidad ”

(Francis Chan)

RESUMO

DAVID A. SALDAÑA MONTEZA. **Fecho Galoisiano de sub-extensões quárticas do corpo de funções racionais sobre corpos finitos**. 2017. 51 f. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação (ICMC/USP), São Carlos – SP.

Seja p um primo, considere $q = p^e$ com $e \geq 1$ inteiro. Dado o polinômio $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{F}_q[x]$, consideremos o polinômio $F(T) = T^4 + aT^3 + bT^2 + cT + d - y \in \mathbb{F}_q(y)[T]$, com $y = f(x)$ sobre $\mathbb{F}_q(y)$. O objetivo desse trabalho é determinar o número de polinômios $f(x)$ que tem seu grupo de galois associado G_F isomorfo a cada subgrupo transitivo (prefixado) de S_4. O trabalho foi baseado no artigo: **Galois closures of quartic sub-fields of rational function fields**, usando equações auxiliares associadas ao polinômio minimal $F(T)$ de graus 3 e 2 (DUMMIT, 1994); bem como uma caraterização das curvas projetivas planas de grau 2 não singulares. Se $car(k) \neq 2$, associamos a $F(T)$ sua cúbica resolvente $R_F(T)$ e seu discriminante Δ_F. Em seguida obtemos condições para $G_F \cong C_4$ (vide Teorema 2.9), que é ocaso fundamental para determinação dos demais casos. Se $\text{car}(k) = 2$, procuramos determinar condições para $G_{R_F} \cong A_3$, associando ao polinômio $R_F(T)$ sua quadrática resolvente $P(T)$ (vide a Proposição 2.13). Apos ter homogeneizado $P(T)$, usamos uma das consequências do teorema de Bézout, a saber, uma curva algébrica projetiva plana C de grau 2 é irredutível se, e somente se, C não tem pontos singulares. Nesta dissertação obtemos resultados semelhantes com uma abordagem relativamente diferente daquela usada pelo autor R. Valentini.

Palavras-chave: Corpos finitos, teoria de Galois, corpo de funções, resolvente cúbica, teorema de Bézout.

ABSTRACT

DAVID A. SALDAÑA MONTEZA. **Fecho Galoisiano de sub-extensões quárticas do corpo de funções racionais sobre corpos finitos**. 2017. 51 f. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação (ICMC/USP), São Carlos – SP.

Let be p a prime, $q = p^e$ whit $e \geq 1$ integer. Let a polynomial $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{F}_q[x]$, considering the polynomial $F(T) = T^4 + aT^3 + bT^2 + cT + d$, with $y = f(x)$ over $\mathbb{F}_q(y)[T]$. The purpose of the current research is to determine the numbers of polynomials $f(x)$ which have its associated Galois group G_F, this G_F is isomorphic for each transitive subgroup (prefixed) of A_4. This project is based on the article: **Galois closures of quartic sub-fields of rational function fields**, using auxiliary equations associated to the minimal polynomial $F(T)$ of degrees 3 and 2 (DUMMIT, 1994); besides a characterization of non-singular projective plane curves of degree 2 was used. If $car(k) \neq 2$, associated to $F(T)$ the resolvent cubic $R_F(T)$ and its discriminant Δ_F. then conditions for G_F are obtained as $G_F \cong C_4$ which is the fundamental case for determining the other cases (Theorem 2.9). If $car(k) = 2$, to find conditions for $G_{R_F} \cong A_3$, associated to the polynomial $R_F(T)$ its resolvent quadratic $p(T)$ (Proposition 2.13). Homogenizing $p(T)$, one of the consequences of the Bezout theorem was applied. It is, a projective plane curve C, which grade 2, is irreducible if and only if C is smooth. In the current dissertation, similar results were obtained using a different approach developed by the author R. Valentini.

Key-words: Finite fields, Galois theory, cubic resolvent, function fields, Bézout theorem.

SUMÁRIO

INTRODUÇÃO

Considere k um corpo, com $\text{car}(k) \neq 2$. Se x é um elemento transcendente sobre k, dado $t = \frac{x^4+1}{x^2}$ temos que $k(x)/\ k(t)$ é Galosiana com grupo de automorfismo isomorfo ao klein-4. Este último tem um gerador o qual não é da forma $t = f(x)$ com $f(x)$ um polinômio de grau 4, de forma análoga podemos associar a $G_F \cong A_4$ o gerador $t = x^4 + 1/x$. Mais geralmente, se x é um elemento transcendente sobre k, para $t = f(x)/g(x)$ tais que $(f,g) = 1$, $f(x), g(x) \in k[x]$, $g(x) \neq 0, 1$ e grau$(f,g) \leq 4$. O objetivo desse trabalho é determinamos o número de polinômios $f(x)$ que tem seu grupo de Galois associado G_F isomorfo a um subgrupo transitivo (pre-fixado) de S_4. O trabalho foi baseado no artigo: **Galois closures of quartic sub-fields of rational function fields**. Dado $\mathbb{F}_q(x)$ o corpo de funções algébricas (corpo de funções racionais) e $y = f(x)$, temos que

$$F(T) = T^4 + aT^3 + bT^2 + cT + d - y \in \mathbb{F}_q(y)[T].$$

é o polinômio minimal (irredutível) da extensão $\mathbb{F}_q(x)/\mathbb{F}_q(y)$. Se $F(T)$ é separável, então o grupo de Galois G_F do fecho galoisiano é um subgrupo transitivo do S_4(vide 1.53). Para determinar a forma de cada uma das classes de polinômios $f(x)$ com seu grupo de Galois G_F, temos que existem equações de grau 2 e 3. Estes últimos foram usados primeiramente por Galois (1811-1832) e I. Kaplansky (KAPLANSKY, 1972) . Galois definiu de maneira mais geral a resolvente associada a um polinômio g de grau arbitrário. Os grupos estabilizadores para as resolventes de grau 2 e 3 são A_3 e V (Klein-4) respetivamente. De maneira mais explicita, seja $f(x) \in k[x]$ um polinômio mônico de grau 4, com $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \overline{k}$ suas raízes. Dados $\sigma_1 = id$, $\sigma_2 = (23)$ e $\sigma_3 = (24)$, então temos a cúbica resolvente

$$R_f = (x - \sigma_1(\theta))(x - \sigma_2(\theta))(x - \sigma_3(\theta)),$$

com as duas escolhas possíveis $\theta = \alpha_1\alpha_2 + \alpha_3\alpha_4$ ou $\theta = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, vide Proposição 2.3 e Observação 2.4. Analogamente dada $g(x) \in k[x]$ um polinômio mônico de grau 3, com $\beta_1, \beta_2, \beta_3 \in \overline{k}$ suas raízes. Considerando $\beta = \theta_1^2\theta_2 + \theta_2^2\theta_3 + \theta_3^2\theta_1$ e a tranposição $\sigma = (12)$, então temos a quadrática resolvente

$$p(x) = (x - \beta)(x - \sigma(\beta)), \text{ vide Proposição 2.13}$$

Otra ferramenta que usamos nesta dissertação é uma caraterização das curvas algébricas projetivas planas de grau 2. Pelo Teorema de Bezout (1730-1783), sabemos que uma curva C projetiva plana de grau 2 é irredutível em $\overline{\mathbb{F}_q}[X,Y,Z]$ se, e somente se, não tem pontos singulares. Dada $R_F(T)$ a

cúbica resolvente de $F(T)$, associamos a ela sua quadrática resolvente $p(T)$. Seja $p(X,Y,Z)$ a homogenização desta última em $\mathbb{F}_q[X,Y,Z]$, se $p(X,Y,Z)$ é irredutível em $\overline{\mathbb{F}_q}[X,Y,Z]$, pelo lema de Gauss temos que $P(T)$ é irredutível em $\mathbb{F}_q(y)[T]$. Em particular, para $a \neq 0$, provamos que $P(T)$ é redutível se, e somente se, $b^2 = ac$ e $q \equiv 1 mod 3$. Nesta dissertação obtemos resultados semelhantes com uma abordagem relativamente diferente daquela usada pelo autor R. Valentini.

CAPÍTULO

1

PRELIMINARES

O problema de nosso trabalho tem três assuntos que devemos tratar neste capitulo: Corpos finitos, polinômios sobre corpos e grupos de Galois. Portanto pretendemos aqui introduzir de forma sucinta esses conceitos que serão frequentemente usados neste trabalho. Para acompanhar este capítulo, o leitor deve possuir conhecimentos prévios como teoria de anéis, teoria de grupos e espaços vetoriais que podem ser encontrados em (GARCIA; LEQUAIN, 2001)

1.1 Corpos Finitos

Um corpo é, grosso modo, um conjunto no qual podemos somar, subtrair, multiplicar e dividir por elementos não nulos, no qual valem todas as propriedades usuais de tais operações, incluindo a comutativa da adiçãoo e da multiplicação. As funções que preservam essas operações são chamadas de homomorfismo de corpos. A seguir apresentaremos essas definições.

Definição 1.1. *Um* corpo F *é um conjunto* F *não vazio munido de duas operações, adição* $(+)$ *e multiplicação* $(\cdot)$*, tal que* $(F,+)$ *é um grupo abeliano com elemento neutro aditiva* 0 *e* $(F^* = F - \{0\},\cdot)$ *é um grupo abeliano com elemento neutro multiplicativa* 1*. Uma função* $\sigma : F \to E$*, onde* E *e* F *são corpos, é chamado de homomorfismo de corpos se* $\sigma(u+v) = \sigma(u) + \sigma(v)$ *e* $\sigma(uv) = \sigma(u)\sigma(v)$*, para todo* $u, v \in F$*.*

Da definição, podemos observar o seguinte: (1) Todo corpo é um domínio de integridade[1]. (2) Os únicos ideias de um corpo são os triviais. (3) Todo homomorfismo de corpos é um homomorfismo de anéis. Desde que o kernel da σ é um ideal de F segue-se que todo homomorfismo de corpos é ou o homomorfismo nulo, ou é injetor. Dentre os corpos que usaremos no trabalho temos os seguintes:

1. Para p primo, $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$, possui estrutura de corpo.

[1] Anel comutativo com unidade 1 e sem divisores de zero.

2. Se D um domínio de integridade então o conjunto

$$F = \left\{ \frac{a}{b} = ab^{-1} \,:\, a,b \in D,\ b \neq 0 \right\}$$

possui estrutura de corpo (vide Dummit (1994, Pag. 262)), chamado *corpo de frações* de D.

Desde que todo corpo é um anel, então podemos discutir a característica de um corpo, em particular um corpo finito[2], como por exemplo, o corpo $\mathbb{Z}_p$ tem característica p, com p primo. De forma geral, temos:

Proposição 1.2. *Se F é um corpo finito, então existe um primo p tal que $(F) = p$.*

Podemos observar que $(F) \neq 0$. De fato, como F é finito, existem m e n inteiros positivos, com $m > n$ tais que $m.1 = n.1$. Assim, $(m-n).1 = 0$, isto é $(F) \neq 0$. Agora, seja $(F) = p > 0$ e suponha que $p = a.b$ seja composto. Daí, $1 < a,b < p$ e então $0 = p.1 = (ab).1 = (a.1)(b.1)$. Desde que F é um domínio de integridade, segue-se que $a.1 = 0$ ou $b.1 = 0$ o que contraria a minimalidade de p. Portanto, p é primo.

Como consequência temos, que o homomorfismo de corpos $\varphi : \mathbb{Z}_p \to F$, $a \mapsto a.1$ é injetora e portanto $\mathbb{Z}_p \subset F$ isomorficamente. Logo, a multiplicação $(a,b) \mapsto ab$, para $a \in \mathbb{Z}_p$ e $b \in F$ torna F um espaço vetorial sobre $\mathbb{Z}_p$ de dimensão finita. A seguir, usando o fato acima, provaremos que a ordem de um corpo finito de característica p, é uma potência de p.

Proposição 1.3. *Seja F um corpo finito com $(F) = p$. Então, existe um inteiro positivo e tal que $|F| = p^e$*

Suponha que $\dim_{\mathbb{Z}_p} F = e$. Seja $\{u_1, u_2, \ldots, u_e\}$ uma base de F. Dado $u \in F$, existem únicos $\alpha_1, \ldots, \alpha_e \in \mathbb{Z}_p$ tais que $u = \alpha_1 u_1 + \ldots + \alpha_e u_e$. Para cada α_i, existem p possibilidades. Portanto, existem p^e possibilidade para u.

Observação 1.4. Daqui em diante, um corpo finito de ordem q, será denotado por $\mathbb{F}_q$, onde $q = p^e$, para algum primo p (característica de $\mathbb{F}_q$), e algum inteiro positivo e.

Para k um corpo qualquer e x transcendente sobre k, podemos considerar o grupo de automorfismos $Aut(k(x)/k)$. Descrevemos tal grupo de automorfismos quando $k = \mathbb{F}_q$ com $q = p^e$ elementos, $e \geq 1$ inteiro e p um número primo dado. No Capítulo 2, faremos uma comparação de certos subgrupos de $Aut(\mathbb{F}_q(x)/\mathbb{F}_q)$ com o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$, onde $f(x)$ é um polinômio mônico de grau 4.

Definição 1.5. *Denotamos por $GL(2,\mathbb{F}_q)$ o grupo de matrizes invertíveis de ordem 2×2 sobre $\mathbb{F}_q$. $GL(2,\mathbb{F}_q)$ é chamado o Grupo Linear.*

[2] Chamado também corpo de Galois em homenagem a Évariste Galois, que foi um dos primeiros matemáticos a investiga-los.

Proposição 1.6. *O Grupo linear $GL(2,\mathbb{F}_q)$ tem ordem $q(q-1)^2(q+1)$.*

Demonstração. Ver Rotman (1965, Pag. 155) □

Proposição 1.7. *A aplicação $det : GL(2,\mathbb{F}_q) \to \mathbb{F}_q^*$, é um homomorfismo sobrejetivo. O núcleo desta aplicação é o conjunto das matrizes com determinante 1, denotamos este grupo por $SL(2,\mathbb{F}_q)$ o Grupo Especial linear.*

Demonstração. Ver Rotman (1965, Pag. 158) □

Observe que, pelo Teorema Fundamental do Isomorfismo de Grupos,

$$\frac{GL(2,\mathbb{F}_q)}{SL(2,\mathbb{F}_q)} \cong \mathbb{F}_q^*.$$

Assim, $| SL(2,\mathbb{F}_q) | = \dfrac{| (GL(2,\mathbb{F}_q) |}{q-1} = (q-1)q(q+1)$.

Exemplo 1.8. O espaço projetivo $\mathbb{P}^1_k = \{(a:0)/a \in k\} \cup \{(0:1)\}$. Em particular, podemos definir a ação:

$$\begin{array}{ccccc} GL(n,k) & \times & \mathbb{P}^1_k & \to & \mathbb{P}^1_k \\ A & \times & \begin{pmatrix} a \\ b \end{pmatrix} & & A \cdot \begin{pmatrix} a \\ b \end{pmatrix} \end{array}$$

O centro desta acção é o grupo das matrizes escalares λId, com $\lambda \in k^\times$. Denotado por $Z(GL(2,\mathbb{F}_q))$.

Definição 1.9. *Dado $Z(GL(2,\mathbb{F}_q))$ o grupo das matrizes escalares, definimos o Grupo Projetivo linear e Grupo Especial Projetivo Linear, por:*

$$PGL(2,\mathbb{F}_q) = \frac{GL(2,\mathbb{F}_q)}{Z(GL(2,\mathbb{F}_q))} \text{ e } PSL(2,\mathbb{F}_q) = \frac{SL(2,\mathbb{F}_q)}{Z(GL(2,\mathbb{F}_q)) \cap SL(2,\mathbb{F}_q)}.$$

Temos que

$$| PGL(2,\mathbb{F}_q) | = \frac{q(q-1)^2(q+1)}{q-1} = (q-1)q(q+1) = | SL(2,\mathbb{F}_q) |$$

$$| PSL(2,\mathbb{F}_q) | = \frac{SL(2,\mathbb{F}_q)}{gcd(2,q-1)} = \frac{(q-1)q(q+1)}{gcd(2,q-1)}.$$

Exemplo 1.10. Claramente, para $q=2$, $PGL(2,\mathbb{F}_2) \cong S_3$. Pelo Exemplo 1.8 temos que $PGL(2,\mathbb{F}_2) \subseteq S_3$ e $| PGL(2,\mathbb{F}_2) | = 6$.

Exemplo 1.11. Para $q=3$, $PGL(2,\mathbb{F}_3) \cong S_4$, pois $PGL(2,\mathbb{F}_3) \subseteq S_4$ e $| PGL(2,\mathbb{F}_3) | = 24$.

Exemplo 1.12. Se $q=4$, $PGL(2,\mathbb{F}_4) \cong A_5$. Temos que $PGL(2,\mathbb{F}_4) \subseteq S_5$ e $| PGL(2,\mathbb{F}_4) | = 60$. Além disso, A_5 é o único subgrupo de índice 2 em S_5.

Exemplo 1.13. Se $q = 5$, $PGL(2,\mathbb{F}_5) \cong S_5$. Temos que $PGL(2,\mathbb{F}_5) \subseteq S_6$ e $\mid PGL(2,\mathbb{F}_5) \mid = 120$. Além disso, $PSL(2,\mathbb{F}_5) \subseteq S_6$ tem ordem 60. Observe que $PGL(2,\mathbb{F}_4) \cong A_5$ tem ordem 60, logo $PSL(2,\mathbb{F}_5) \cong PGL(2,\mathbb{F}_4) \cong A_5$. logo $PGL(2,\mathbb{F}_5)$ é um subgrupo de ordem 120, que tem A_5 um subgrupo de índice 2. Logo $PGL(2,\mathbb{F}_5) \cong S_5$.

O seguinte lema descreve a os corpos intermediários para extensões com grau de transcendência 1.

Lema 1.14. *Consideremos $k(t)/k$ o corpo de funções de racionais, se $t = P(x)/Q(x)$ com $(P,Q) = 1$ e $Q \neq 0$, para $Q(X)t - P(X)$ polinômio minimal de x sobre $k(t)$, temos que*

$$[k(x) : k(t)] = max\{deg(P), deg(Q)\}.$$

Demonstração. Dummit (1994, Pag. 530-531) □

Proposição 1.15. *O grupo $PGL(2,\mathbb{F}_q) \cong Aut(\mathbb{F}_q(x)/\mathbb{F}_q)$.*

Demonstração. Pelo Lema 1.14, temos que $k(r) = k(t)$ se, e somente se, $r = \frac{at+b}{ct+d}$ com $ad - bc \neq 0$. O mapa $\sigma_A : k(t) \to k(t)$, dada por $\sigma_A(t) = \frac{at+b}{ct+d}$, é sobrejetivo e $\sigma_A \mid_k = id$, então $\sigma_A \in Aut(k(t)/k)$. O mapa

$$\begin{array}{ccc} GL(2,\mathbb{F}_q) & \to & Aut(k(t)/k) \\ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} & & \sigma_A \end{array}$$

é sobrejetivo, e seu núcleo são as matrizes escalares. Logo

$$PGL(2,\mathbb{F}_q) \cong Aut(\mathbb{F}_q(x)/\mathbb{F}_q).$$

□

1.2 Anel de polinômios

O objetivo do trabalho é a contagem dos polinômios de grau 4, sobre corpos finitos. Então precisaremos saber um pouco da teoria do anel de polinômios.

Definição 1.16. *Seja A um anel. Um polinômio $f(x)$ de uma variável sobre A é uma expressão do tipo*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \quad n \geq 0$$

onde $a_i \in A$. Se $a_n \neq 0$, então o inteiro n se chama o grau do f, e é denotado por (f) e a_n se chama coeficiente líder. Se o coeficiente líder é igual a 1, o polinômio é dito mônico.

Diremos que o polinômio f é linear se $(f) = 1$, quadrática se $(f) = 2$, cúbica se $(f) = 3$ e quartica se $(f) = 4$. O conjunto de todos os polinômios de uma variável sobre A com as operações usuais de adição e multiplicação de polinômios possui estrutura de anel, será denotado por $A[x]$.

Definição 1.17. *O anel $A[x]$ é chamado de anel de polinômios de uma variável sobre A. Por indução, podemos definir o* anel de polinômios em k variáveis sobre A *do modo seguinte:* $A[x_1,\ldots,x_k] = (A[x_1,\ldots,x_{k-1}])[x_k]$.

A seguir apresentaremos três tipos de polinômios que serão usados no trabalho.

Definição 1.18.

1. *Sejam D um domínio de integridade e $f(x) \in D[x]$ com $(f) \geq 1$. Dizemos que $f(x)$ é um polinômio irredutível sobre D se toda vez que $f(x) = g(x)h(x)$, $g(x), h(x) \in D[x]$ então temos $g(x) = a \in D$ ou $h(x) = b \in D$. Se $f(x)$ for não irredutível sobre D dizemos que $f(x)$ é redutível sobre D. De forma análoga, podemos definir um polinômio $f(x_1,\ldots,x_k)$ em k variáveis irredutível sobre D.*

2. *Sejam D um domínio de fatoração única*[3]*. Dizemos que $f(x) \in D[x]$ é um polinômio* primitivo *se $c(f(x)) = M.D.C.\{a_i\} = 1$.*

3. *Um polinômio $f(x_1,\ldots,x_n) \in A[(x_1,\ldots,x_n]$ é dito homogêneo de grau $d \in \mathbb{N}$ se para todo $\alpha \in A$, $f(\alpha x_1,\cdots,\alpha x_n) = \alpha^d f(x_1,\cdots,x_n)$.*

Observação 1.19. Seja k um corpo. Se $p(x) \in k[x]$ é um polinômio irredutível, segue-se que o ideal $(p(x))$ gerado por $p(x)$ é máximal, e portanto pode-se provar que $k[x]/(p(x))$ é um corpo.

A seguir, provaremos o primeiro criterio de irredutibilidade

Proposição 1.20 (Lema de Gauss)**.** *Seja D um domínio de fatoração única com corpo de frações F. Dado $f(x) \in D[x]$, se $f(x)$ é irredutível sobre $D[x]$ se, e somente se, $f(x)$ é primitiva sobre $D[x]$ e irredutível sobre $F[x]$.*

A volta é imediata. Suponhamos que $f(x)$ é irredutível sobre $D[x]$. É claro que $f(x)$ é primitivo em $D[x]$. Agora, suponha por absurdo que $f(x)$ é redutível em $F[x]$, ou seja, $f(x) = h(x)g(x)$, com ambos $h(x), g(x) \in F[x]$ de grau maior que 1. Desde que F é o corpo de frações, então podemos, escrever $h(x) = (a/b)h_1(x)$ e $g(x) = (a'/b')g_1(x)$ com $a,b,a',b' \in D$, $b \neq 0$, $b' \neq 0$ e $h_1(x), g_1(x) \in D[x]$ polinômios primitivos de grau maior que 1. Portanto temos $f(x) = (aa'/bb')h_1(x)g_1(x)$, ou equivalentemente $bb'f(x) = aa'h_1(x)g_1(x)$. Desde que $f(x)$, $h_1(x)$ e $g_1(x)$ são primitivos, temos que $bb' = aa'$. Logo $f(x) = h_1(x)g_1(x)$ ou seja $f(x)$ é redutível em $D[x]$; absurdo.

Na próxima seção trataremos sobre tipos extensões de corpos e para isso precisaremos da seguinte definição

[3] Um domínio de fatoração única é um domínio de integridade D onde todo elemento não-nulo e não-invertível de D se escreve de "maneira única" como produto de elementos irredutíveis de D.

Definição 1.21. *Sejam A uma anel, $f(x) \in A[x]$ não constante, $\alpha \in A$, e um inteiro $s \geq 1$. Dizemos que α é uma raiz de $f(x)$ se $(x-\alpha)$ divide $f(x)$, ou seja $f(\alpha) = 0$. Dizemos que α é uma raiz de multiciplidade s se $(x-\alpha)^s$ divide $f(x)$ mas $(x-\alpha)^{s+1}$ não divide $f(x)$. O corpo k diz-se algebricamente fechado, se todo polinômio $f(x)$ possui uma raiz em k*

Para enunciar o segundo criterio de irredutibilidade, usaremos a seguir fatos de curvas algébricas. O conjunto

$$\mathbb{P}^n(k) = \frac{k^{n+1-\{0\}}}{\sim}$$

onde $a \sim b$ se e somente se existe $\lambda \in k^*$ tal que $a = \lambda b$ para todo $a, b \in k^{n+1} - 0$ é chamado o espaço projetivo $n-$dimensional sobre k, onde $k^n = \{(a_1, \cdots, a_n) : a_1, \cdots, a_n \in k\}$.

Definição 1.22. *Seja $P(X,Y,Z) \in k[X,Y,Z]$ um polinômio homogêneo de grau d. A curva projetiva C definida por $P(X,Y,Z)$ é o conjunto*

$$C = \{[X,Y,Z] \in \mathbb{P}^2(k) / P(X,Y,Z) = 0\}$$

A curva C é chamada de irredutível se o polinômio $P(X,Y,Z)$ é irredutível.

Definição 1.23. *Seja C uma curva projetiva definida por $P \in k[X,Y,Z]$. As derivadas parciais são dadas por*

$$P_X(X,Y,Z) = \frac{\partial P}{\partial X},\ P_Y(X,Y,Z) = \frac{\partial P}{\partial Y},\ P_Z(X,Y,Z) = \frac{\partial P}{\partial Z}$$

(isto é definimos $P_X(X^n) = nX^{n-1}$ para $n \geq 1$ e estendê-lo linearmente a $(k[Y,Z])[X] = k[X,Y,Z]$). Um ponto $[a,b,c] \in C$ é chamado singular se

$$P(a,b,c) = P_X(a,b,c) = P_Y(a,b,c) = P_Z(a,b,c).$$

Se k um corpo algebricamente fechado e sejam C e D curvas projetivas definidos pelos polinômios homogêneos $P(X,Y,Z)$ e $Q(X,Y,Z)$ respetivamente

Definição 1.24. *A multiplicidade de um ponto $q \in \mathbb{P}^2(k)$, denotado por $I_P(C,D)$ é definido por:*

$$I_P(C,D) = \begin{cases} \infty, & q \text{ pertence a uma componente de } C \text{ e } D \\ \in \mathbb{Z} > 0, & q \in C \cap D, \text{ no esta numa componente comum.} \\ 0, & q \notin C \cap D. \end{cases} \quad (1.1)$$

Teorema 1.25 (Teorema de Bézout)**.** *Sejam C e D curvas projetivas definidas pelos polinômios homogêneos $P(X,Y,Z)$ e $Q(X,Y,Z)$ respetivamente, sem componentes em comum. Sejam m,n os graus de P e Q respetivamente. Então*

$$\sum_{q \in C \cap D} I_q(C,D) = mn$$

Demonstração. vide (VAINSENCHER, 1979) □

Proposição 1.26. *Qualquer curva projetiva não singular em $\mathbb{P}^2(k)$ é irredutível.*

Demonstração. Suponha que C não é irredutível, isto é existem $R,S \in k[X,Y,Z]$ tal que $\partial R \leq 1$ e $\partial S \leq 1$ e C é definido por $P = RS$. Pelo teorema de Bézout existe um zero comum $q = [a,b,c]$ de R e S satisfazendo

$$P(q) = P_X(q) = P_Y(q) = P_Z(q).$$

Logo temos que C é não singular.

□

A seguente proposição é usada para determinar que dado um polinômio $p(X) \in \mathbb{F}_q(y)[X]$, é irredutível, se o polinômio homogêneo em $\overline{\mathbb{F}_q}[X,Y,Z]$ é não singular (ver equação (2.8)).

Proposição 1.27. *Para uma curva C projetiva plana de grau 2 sobre um corpo k algebricamente fechado. C é redutível em $k[X,Y,Z]$ se, e somente se, a curva C tem ponto singular, isto é, existe $q \in C$ tal que $C_X(q) = C_Y(q) = C_Z(q) = 0$ (derivadas parciais).*

Demonstração. Suponha que C é singular em q. Se C é definida pelo polinômio P, então $m_q(P) \geq 2$. Dado r outro ponto em C tal que $r \neq q$ e L a reta que une os dois pontos, temos pelo Teorema de Bezout, que q e p são os dois pontos de intercessão de L e C. Suponha que L não é uma componente de C e L é definida pelo polinômio g, temos que:

$$\begin{aligned} 2 &= deg(L)\ .\ deg(C) \\ &= deg(g)\ .\ deg(P) \\ &= I_r(L,C) + I_q(L,C) \\ &\geq m_r(L)m_r(C) + m_q(L)m_q(C) \\ &\geq 2+1 \\ &= 3 \end{aligned}$$

que é absurdo, logo L é uma componente de C. Então C é redutível. □

1.3 Extensão de Corpos

Apresentamos nesta seção definições e fatos na teoria geral de extensão de corpos relevantes para nosso estudo.

Definição 1.28. *Um corpo F é chamado uma extensão de um corpo k, se k é $k \subset F$ isomorficamente. O corpo F pode-se ver como um espaço vetorial sobre k, se $\langle \alpha_1, \alpha_2, \cdots \rangle$ é uma base para F sobre k, todo elemento pode-se escrever como $k_1\alpha_1 + k_2\alpha_2 + \cdots$, escrevemos $[F:k]$ a dimensão do espaço vetorial sobre k, se $[F:k]$ é finito dizemos que F/k é uma extensão finita.*

Definição 1.29. *Um elemento α de uma extensão F sobre um corpo k é dito algébrico sobre k se $f(\alpha) = 0$ para algum polinômio não nulo $f(x)$ de $k[x]$. Se α não for algébrico, dizemos que α é transcendente sobre k.*

Dado f um polinômio mônico de grau 4. A seguinte definição é uma propriedade que é herdada aos polinômios R_f (cúbica resolvente, veja 2.3), e a quadrática resolvente de R_f (veja 2.13).

Definição 1.30. *Seja $f(x) \in k[x]$ um polinômio não constante dizemos que f é **polinômio separável** se não tem raízes múltiplas, ie f tem raízes distintas em $\overline{k}$.*
*Seja F/k uma extensão algébrica um elemento $\alpha \in F$ é dito **elemento separável** sobre k se $irr(\alpha, k)$ é un polinômio separável.*
*Uma extensão algébrica F/k é dita **extensão separável** se todo $a \in F$ é separável sobre k.*

A Proposição a seguir é usada como critério para determinar si um polinômio f dado é separável. Isto é, se f é irredutível e $f' \neq 0$, então f é separável.

Proposição 1.31. *O polinômio $f(x) \in k[x]$ tem raiz múltipla α se, e somente se, α é raiz de $f'(x)$ (sua derivada).*

Demonstração. Ver Dummit (1994, Pag. 547) □

Definição 1.32. *Se F/k é uma extensão, e suponha $\alpha \in F$ algébrico sobre k, o polinômio minimal de α sobre k, denotado por $m_{\alpha,k}(x)$ é o único polinômio mônico sobre k de menor grau onde $m_{\alpha,k}(\alpha) = 0$.*

A proposição 1.33 a seguir pode-se ver como o menor grau possível para uma extensão algébrica e simple dada sobre k.

Proposição 1.33. *Seja $k(\alpha)/k$ é uma extensão simple e algébrica, então $[k(\alpha) : k] = deg(m_{\alpha,k}(x))$.*

Demonstração. Ver Dummit (1994, Pag. 521). □

Definição 1.34. *Seja F/k uma extensão algébrica dizemos que F/k é uma **extensão normal** se todo polinômio irredutível $f(x) \in k[x]$ que tem uma raiz em F tem todas as raízes em F.*

Definição 1.35. *O mapa $\sigma : E_1 \to E_2$ onde E_1 e E_2 são corpos e*

1. $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$
2. $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$

É chamado um isomorfismo. Observe que $\sigma(0) = 0$ e $\sigma(1) = 1$.

Definição 1.36. *Ao corpo onde estão todas as raízes de um polinômio $f(x) \in k[x]$ é chamado de corpo de fatoração.*

Proposição 1.37. *Seja k um corpo e $f(x) \in k[x]$, então sempre existe um corpo de fatoração para $f(x)$ sobre k.*

Demonstração. Ver Dummit (1994, Pag. 536) □

Teorema 1.38. *Se $f(x) \in k[x]$ tem n raízes distintas no seu corpo de descomposição F, então G_f é isomorfo a um subgrupo do grupo Simétrico S_n e sua ordem é um divisor de $n!$*

Demonstração. Se $X = \{\alpha_1, \cdots, \alpha_n\}$ o conjunto de todas raízes de $f(x)$ em F. Pelo Lema 1.39, se $\sigma \in G_f = Gal(F/k)$, então $\sigma(x) = x$. A aplicação

$$\begin{array}{ccc} G_f & \to & S_X = S_n \\ \sigma & \to & \sigma/X \end{array}$$

é um homomorfismo, a qual é injetora. Por tanto $G_f \leq S_n$. □

Lema 1.39. *Seja $f(x) \in k[x]$ e seja F/k um corpo de estensão de k. Se $\sigma : F \to F$ é um automorfismo fixando k ponto a ponto, (ou seja $\sigma(\alpha) = \alpha, \forall \alpha \in k$) e se $\alpha \in F$ é uma raiz de $f(x)$ então $\sigma(\alpha)$ é tambem uma raiz de $f(x)$.*

Demonstração. Seja $f(x) = c_0 + c_1 x + \cdots c_n x^n$. Desde que α é raiz de $f(x)$, temos

$$c_0 + c_1\alpha + \cdots c_n\alpha^n = 0.$$

Aplicando $\sigma \in Aut_k F$, temos

$$\begin{array}{rcl} \sigma(c_0) + \sigma(c_1)\sigma(\alpha) + \cdots \sigma(c_n)\sigma(\alpha)^n & = & 0 \\ c_0 + c_1\sigma(\alpha) + \cdots c_n\sigma(\alpha)^n & = & 0 \end{array}$$

Portanto, $\sigma(\alpha)$ é raiz de $f(x)$. □

Por exemplo, o grupo de Galois de um polinômio quártico f é un subgrupo de S_4 e além disso $| G_f |$ divide a $4! = 24$.

Exemplo 1.40. O corpo de descomposição de $x^2 + 1 \in \mathbb{R}[x]$ é de fato $\mathbb{C}$. Pelo teorema anterior $| G_f | \leq 2$. desde que $Aut_{\mathbb{R}}\mathbb{C}$ contem

$$\sigma(a + bi) = a - bi$$

então $| G_f | = 2$. Neste caso, $G_f = \{Id, \sigma\}$.

Teorema 1.41. *Se $f(x) \in k[x]$ é um polinômio separável e F é seu corpo de descomposição, então $| G_f | = [F : k]$*

Demonstração. Pelo Teorema 1.42 com $k = k'$, $F = F'$ e $\sigma : k \to k$ segue-se que existem $[F : k]$ automorfismo de F que fixam k. □

Teorema 1.42. *Dado $\sigma : k \to k'$ um isomorfismo e os polinômios $f(x) \in k[x]$ e $f'(x) \in k'[x]$ com $f'(x) = \sigma(f(x))$, se E é o corpo de fatoração de $f(x)$ e E' é o corpo de fatoração de $f'(x)$ então σ pode-se estender a um isomorfismo $\beta : E \to E'$.*

Demonstração. Ver Dummit (1994, Pag. 541) □

Corolário 1.43. *Dado o polinômio $f(x) \in k[x]$, então temos que dois corpos de fatoração para $f(x)$ são isomorfos.*

Lema 1.44. *Dado o polinômio $f(x) \in k[x]$ irredutível, para α, β raízes de $f(x)$ num corpo de fatoração de $f(x)$ sobre k, temos que existe um isomorfismo $\alpha^* : k(\alpha) \to k(\beta)$*

Demonstração. Dado que $k(\alpha)$ têm como base a $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$, dado a_0, a_1, $a_2 \cdots, a_{n-1} \in k$, todo elemento de $k(\alpha)$ se escreve como:

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$$

defina $\alpha^*(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta^{n-1}$ □

Definição 1.45. *Seja F/k uma extensão de corpos, definimos o seguinte grupo:*

$$Aut(F) := \{\sigma : F \to F / \sigma \text{ é automorfismo}\}.$$

Se $G \subseteq Aut(F)$ é subgrupo, definimos o seguinte subcorpo de F:

$$F^G = \{\alpha \in F / \sigma(\alpha) = \alpha, \forall \sigma \in G\},$$

que é chamado o corpo fixo de G.

Proposição 1.46. *Seja F/k uma extensão finita, então:*

$$\#Aut(F/k) \leq [F : k].$$

Demonstração. Como F/k é uma extensão finita, temos que é algébrica e finitamente gerada. Logo $\mathrm{Aut}(F/k) \subset \{\sigma : F \to \overline{F} / \sigma|_k = id\} \leq [F : k]$. □

Observação 1.47. Se F/k é normal então todo automorfismo é um k-morfismo, e σ's são mutuamente distintos se F/k é separável. Logo $\#\mathrm{Aut}(F/k) = [F : k]$

Lema 1.48 (Lema de Artin)**.** *Dado G um subgrupo de $Aut(F)$, temos as seguintes relações*

$$[F : F^G] = |G| = \#Aut(F/F^G).$$

Demonstração. Ver Artin (1971, Pag. 42) □

Observação 1.49. Se $F = \mathbb{F}_q(x)$, então $|PGL(2,\mathbb{F}_q)| = \#\mathrm{Aut}(\mathbb{F}_q(x)/\mathbb{F}_q) = [\mathbb{F}_q(x) : \mathbb{F}_q]$

Apresentamos o estudo de Extensões de Galois F/k, e os subgrupos associados $Aut(F/k)$ que tínhamos apresentado na seção anterior. Em particular, se k é um corpo e F/k o corpo de fatoração de f um polinômio irredutível e separável de grau 4, provamos que o grupo de Galois G_f age transitivamente no conjunto das raízes de f, isto é G_f é isomorfo a algum dos subgrupos transitivos de S_4, veja as Proposições 1.52 e 1.53.

O seguinte lema prova que, dado F/k uma extensão normal e separável, temos que o grupo $Aut(F/k)$ fixa ao corpo base k.

Teorema 1.50. *Seja F/k uma extensão finita. São equivalentes:*

1. *F é um corpo de raízes de um polinômio separável $f \in k[x]$*
2. *k é o corpo fixo de $G = Aut(F/k)$, ou seja, $F^G = k$.*
3. *$k = F^H$ para algum subgrupo $H \subseteq Aut(F)$*
4. *F/k é normal e separável.*

Demonstração. Ver Dummit (1994, Pag. 572) □

Exemplo 1.51. O corpo $k = \mathbb{Q}(\sqrt{2}, i)$ é o corpo de descomposição dos polinômios $x^2 - 2$ e $x^2 + 1$ e portanto é uma extensão normal sobre $\mathbb{Q}$. como o corpo possuí característica zero, $k/\mathbb{Q}$ é uma extensão separável de $\mathbb{Q}$, além disso, como $x^2 + 1$ é um polinômio irredutível sobre $\mathbb{Q}(\sqrt{2})$ temos $[k : \mathbb{Q}] = 4$, e o conjunto de automorfismos σ_i:

$$Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$$

	$\sqrt{2}$	$-\sqrt{2}$	i	$-i$
σ_1	$\sqrt{2}$	$-\sqrt{2}$	i	$-i$
σ_2	$\sqrt{2}$	$-\sqrt{2}$	$-i$	i
σ_3	$-\sqrt{2}$	$\sqrt{2}$	i	$-i$
σ_4	$-\sqrt{2}$	$\sqrt{2}$	$-i$	i

Seja $f(x)$ um polinômio irredutível e separável de grau n que se fatora em F/k. As seguintes proposições 1.52 e 1.53 a seguir estabelecem que o grupo G_f do fecho galoisiano de F/k é sempre um subgrupo transitivo de S_n.

Proposição 1.52. *Seja $f(x)$ um polinômio irredutível e separável de grau n, então G_f é um subgrupo transitivo de S_n.*

Demonstração. Suponha $f(x)$ irredutível. Seja α, β raízes de $f(x)$ que são distintas pois $f(x)$ é separável. Como $f(x)$ é irredutível existe $\lambda^* : k(\alpha) \to k(\beta)$ tal que $\lambda^*(\alpha) = \beta$. Estendemos λ^* pelo pelo Lema 1.44, isto é existe $\sigma : E \to E$ tal que $k(\alpha), k(\beta) \hookrightarrow E$. Logo temos que $\sigma(\alpha) = \sigma|_{k(\alpha)}(\alpha) = \lambda^*(\alpha) = \beta$. □

Proposição 1.53. *Dado $f(x)$ é um polinômio separável. Temos que $f(x)$ é irredutível se, e somente se, G_f age transitivamente nas raízes de $f(x)$.*

Demonstração. Pela Proposição 1.52 temos provado que se $f(x)$ é irredutível, então G_f age transitivamente nas raízes de $f(x)$. Agora suponha que $f(x)$ não for irredutível. Dado a fatoração $f(x) = g(x)h(x) \in k[x]$, onde $g(x) = \prod(x - \alpha_i)$ e $h(x) = \prod(x - \beta_j)$ em $E[x]$. Como $f(x)$ não tem raízes repetidas, temos que cada $\alpha_i \neq \beta_j$. Por outro lado, temos que G_f age transitivamente nas raízes de $f(x)$. Isto é, existe $\sigma \in G_f$ tal que $\sigma(\alpha_1) = \beta_1$, logo β_1 é raiz de $g(x)$ e $h(x)$. Então $f(x)$ tem uma raiz com multiplicidade 2, que é uma contradição. □

Dado F/k galois, com $G = Aut(F/k)$, o seguinte Teorema nos ajudará a estabelecer as relações dos subgrupos $H \leq G_F$ e os sub corpos $k \subseteq E \subseteq F$, onde E é o corpo fixo de H.

Teorema 1.54 (Teorema Fundamental de Galois)**.** *Seja F/k uma extensão de Galois, temos que existe uma bijeção entre o conjunto de subcorpos intermediários de F/k e os subgrupos de $G = Gal(F/k)$ dada por*

$$\begin{array}{ccc} k \subseteq E \subseteq F & & H \leq G \\ E & \longrightarrow & \mathfrak{F}(E) = Gal(F/E) \\ F^H = \mathfrak{G}(H) & \longleftarrow & H \end{array}$$

tal que:

a) Seja $H_1, H_2 \leq G$, então $H_1 \subseteq H_2$ se e somente se $F^{H_2} \subseteq F^{H_1}$.

b) $[H_1 : H_2] = [F^{H_2} : F^{H_1}]$.

c) Se $\sigma \in G$, então fazer $\sigma H \sigma^{-1}$ é equivalente a fazer $\sigma(F^H)$. Isto é $\sigma Gal(F/E)\sigma^{-1} = Gal(F/\sigma(E))$

d) $H \triangleleft G$ se e somente se F^H/k é normal. Logo $Gal(F^H/k) \cong G/H$

e) $H_1 \cap H_2$ está em bijeção com $F^{H_1}F^{H_2}$

f) $E_1 \cap E_2$ está em bijeção com $\langle Gal(F/E_1), Gal(F, E_2)\rangle$

Demonstração. Ver Artin (1971, Pag. 47-49) □

CAPÍTULO

2

FECHO GALOISIANO DE EXTENSÕES QUÁRTICAS

Na primeira parte deste capítulo apresentamos a teoria geral para extensões quárticas sobre um corpo qualquer, que são as ferramentas principais para a realização deste trabalho. Logo, sobre o corpo $\mathbb{F}_q(f(x))$ apresentamos a contagem dos polinômios f com seu grupo de Galois associado. A prova dos resultados obtidos, foram feitos com uma abordagem levemente diferente ao proposto pelo autor R. Valentini no artigo: Galois closures of quartic subfields of rational function fields (VALENTINI, 2013).

2.1 Grupo de Galois para um polinômio de grau 4

Dado k um corpo qualquer, nesta parte estudamos extensões F/k de grau 4. Para $f(x)$ um polinômio mônico irredutível de grau 4, associamos assim sua cúbica resolvente R_f, para estabelecer uma relação com os grupos de Galois G_f e G_{R_f} associados as extensões.

Proposição 2.1. *Dado $F(T) \in k(y)[T]$ e $\lambda \in k$, temos as seguintes relações:*

(i) $Gal(F(T)) = Gal(F(T+\lambda))$

(ii) *Para* $F(T) = T^4 + aT^3 + bT^2 + cT + d - y \in k(y)[T]$ *e* $G(T) = F(T - a/4) = T^4 + \beta T^2 + \gamma T + \delta - y \in k(y)[T]$ *Por (i)* $Gal(G(T)) = Gal(F(T))$
$Gal(G(T)) = Gal(L/k(y))$, *onde L é corpo de raízes de* $G(T)$.

(iii) $k = \mathbb{F}_q(y) = \mathbb{F}_q(y-\delta) = \mathbb{F}_q(\tilde{y})$

$$\tilde{G}(T) = T^4 + \beta T^2 + \gamma T - \tilde{y} \in \mathbb{F}_q(\tilde{y})[T]$$

$Gal(\tilde{G}(T)) = Gal(F(T))$

Em conclusão, temos que para $F(T) = T^4 + aT^3 + bT^2 + cT + d - y \in k(y)[T]$ *e* $G(T) = T^4 + \beta T^2 + \gamma T - \tilde{y} \in k(\tilde{y})[T]$

$$Gal(F) = Gal(G).$$

Demonstração. Para $\sigma \in Gal(F(T))$ e $x_1,\ x_2,\ x_3,\ x_4 \in \overline{k}(y)$ as raízes de $F(T)$, temos que $\sigma(x_j) = x_{\sigma(j)}$ para todo $j = \overline{1,4}$. Como $x_j, x_{\sigma(j)}, x_j + \lambda, x_{\sigma(j)} + \lambda \in \mathscr{R}(G(T))$ (corpo de raízes de $G(T)$), assim $\mathscr{R}(G(T)) = \mathscr{R}(F(T))$. Logo

$$Gal(F(T)) = Gal(\mathscr{R}(F(T))/k(y)) = Gal(\mathscr{R}(F(T+\lambda))/k(y)) = Gal(G(T)).$$

□

Lema 2.2. *Dado* $F(T) \in k(y)[T]$ *e* $\lambda, \sigma \in k$*, então*

(i) $Gal(F(T)) = Gal(F(T+\lambda))$

(ii) $Gal(F(T)) = Gal(F(T+\lambda) + \sigma)$

Demonstração. Para (ii) observe que, dado $\theta_i + \lambda$ raiz de $F(T+\lambda)$ então $F(\theta_i + \lambda) = 0$ se, e somente, se $F(\theta_i + \lambda) + \sigma = 0$.

□

Dado F o polinômio minimal de $\mathbb{F}(x)/\mathbb{F}(x^4 + ax^3 + bx^2 + cx + d)$. A seguinte Proposição proporciona as propriedades da cúbica resolvente R_F com respeito ao F dado, e as relações dos grupos de galois associados G_F e G_{R_F}.

Proposição 2.3. *Dado* k *um corpo, e* $f(x) = x^4 + ax^3 + bx^2 + cx + d \in k[x]$ *um polinômio irredutível e separável, e* $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \bar{k}$ *suas raízes. Considere*

$$\theta_1 = (\alpha_1\alpha_2) + (\alpha_3\alpha_4),\ \theta_2 = (\alpha_1\alpha_3) + (\alpha_2\alpha_4),\ \theta_3 = (\alpha_1\alpha_4) + (\alpha_2\alpha_3)$$

que geram o polinômio

$$R_f(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - c^2 - 4bd). \tag{2.1}$$

dado o discriminante:

$$\Delta_f = -128b^2d^2 - 4a^3c^3 + 16b^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 + 144a^2bd^2 - 192acd^2 + a^2b^2c^2 - 4a^2b^3d - 6a^2c^2d + 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd$$

temos que:

a) $\Delta_g = \Delta_f$.

b) $k(\theta_1,\theta_2,\theta_3) = \mathfrak{F}(V \cap G_f)$, *logo* $k \subseteq k(\theta_1,\theta_2,\theta_3) \subseteq M$, *onde* M *é o corpo de fatoração de* f.

c) $\#G_{R_f}$ *divide a* $\#G_f$ *e* $[G_f : V \cap G_f] = \#Aut(k(\theta_1,\theta_2,\theta_3)/k)$.

O polinômio $R_f(x)$ *é chamado a* ***cúbica resolvente*** *de* f.

Demonstração. A igualdade $a)$ é clara pelas equações dos $\theta_i \in k$ raízes da cúbica resolvente. Para a prova de $b)$ fazemos por doble inclusão. Tomando primeiro $\sigma \in G_f \cap V$, temos que σ fixa a cada θ_i. Logo $k(\theta_1,\theta_2,\theta_3)$ é um subcorpo do corpo fixado por $G_f \cap V$. Para a outra inclusão usamos o teorema fundamental da teoria de Galois. Logo dado $\sigma \notin G_f \cap V$, temos que os θ_i não são fixados por σ. Então σ não fixa ao corpo $k(\theta_1,\theta_2,\theta_3)/k$. Isto é $\sigma \notin \mathfrak{G}(k(\theta_1,\theta_2,\theta_3)/k)$. O qual é equivalente a $\mathfrak{G}(k(\theta_1,\theta_2,\theta_3)/k) \subseteq G_f \cap V$. Assim $\mathfrak{F}(G_f \cap V) \subseteq k(\theta_1,\theta_2,\theta_3)/k$. Para a parte $c)$, considerando L o corpo de fatoração de f, usamos $b)$. Logo $k \subseteq k(\theta_1,\theta_2,\theta_3) = \mathfrak{F}(G_f \cap V) \subseteq L$. Logo, usado o teorema fundamenta de Galois, temos que $Aut(k(\theta_1,\theta_2,\theta_3)/k) = [G_f : V \cap G_f]$. □

Observação 2.4. Pela prova vemos que, existe outra forma de definir una cúbica resolvente. Consideremos

$$\theta_1 = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4),\ \theta_2 = (\alpha_1+\alpha_3)(\alpha_2+\alpha_4),\ \theta_3 = (\alpha_1+\alpha_4)(\alpha_2+\alpha_3)$$

então $R'_f(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3)$.

$$R'_f(x) = x^3 - (\theta_1+\theta_2+\theta_3)x^2 + (\theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3)x - \theta_1\theta_2\theta_3$$

$$R'_f(x) = x^3 - 2bx^2 + (b^2+ac-4d)x + (c^2+a^2d-abc) \tag{2.2}$$

Se $car(k) \neq 2$, e fazendo a substituição $x = y - a/4$, temos que toda quártica f se escreve da forma:

$$f(y) = y^4 + py^2 + qy + r$$

com

$$\begin{aligned} p &= \frac{-3a^2+8b}{8} \\ q &= \frac{a^3-4ab+8c}{8} \\ r &= \frac{-3a^4+16a^2b-64ac+256d}{256} \end{aligned}$$

sua cúbica resolvente é:

$$R''_f(x) = x^3 - 2px^2 + (p^2-4r)x + q^2 \tag{2.3}$$

Onde $(\theta_1+\theta_2+\theta_3) = 2p$,
$\theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3 = p^2-4r$ e $\theta_1\theta_2\theta_3 = q^2$
e o discriminante de $f(x)$ é

$$\Delta = -(4p^3+27q^2)q^2 + 16p(p^3+9q^2)r - 128p^2r^2 + 256r^3 [Dummit(1994, p.613-614)].$$

Para k um corpo, e $f(x) = x^4 + ax^3 + bx^2 + cx + d \in k[x]$ um polinômio irredutível e separável, o Teorema 2.5 apresenta uma classificação geral dos G_f com k um corpo de caraterística arbitraria.

Teorema 2.5. *Seja f é um polinômio separável e irredutível de grau 4 sobre um corpo k, e $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \bar{k}$ suas raízes. Se $R_f(x)$ é sua cúbica resolvente, então para $m :=$# $Gal(R_f, k)$ =1,2,3 ou 6 temos:*

(1) $m = 6$ se, e somente se, G_f é isomorfo a S_4.

(2) $m = 3$ se, e somente se, G_f é isomorfo a A_4.

(3) $m = 2$ se, e somente se, G_f é isomorfo a C_4 ou D_4.

(4) $m = 1$ se, e somente se, G_f é isomorfo a V.

(KAPLANSKY, 1972, Pag.52)

Demonstração. Como $f(x)$ é um polinômio irredutível e separável, pela Proposição 1.53 temos que $k(\alpha_1, \alpha_2, \alpha_3, \alpha_4)/k$ é uma extensão com grupo de Galois com subgrupo transitivo do S_4. (1) para o caso $m = 6$, temos pela Proposição 2.3 que $\mid G_f \mid = 6 \mid G_f \cap V \mid$, isto é G_f é um subgrupo transitivo do S_4 com ordem divisível por 6. Logo G_f é isomorfo a S_4 ou A_4. Suponha $G_f \cong A_4$, temos que $12 = \mid G_f \mid = 6 \mid G_f \cap V \mid$=24, que é absurdo. Assim $G_f \cong S_4$, analogamente provamos $m = 3$ (2). Para o caso $m = 2$, temos que $\mid G_f \mid = 2 \mid G_f \cap V \mid$. Logo G_f é um subgrupo transitivo de S_4 com ordem múltiplo de 2. Observe que G_f não é isomorfo a V, S_4 ou A_4, usando os argumentos para o caso $m = 6$. Assim G_f é isomorfo a C_4 ou D_4. Por último o caso (4) temos que é direito. Pois usando a igualdade $\mid G_f \mid = \mid G_f \cap V \mid$, então G_f é um subgrupo de V tal que $\mid G_f \mid \leq 4$. Logo $\mid G_f \mid = 4$, isto é $G_f \cong V$. O caso $G_f \cong V$, implica $m = 1$, e análogos são óbvios. □

Observação 2.6. Para k um corpo, Se $R_f(x)$ é irredutível, então G_f é isomorfo a S_4 o A_4.

Teorema 2.7. *Consideremos car(k)$\neq$ 2. Para f um polinômio de grau 4 irredutível e separável e R_f sua cúbica resolvente, com fatoração em polinômios irredutíveis dada por:*

$$R_f(x) = (x - r)(x^2 - sx + t) \in k[x], \tag{2.4}$$

e $L = k(\sqrt{s^2 - 4t})$ seu corpo de fatoração, com $r = \alpha_1\alpha_2 + \alpha_3\alpha_4$. Temos que $G_f \cong C_4$ se, e somente se, $\alpha_1\alpha_2$, $\alpha_1 + \alpha_2 \in L$. Isto último é equivalente a dizer que os polinômios

$$x^2 - rx + d \quad e \quad x^2 + ax + (b - r) \tag{2.5}$$

se fatoram em L. Kappe e Warren (1989, Theorem 1,iv)

Demonstração. Seja M o corpo de raízes de f. Dados $\alpha_1\alpha_2$, $\alpha_1 + \alpha_2 \in L$, temos que os polinômios em 2.5 se fatoram. Para provar que G_f é isomorfo a C_4, observamos que $\#D_4 = 8$. Logo basta provar que $[M : k] \leq 4$. Temos que todas a raízes de $g(x)$ estão no corpo L, então

$$\theta_2 - \theta_3 = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) \in L,$$

logo $\alpha_3 - \alpha_4 \in L$, assim $\alpha_3, \alpha_4 \in L$. Isto é $M = L(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = L(\alpha_1, \alpha_2)$. Considerando $\phi(x) = (x - \alpha_1)(x - \alpha_2)$, a extensão $[L(\alpha_1, \alpha_2) : L] \leq 2$ e temos que a extensão

$$[M : k] = [L(\alpha_1, \alpha_2) : L][L : k] \leq 4.$$

Agora suponhamos $G_f \cong C_4$. Para $\sigma = (1324)$ um gerador de C_4, temos que o grupo $G_f \cap V = \{id, (12)(34)\}$. Definindo

$$h(x) = (x^2 - rx + d)(x^2 + ax + (b - r)),$$

temos que $h(x)$ se fatora em L. Assim provamos que $\alpha_1\alpha_2$, $\alpha_1 + \alpha_2 \in L$. □

Observação 2.8. Da prova do Teorema temos que para $r = \alpha_1\alpha_2 + \alpha_3\alpha_4$,

$$h(x) = (x^2 - rx + d)(x^2 + ax + (b - r)).$$

Sobre $car(k) \neq 2$. Se $f(x)$ é um polinômio irredutível, para $r = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$ e $R_f(x) = (x - r)(x^2 - sx + t)$, considerando $L = k(\sqrt{s^2 - 4t})$, temos que $G_f \cong C_4 = \langle (1324) \rangle$ se, e somente se, $\alpha_1\alpha_2$ e $\alpha_1 + \alpha_2 \in L$. Neste caso temos o polinômio

$$h(x) = (x^2 - (b - r)x + d)(x^2 + ax + r).$$

Teorema 2.9. *Para car(k)≠ 2 e $f(x) = x^4 + bx^2 + d \in k[x]$ um polinômio irredutível, temos a seguinte classificação:*

(1) Se $d \in [k^\times]^2$, então $G_f \cong V$

(2) Se $d \notin [k^\times]^2$ mas $d(b^2 - 4d) \in [k^\times]^2$, então $G_f \cong C_4$

(3) Se $d \notin [k^\times]^2$ e $d(b^2 - 4d) \notin [k^\times]^2$, então $G_f \cong D_4$

Kappe e Warren (1989, Theorem 3)

Demonstração. Consideremos a cúbica resolvente

$$R_f(x) = x(x^2 - 2bx + b^2 - 4d),$$

temos que o caso (1) é direito. Para o caso (2), temos que $d \notin [k^*]^2$ mas $d(b^2 - 4d) \in [k^*]^2$. Logo temos a igualdade de corpos $k(\sqrt{d}) = k(\sqrt{b^2 - 4d})$. Assim o polinômio

$$h(x) = (x^2 - bx + d)(x^2)$$

se fatora em $k(\sqrt{d})$. Pelo Teorema 2.7 temos que $G_f \cong C_4$. O caso (3) é consequência do último. □

Seja $\mathbb{F}_q$ um corpo finito tal que $car(\mathbb{F}_q) \neq 2$, o seguinte Teorema é usado para determinar quando o grupo G_F do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(x^4+bx^2+cx)$ é um subgrupo transitivo de A_4.

Teorema 2.10. *Para $car(k) \neq 2$. Dado $f(x) \in k[x]$ separável e $\alpha_1, \cdots, \alpha_n \in \overline{k}$ suas raízes, Temos que Δ_f é um quadrado perfeito se, e somente se, $G_f \subseteq A_n$. Dummit (1994, p. 611)*

Observação 2.11. Se Δ_f não é um quadrado, logo G_f é isomorfo a algum dos seguintes grupos S_4, C_4 ou D_4.

Para $car(k) = 2$, e $F(T) = T^4 + bT^2 + cT + y \in \mathbb{F}_q[T]$ com $c \neq 0$. A seguinte Proposição apresenta que não existe elemento $\sigma \in G_F$ de ordem 4.

Proposição 2.12. *Para $q = 2^e$, com $e \geq 1$ inteiro. Dado $a(T) = T^4 + bT^2 + cT \in \mathbb{F}_q[T]$, com $c \neq 0$, então o Grupo de Galois do corpo de fatoração de $a(T) = y$ sobre $\mathbb{F}_q(y)$ não tem subgrupo cíclico de ordem 4. Donde $a(T)$ é chamado polinômio linearizado sobre $\mathbb{F}_q$ de grau 4.*

Demonstração. Como $c \neq 0$, então $a(T)$ é separável. Seja $F/\mathbb{F}_q$ uma extensão de corpos, para $u, v \in F/\mathbb{F}_q$ e $\lambda \in \mathbb{F}_q$, temos $a(u+v) = a(u) + a(v)$. Sejam $u_1 = 0$, u_2, u_3, u_4 as raízes de $a(T)$, para x raiz de $A(T)$, temos que x, $x+u_2$, $x+u_3$, $x+u_4$ são as raízes de $A(T)$. Considere λ um gerador do corpo de fatoração de $a(T)$ da forma $\mathbb{F}_{q^s}/\mathbb{F}_q$, então $s = 1, 2$ ou 3. Logo, o fecho galoisiano para o polinômio $A(T)$ sobre $\mathbb{F}_q$ é $\mathbb{F}_q(y)(x, \lambda)$. Considere os automorfismo

$$\sigma_{ij} \begin{cases} x & \to & x + u_i \\ \lambda & \to & \lambda^{q^j} \end{cases}, \ i = 1, \cdots, 4.$$

Então

$$\sigma_{ij}^2(x) = x \text{ e } \sigma_{ij}^s(\lambda) = \lambda.$$

Logo $\sigma_{ij}^{mmc(2,s)} = id$. Então, temos os seguintes casos:

(i) Para $s = 1$, $\sigma_{ij} = id$.

(ii) Para $s = 2$, $\sigma_{ij}^2 = id$.

(iii) Para $s = 3$, $\sigma_{ij}^2(x) = x$, $\sigma_{ij}^3(\lambda) = \lambda$.

Então não ha subgrupo cíclico de ordem 4 no grupo de Galois de $a(T) = y$. □

Para $q = 2^e$, seja F o polinômio minimal de $\mathbb{F}_q(x)/\mathbb{F}_q(x^4+ax^3+bx^2+cx)$, associamos a ele sua cúbica R_F (ver equação 2.1). Se R_F é irredutível, então a seguinte proposição é usada para determinar quando $G_{R_F} \cong A_3$.

Proposição 2.13. *Dado o polinômio irredutível $x^3 + px + q$, com z_1, z_2 e z_3 suas raízes no corpo de fatoração F/k e o polinômio $p(x) = y^2 + qy + p^3 + q^2$, com raízes*

$$\beta_1 = z_1^2z_2 + z_2^2z_3 + z_3^2z_1 \text{ e } \beta_2 = z_2^2z_1 + z_1^2z_3 + z_3^2z_2.$$

Se $p(T)$ se fatora em k, então o grupo de Galois da cúbica é A_3.

Demonstração. Se $p(T)$ se fatora em k, então $\beta_1, \beta_2 \in k$. Dado $\sigma \notin A_3$, temos que σ não fixa β_1 e β_2. Então $\sigma \notin Gal(p(x),k)$. Isto é $Gal(p(x),k) \subseteq A_3$. Logo $\mathfrak{F}(A_3) \subseteq k(\beta_1,\beta_2) = k$. □

Exemplo 2.14. Seja $f(x) = x^4 + 5x + 5$ em $\mathbb{Q}[x]$, então $G_f \cong C_4$.

Usando o teorema 2.7. Sua cúbica resolvente é:

$$R_f(x) = (x-5)(x^2+5x+5),$$

Temos que para $q = 5$, q divide a 5 e q^2 não divide a 5, pelo critério de Einstein temos que $f(x)$ é irredutível sobre $\mathbb{Z}[x]$, logo é irredutível em $\mathbb{Q}[x]$.
E no mesmo teorema, seja $h(x) = (x^2-5x+5)(x^2-5)$, e $L = \mathbb{Q}(\sqrt{5})$, temos que $h(x)$ e $R_f(x)$ tem o mesmo corpo de fatoração. Logo $G_f \cong C_4$

Exemplo 2.15. Seja $f(x) = x^4 - x - 1$ em $\mathbb{Q}[x]$, então $G_f \cong S_4$.

Provemos que $f(x)$ e sua cúbica resolvente $R_f(x) = x^3 + 4x - 1$ são irredutíveis sobre $\mathbb{Q}[x]$. Temos que ± 1 não são raízes de $f(x)$ então é irredutível em $\mathbb{Q}[x]$. Analogamente ± 1 não são raízes de $R_f(x)$, temos que $g(x)$ é irredutível em $\mathbb{Q}[x]$. então $m = 3$ ou 6, e $\Delta_{R_f} = -283$ não é um quadrado. Então pelo Teorema 2.5, temos que $G_f \cong S_4$.

Exemplo 2.16. Seja $f(x) = x^4 + 8x + 12$ em $\mathbb{Q}[x]$, então $G_f \cong A_4$.

Provemos que $f(x)$ e sua cúbica resolvente $R_f(x)$ são irredutíveis sobre $\mathbb{Q}[x]$.
Se $f(x)$ é redutível, então ele tem um fator linear ou é o produto de dois quárticos irredutíveis. Se tem um fator linear, então temos é um divisor de 12, que não é possível. Se $f(x)$ é levado para $mod 5$, temos que $x^4 + 8x + 12 \equiv (x-4)(x^3+4x^2+x+2)(mod 5)$, e como $\phi(x) = x^3+4x^2+x+2$ não tem raízes em $\mathbb{Z}/p\mathbb{Z}[x]$, então $f(x)$ é irredutível em $\mathbb{Z}[x]$ ou tem raiz $\alpha \equiv (4 mod 5)$ (que não é verdade). Então $f(x)$ é irredutível em $\mathbb{Z}[x]$, logo pelo Lema de Gauss, temos que $f(x)$ é irredutível em $\mathbb{Q}[x]$.
Como sua cúbica resolvente é:

$$R_f(x) = x^3 - 48x - 64$$

temos que $R_f(x+1) = x^3 - 3x^2 - 45x - 111$ é irredutível em $\mathbb{Q}[x]$ pelo criterio de Einstein com $q = 3$. Como $\Delta_{R_f} = 576^2$ que é um quadrado, logo pelo Teorema 2.5 temos que $G_f \cong A_4$.

Exemplo 2.17. Seja $f(x) = x^4 - 3x^2 + 5$ em $\mathbb{Q}[x]$, então $G_f \cong D_4$.

Se $x^2 = y$, $f(y) = y^2 - 3y + 5$ em $\mathbb{Q}[x]$ e $D_f = i\sqrt{11}$, $f(x)$ não tem raízes em $\mathbb{Q}$. Sua cúbica resolvente é:

$$R_f(x) = (x+3)(x^2-20),$$

E usando o Teorema 2.7, Para $h(x) = (x^2+3x+5)(x^2)$, e $L = \mathbb{Q}(\sqrt{5})$, temos que $h(x)$ e $g(x)$ não tem o mesmo corpo de fatoração ($h(x)$ se fatora em $\mathbb{Q}(i,\sqrt{11})$). Também pode-se ver pelo Teorema 2.9, que $5 \notin [\mathbb{Q}]^2$ e $5((-3)^2-20) = -55 \notin [\mathbb{Q}]^2$ então $G_f \cong D_4$.

Exemplo 2.18. Seja $f(x) = x^4 - x^2 + 36$ em $\mathbb{Q}[x]$, então $G_f \cong V$.

Temos que se $y = x^2$, $\Delta_f = 1 - 144 = -143$, então $f(x)$ é irredutível, e $R_f(x) = (x+1)(x^2-144)$ se fatora em $\mathbb{Q}[x]$ pelo Teorema 2.5, temos que $G_f \cong V$.

Observação 2.19. A seguinte Proposição prova que $F(T) = T^4 + aT^3 + bT^2 + cT + d - y \in k(y)[T]$ é o polinômio minimal da extensão $\mathbb{F}_q(x)/\mathbb{F}_q(x^4+ax^3+bx^2+cx+d)$.

Proposição 2.20. *Seja k um corpo e considere o polinômio $f(x) = x^4+ax^3+bx^2+cx+d \in k[x]$, então $F(T) = T^4+aT^3+bT^2+cT+d-y \in k(y)[T]$ é irredutível.*

Demonstração. Como F é primitivo em $k[T][y]$ e é linear em y, então F é irredutível em $k[T][y]$. Pelo Lema de Gauss, a irredutibilidade de $F \in k[y][T]$ implica que $F \in k(y)[T]$ é irredutível. □

2.2 Fecho galoisiano de extensões quárticas do corpo de funções sobre corpos finitos

Seja k um corpo e considere um polinômio $f(x) = x^4+ax^3+bx^2+cx+d \in k[x]$. Para $y := f(x)$, temos claramente que x é raiz do polinômio

$$F(T) = T^4+aT^3+bT^2+cT+d-y \in k(y)[T].$$

A Proposição 2.20, implica que $F \in k(y)[T]$ é irredutível. Em particular, temos que F é o polinômio minimal de x sobre o corpo $k(y)$, de onde segue $[k(y,x) : k(y)] = 4$. Lembremos que se $F \in k(y)[T]$ é separável, ou seja, se $F' := 4T^3+3aT^2+2bT+c \neq 0$, então o grupo de Galois G_F do fecho normal de $k(y,x)/k(y)$ é um subgrupo transitivo de S_4 (Proposição 1.53 e Teorema 2.5). Assim, pelo Exemplo A.2, temos que G_F é isomorfo a algum dos seguintes grupos: S_4, A_4, D_4 (o grupo diedral de ordem 8), C_4 (o grupo cíclico de ordem 4) ou o grupo Klein-4

$$V := \{id, (12)(34), (13)(24), (14)(23)\}.$$

Seja $\mathbb{F}_q$ um corpo finito com q elementos, onde q é potência de um primo p. Nessa seção, determinaremos o número de polinômios $f(x) = x^4+ax^3+bx^2+cx+d \in \mathbb{F}_q[x]$ para os quais o grupo de Galois G_F associado (conforme discussão anterior) corresponde a cada um dos subgrupos transitivos de S_4.

Teorema 2.21. *Sejam $p \neq 2$ um primo e $q = p^e$, onde $e \geq 1$ é um inteiro. Para cada $f(x) \in M := \{f(x) \in k[x] \,|\, f(x)$ é mônico de grau $4\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$. Então o conjunto M é particionado da seguinte forma :*

(i) *Existem* $q^4 - q^3$ *elementos* $f(x) \in M$ *tais que* $G_F \cong S_4$.

(ii) *Se* $q \equiv 3 \mod 4$, *então existem* q^3 *elementos* $f(x) \in M$ *tais que* $G_F \cong D_4$.

(iii) *Se* $q \equiv 1 \mod 4$, *então existem* $q^3 - q^2$ *elementos* $f(x) \in M$ *tais que* $G_F \cong D_4$ *e outros* q^2 *tais elementos para os quais* $G_F \cong C_4$.

Demonstração. • Caso $a = d = 0$.

Para $y = x^4 + bx^2 + cx$, conforme Proposição 2.20, temos o polinômio irredutível

$$F(T) = T^4 + bT^2 + cT - y \in \mathbb{F}_q(y)[T] \tag{2.6}$$

o qual é separável. De fato, como $car(\mathbb{F}_q) \neq 2$, temos que $F'(T) = 4T^3 + 2bT + c \neq 0$. Assim, pelo Teorema 2.5, G_F é isomorfo a algum dos seguintes subgrupos de S_4: A_4, V, D_4, C_4 ou S_4, onde $V := \{id, (12)(34), (13)(24), (14)(23)\}$. O discriminante de F é (veja Proposição:2.3)

$$\Delta_F = -(4b^3 + 27c^2)c^2 - 16b(b^3 + 9c^2)y - 128b^2y^2 - 256y^3.$$

Observamos que, por ter grau 3 em y, o discriminante Δ_F não é um quadrado em $\mathbb{F}_q(y)$. Assim, pelo Teorema 2.10, G_F não é um subgrupo de A_4. Como $V \subseteq A_4$, as únicas possibilidades para G_F são: S_4, D_4, ou C_4. Nesse caso, G_F dependerá da cúbica resolvente de $F(T)$, a qual é dada por (ver (2.2))

$$R_F(T) = T^3 - 2bT^2 + (b^2 + 4y)T + c^2,$$

- Subcaso $c \neq 0$.

Como R_F (que é linear em y) é primitivo em $\mathbb{F}_q[T][y]$, temos que $R_F \in \mathbb{F}_q[T][y]$ é irredutível. Assim, pelo Lema de Gauss 1.20, $R_F \in \mathbb{F}_q(y)[T]$ é irredutível. Logo, $R_F'(T) = 3T^2 - 4bT + (b^2 + 4y) \neq 0$ implica que R_F é separável. Dessa forma, pela Proposição 1.53, G_{R_F} é subgrupo transitivo de S_3, ou seja G_{R_F} é (isomorfo a) S_3 ou A_3. Como Δ_F não é um quadrado em $\mathbb{F}_q(y)$ e $\Delta_{R_F} = \Delta_F$ (veja Teorema 2.10), temos que G_{R_F} não é isomorfo a A_3. Logo, para $c \neq 0$, temos $G_{R_F} \cong S_3$ e portanto $G_F \cong S_4$ (veja Teorema 2.5). Conforme esta análise, existem $q(q-1)$ polinômios da forma

$$f(x) = x^4 + bx^2 + cx \in \mathbb{F}_q[x]$$

para os quais $G_F \cong S_4$

- Subcaso $c = 0$.

Nesse caso, a cúbica resolvente de $F(T)$ é dada por

$$R_F(T) = T(T^2 - 2bT + b^2 + 4y),$$

e seu discriminante $\Delta_{R_F} = -16y$ não é um quadrado em $k(y)$. Ou seja, o polinômio $R_F(T) = T^2 - 2bT + b^2 + 4y \in \mathbb{F}_q(y)[T]$ é irredutível. Assim, pelo Teorema 2.9, $G_F \cong D_4$ ou C_4 e este

último caso o ocorre se, e somente se, $-y(b^2+4y)$ é um quadrado em $\mathbb{F}_q(y)$. Claramente, essa última condição é equivalente $b=0$ e $4 \mid (q-1)$.
Assim, para $q \equiv 1 \mod 4$, temos que $G_F \cong C_4$ para $f(x)=x^4 \in M$, e $G_F \cong D_4$ para os demais $q-1$ polinômios $f(x)=x^4+bx^2 \in M$. Além disso, para $q \equiv 3 \mod 4$, temos que $G_F \cong D_4$ para todos os q polinômios $f(x)=x^4+bx^2 \in M$.

- Caso $a,b,c,d \in \mathbb{F}_q$ arbitrários.

Como $\mathrm{car}(\mathbb{F}_q) \neq 2$, para $F(T)=T^4+aT^3+bT^2+cT+d-y$, consideramos o polinômio $G(T)-\delta = F(T-a/4) = T^4+\beta T^2+\gamma T-\tilde{y}$ com $\tilde{y}=f(x-a/4)$, e

$$\begin{aligned} \beta &= \tfrac{1}{8}(-3a^2+8b) \\ \gamma &= \tfrac{1}{8}(a^3-4ab+8c) \\ \delta &= \tfrac{1}{256}(-3a^4+16a^2b-64ac+256d), \end{aligned}$$

que pela Proposição 2.1 os grupos de Galois G_F e G_G são iguais.

Agora, fixemos um par $(a,d) \in \mathbb{F}_q \times \mathbb{F}_q$. Temos que o mapa

$$\begin{array}{ccc} \mathbb{F}_q \times \mathbb{F}_q & \to & \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \\ (\ b\ ,\ c\ ) & \to & (\ \beta\ ,\ \gamma\ ,\ \delta\ ) \end{array}$$

é injetivo. De fato, para (b_1,c_1) e $(b_2,c_2) \in \mathbb{F}_q \times \mathbb{F}_q$, temos que:

$$\begin{aligned} -3a^2+8b_1 &= -3a^2+8b_2 \\ a^3-4ab_1+8c_1 &= a^3-4ab_2+8c_2 \end{aligned}$$

implica $b_1=b_2$ e $c_1=c_2$. Assim cada (b,c) gera um único polinômio $G(T)-\delta$, o qual tem a forma (2.6). Dado $G(T)-\delta$, conforme discussão anterior no caso $(a,d)=(0,0)$, seu grupo de Galois G_F é dado pelos seguintes casos:

(i) $\gamma = \frac{1}{8}(a^3-4ab+8c) \neq 0$. Claramente, existem q^2-q pares $(b,c) \in \mathbb{F}_q \times \mathbb{F}_q$ tais que $\gamma \neq 0$. Assim das q^2 escolhas para $(a,d) \in \mathbb{F}_q \times \mathbb{F}_q$ temos que existem $q^2(q^2-q)$ polinômios $f(x)$ em M tais que $G_F \cong S_4$.

(ii) $\gamma = \frac{1}{8}(a^3-4ab+8c) = 0$.

(a) $q \equiv 1 \mod 4$.

* $\beta = 0$. Como $-a^3+4ab=8c$, temos que $\beta=0$ se, e somente se $b=3a^2/8$. Ou seja, que (b,c)=$(3a^2/8, a^3/16)$ é o único par em $\mathbb{F}_q \times \mathbb{F}_q$ que satisfaz tais condições. Logo, das q^2 escolhas para $(a,d) \in \mathbb{F}_q \times \mathbb{F}_q$, segue que existem q^2 polinômios $f(x)$ em M tais que $G_F \cong C_4$.

* $\beta \neq 0$. De $\beta = \frac{1}{8}(-3a^2+8b)$, temos que existem $q-1$ pares $(b,c) \in \mathbb{F}_q \times \mathbb{F}_q$ tais que $\beta \neq 0$. Das q^2 escolhas para $(a,d) \in \mathbb{F}_q \times \mathbb{F}_q$, segue que existem $q^2(q-1)$ polinômios $f(x)$ em M tais que $G_F \cong D_4$.

(b) $q \equiv 3 \mod 4$. Lembremos que neste caso o grupo G_F não depende de β. Como temos q pares $(b,c) \in \mathbb{F}_q \times \mathbb{F}_q$ tais que $\gamma = 0$, logo as q^2 escolhas para $(a,d) \in \mathbb{F}_q \times \mathbb{F}_q$ geram q^3 polinômios $f(x)$ em M tais que $G_F \cong D_4$.

□

Teorema 2.22. *Seja $q = 2^e$, onde $e \geq 1$ é um inteiro. Para cada polinômio $f(x) \in M_s$ onde $M_s := \{f(x) \in \mathbb{F}_q[x] | f(x) = x^4 + ax^3 + bx^2 + cx + d$, com $a \neq 0$ ou $c \neq 0\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$, então o conjunto M_s é particionado da seguinte forma:*

(i) Se $q \equiv 2 \mod 3$, então existem $q(q^2-1)/3$ elementos $f(x) \in M_s$ tais que $G_F \cong A_4$ e outros $q^3(q-1)$ tais elementos para os quais $G_F \cong S_4$.

(ii) Se $q \equiv 1 \mod 3$, então existem $q(q-1)(4q+1)/3$ elementos $f(x) \in M_s$ tais que $G_F \cong A_4$ e outros $q^2(q-1)^2$ tais elementos para os quais $G_F \cong S_4$.

(iii) Existem $\dfrac{q(q-1)(q-2)}{6}$ elementos $f(x) \in M_s$ tais que $G_F \cong V$.

(iv) Existem $\dfrac{q^2(q-1)}{2}$ elementos $f(x) \in M_s$ tais que $G_F \cong D_4$.

Demonstração. Para $y = f(x) + d$, conforme Proposição 2.20, temos que o polinômio

$$F(T) = T^4 + aT^3 + bT^2 + cT + y \in \mathbb{F}_q(y)[T]$$

é irredutível. Como $a \neq 0$ ou $c \neq 0$ implica $F'(T) = 3aT^2 + c \neq 0$, $F(T)$ é separável. Assim pelo Teorema 2.5, G_F é isomorfo a algum dos seguintes subgrupos de S_4: A_4, V, D_4, C_4 ou S_4.

- Caso $a \neq 0$.

A cúbica resolvente de $F(T)$, é dada por (ver (2.1))

$$R_F(T) = T^3 + bT^2 + acT + (a^2y + c^2). \tag{2.7}$$

Como R_F (que é linear em y) é primitivo em $\mathbb{F}_q[T][y]$, temos que $R_F \in \mathbb{F}_q[T][y]$ é irredutível. Assim, pelo Lema de Gauss (Lema 1.20), $R_F \in \mathbb{F}_q(y)[T]$ é irredutível. Logo, $R_F'(T) = 3T^2 + ac \neq 0$ implica que R_F é separável. Dessa forma, pela Proposição 1.53, G_{R_F} é subgrupo transitivo de S_3, ou seja G_{R_F} é (isomorfo a) S_3 ou A_3. Como

$$R_F(T+b) \quad = \quad T^3 + (ac + b^2)T + acb + (a^2y + c^2),$$

pela Proposição 2.13, temos que $G_{R_F} \cong A_3$, se a resolvente quadrática $p(T) = T^2 + (abc + a^2y + c^2)T + (ac + b^2)^3 + (abc + a^2y + c^2)^2$ se fatora em $\mathbb{F}_q(y)[T]$.

- Afirmação 1: Se $ac = b^2$, é $p(T)$ é redutível em $\mathbb{F}_q(y)[T]$ se, somente se, $q \equiv 1 \mod 3$.

$P(T) = T^2 + (abc + a^2y + c^2)T + (abc + a^2y + c^2)^2$, fazendo a translação $(abc + a^2y + c^2)T$ em $P(T)$, definimos $G(T) := P((abc + a^2y + c^2)T) = T^2 + T + 1$. Tendo, pois $q \equiv 1 \mod 3$, o polinômio $T^3 + 1$ é redutível, isto é $G(T)$ é redutível em $\mathbb{F}_q[T]$. Logo, para $q \equiv 1 \mod 3$ e $ac = b^2$, $P(T)$ é redutível em $\mathbb{F}_q(y)[T]$. Observe que, dado $a \neq 0$, da igualdade $ac = b^2$, temos que $abc = b^3$. Com o qual a cúbica resolvente é $R_F(T + b) = T^3 + b^3 + a^2y + c^2$ com $a \neq 0$, $b \in \mathbb{F}_q$ e $c = a^{-1}b^2$.

- Afirmação 2: Se $ac \neq b^2$, então $p(T)$ é irredutível em $\mathbb{F}_q(y)[T]$.

Homogenizando $p(T)$, temos a curva projetiva C de grau 2:

$$p(X,Y,Z) = X^2 + (abcZ + a^2Y + c^2Z)X + Z^2(ac + b^2)^3 + (abcZ + a^2Y + c^2Z)^2 \tag{2.8}$$

a qual tem suas derivadas parciais:

$$p_X = (abc + c^2)Z + a^2Y,\ p_Y = a^2X,\ p_Z = (abc + c^2)X.$$

sabemos que $p(X,Y,Z)$ é redutível em $\overline{\mathbb{F}}_q[X,Y,Z]$ se, e somente se, a curva tem ponto singular, isto é, existe $q \in C$ tal que $p_X(q) = p_Y(q) = p_Z(q) = 0$. Claramente

$$q = \begin{cases} (0:0:1),\ se\ abc + c^2 = 0 \\ (0:1:a^2/(abc + c^2)),\ se\ abc + c^2 \neq 0. \end{cases}$$

Em ambos casos é fácil ver que tal ponto esta na curva se, e somente se, $b^2 = ac$. Por tanto $P(X,Y,Z)$ é redutível em $\overline{\mathbb{F}}_q[X,Y,Z]$ se, e somente se, $b^2 = ac$. Equivalentemente, $P(X,Y,Z)$ é irredutível em $\overline{\mathbb{F}}_q[X,Y,Z]$ se, e somente se, $b^2 \neq ac$. A irredutibilidade em $\overline{\mathbb{F}}_q[X,Y,Z]$, implica irredutibilidade em $\mathbb{F}_q[X,Y,Z]$. Logo, para $b^2 \neq ac$, $P(T)$ é irredutível em $\mathbb{F}_q(y)[T]$.

Agora visto estas afirmações, para $b^2 \neq ac$, $P(T)$ é irredutível em $\mathbb{F}_q(y)[T]$. Logo pela Proposição 2.13, temos que $G_{R_F} \cong S_3$. Se $b^2 = ac$ e $q \equiv 1 \mod 3$, então $p(T)$ é redutível e, pela Proposição 2.13, temos que $G_{R_F} \cong A_3$. Se $ac = b^2$ e $q \equiv 2 \mod 3$, então $p(T)$ é irredutível e $G_{R_F} \cong S_3$. Logo considerando $q \equiv 1 \mod 3$, a afirmação 1 e Teorema 2.5 implicam que temos $q^2(q-1)$ polinômios $f(x)$ em M_s, tais que $G_F \cong A_4$, e temos $q^2(q-1)^2$ polinômios $f(x)$ em M_s, tais que $G_F \cong S_4$.

Para $q \equiv 2 \mod 3$, temos pelo Teorema 2.5 que todos os $q^3(q-1)$ polinômios $f(x)$ em M_s são tais que $G_F \cong S_4$.

- Caso $a = 0$ e $c \neq 0$.

Então, temos o polinômio

$$F(T) = T^4 + bT^2 + cT + y.$$

Em diante consideramos:

$$R_1(T) := R_F(T+b) = T^3 + b^2T + c^2, \tag{2.9}$$

e $p(T)$ fator irredutível de $R_1(T)$ de grau $m = 1$, 2 ou 3 em $\mathbb{F}_q[T]$. Se α é um elemento primitivo, seja $\mathbb{F}_q(\alpha) \cong \frac{\mathbb{F}_q[T]}{p(T)}$, então $Gal(R_1(T), \mathbb{F}_q) = Gal(\mathbb{F}_q(\alpha), \mathbb{F}_q)$, e este último é grupo cíclico de ordem 1,2 ou 3. Pelo Teorema 2.5, G_F é isomorfo a algum dos seguintes grupos: V, C_4, D_4, A_4.

- Subcaso $m = 1$.

Precisamos contar o número de polinômios da forma $R_F(T+b)$ em $\mathbb{F}_q[T]$ que possuem 3 raízes distintas em $\mathbb{F}_q$. Observamos que tais raízes, digamos z_1, z_2, $z_3 \in \mathbb{F}_q$ devem satisfazer

$$z_1 + z_2 + z_3 = 0 \text{ e } z_1z_2z_3 \neq 0.$$

Para tal, basta escolher elementos z_1, $z_2 \in \mathbb{F}_q^*$ distintos e dai definimos $z_3 = z_1 + z_2$ que é não nulo, pois $z_1 \neq z_2$. Temos que existem $(q-1)(q-2)$ possíveis escolhas para o par ordenado (z_1, z_2), e por tanto $(q-1)(q-2)$ possíveis escolhas para a terna (z_1, z_2, z_3). Como as 6 possíveis permutações das raízes de $(T+z_1)(T+z_2)(T+z_3)$ não alteram o polinômio, temos $(q-1)(q-2)/6$ polinômios do tipo procurado. Logo temos. Assim, para $d \in \mathbb{F}_q$, os $(q-1)(q-2)/6$ pares da forma $(b^2, c^2) \in \mathbb{F}_q \times \mathbb{F}_q^*$, geram $q\dfrac{(q-1)(q-2)}{6}$ polinômios $f(x)$ em M_s, tais que $G_F \cong V$.

- Subcaso $m = 2$.

Observamos que G_F não é isomorfo a C_4, pois o grupo de Galois do corpo de fatoração de $F(T) = T^4 + bT^2 + cT + y$ sobre $\mathbb{F}_q(y)$ somente tem subgrupos de ordem 2 (veja Proposição 2.12).

Dado $0 \neq r \in \mathbb{F}_q$ raiz de $R_F(T+b)$, o polinômio R_1 (2.9), pode ser escrito da forma $R_1(T) = (T+r)(T^2 + rT + s)$ com $T^2 + rT + s$ irredutível, logo $r \neq 0$, $s \neq 0$. Precisamos contar o número de polinômios irredutíveis da forma $T^2 + rT + s$ tais que $r \neq 0$ e $s \neq 0$. Temos que existem $(q-1)^2$ polinômios da forma $T^2 + rT + s$. Observe que a quantidade de polinômios $T^2 + rT + s$ que se fatoram em $\mathbb{F}_q$ são $(q-1)(q-2)/2$. Então subtraindo estes dois casos, temos $q(q-1)/2$ polinômios irredutíveis em $F_q[T]$. Isto é, temos $q(q-1)/2$ pares da forma $(b^2, c^2) \in \mathbb{F}_q \times \mathbb{F}_q^*$,os quais geram $q\dfrac{q(q-1)}{2}$ polinômios $f(x)$ em M_s, tais que $G_F \cong D_4$.

- Subcaso $m = 3$.

Temos que o polinômio $R_1(T)$ (2.9) é irredutível, logo pelo Teorema 2.5 temos que $G_F \cong A_4$. Visto que existem $q^2(q-1)$ polinômios $f(x)$ em M_s, subtraindo a quantidade de polinômios nos casos $m = 1$ e $m = 2$, temos que existem $q(q^2-1)/3$ polinômios de $f(x) \in M_s$, tais que $G_F \cong A_4$. □

Observação 2.23. Observe que dado $f(x) = x^4 + ax^3 + bx^2 + cx + d$ temos que:

(a) Para $q \equiv 1 \mod 3$, se $a \neq 0$ e $b^2 = ac$, existem $q^2(q-1)$ polinômios de $f(x) \in M_s$, tais que $G_F \cong A_4$.

(b) Para $a = 0$ e $c \neq 0$, existem outros $q(q^2-1)/3$ polinômios de $f(x) \in M_s$, tais que $G_F \cong A_4$.

Logo, para $q \equiv 1 \mod 3$, existem $q(q-1)(4q+1)/3$ polinômios de $f(x) \in M_s$, tais que $G_F \cong A_4$.
Se $q \equiv 2 \mod 3$ existem $q(q^2-1)/3$ polinômios de $f(x) \in M_s$, tais que $G_F \cong A_4$.

Observação 2.24. Dado $p \neq 2$ e $f(x) = x^4 + ax^3 + bx^2 + cx + d$

Dado $c \neq 0$	Temos que $G_F \cong S_4$ (vide Teorema 2.21)
Para $c = 0$	*Temos que* $q \equiv 1 \mod 4$ *e* $b = 0$ *se, e somente se,* $G_F \cong C_4$. *Se* $q \equiv 3 \mod 4$ *ou* $b \neq 0$, *logo* $G_F \cong D_4$.(*vide Teorema* 2.21)
Se $t = \frac{x^4+1}{x}$ e $q = 3$ ou 5	Temos que $G_F \cong A_4$ (vide Exemplo 2.35)
Se $t = \frac{x^4+1}{x^2}$ e $q = 3$ ou 5	Temos que $G_F \cong V$ (vide Exemplo 2.36)
Se $t = \frac{x^4+1}{x^3}$ e $q = 3$ ou 5	Temos que $G_F \cong A_4$ (vide Exemplo 2.37)

Observação 2.25. Dado $p = 2$ e $f(x) = x^4 + ax^3 + bx^2 + cx + d$, do Teorema 2.22 temos a seguinte classificação:

Dado $a \neq 0$	*Temos que* $q \equiv 1 \mod 3$ *e* $b^2 = ac$ *se, e somente se,* $G_F \cong A_4$. *Se* $q \equiv 2 \mod 3$ *ou* $b^2 \neq ac$, *logo* $G_F \cong S_4$.
Para $c = 0$ e $a \neq 0$	*Se* $\mid G_{R_F} \mid = 1$, *logo* $G_F \cong V$. *Se* $\mid G_{R_F} \mid = 2$, *logo* $G_F \cong D_4$. *Se* $\mid G_{R_F} \mid = 3$, *logo* $G_F \cong A_4$.
Se $t = \frac{x^4+1}{x^3}$ ou $\frac{x^4+1}{x}$	Temos que $q \equiv 1 \mod 3$ se, e somente se, $G_F \cong A_4$ (vide Exemplo 2.37)

Observe que do Exemplo 2.38, não existe t tal que $G_F \cong C_4$.

Exemplo 2.26. Seja $p \neq 2$. Para cada polinômio $f(x) \in M_s$ onde $M_s := \{f(x) \in \mathbb{F}_q[x] | f(x) = x^4 + bx^2 + d\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$, então o conjunto M_s é particionado da seguinte forma:

(i) Se $q \equiv 3 \mod 4$, então existem q^2 elementos da forma $f(x) = x^4 + bx^2 + d$ tais que $G_F \cong D_4$.

(ii) Se $q \equiv 1 \mod 4$, então existem $q^2 - q$ elementos da forma $f(x) = x^4 + bx^2 + d$, $b \neq 0$ tais que $G_F \cong D_4$ e outros q da forma $f(x) = x^4 + d$ para os quais $G_F \cong C_4$.

Observe que para $p = 2$, temos que $f(x)$ não é separável.

Exemplo 2.27. Seja p um primo. Para cada polinômio $f(x) \in M_s$ onde $M_s := \{f(x) \in \mathbb{F}_q[x] | f(x) = x^4 + ax^3 + d\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$, então o conjunto M_s é particionado da seguinte forma:

a) $p \neq 2$.

(i) Se $q \equiv 3 \mod 4$, então existem q^2 elementos da forma $f(x) = x^4 + ax^3 + d$ tais que $G_F \cong D_4$.

(ii) Se $q \equiv 1 \mod 4$, então existem q^2 elementos da forma $f(x) = x^4 + ax^3 + d$ tais que $G_F \cong C_4$.

b) $p = 2$ e $a \neq 0$.

(i) Se $q \equiv 2 \mod 3$, então existem $q(q-1)$ elementos da forma $f(x) = x^4 + ax^3 + d$ tais que $G_F \cong S_4$.

(ii) Se $q \equiv 1 \mod 3$, então existem $q(q-1)$ elementos da forma $f(x) = x^4 + ax^3 + d$ tais que $G_F \cong A_4$.

Exemplo 2.28. Dado k um corpo com $car(k) \neq 2$ e $f(x) = x^4 + ax^3 + bx^2 + d \in k[x]$. Para $k = \mathbb{R}$ temos que $G_F \cong D_4$. Se $k = \mathbb{C}$ e $b = 0$, temos que $G_F \cong C_4$. De fato considerando $a = d = 0$, temos que

$$F(T) = T^4 + bT^2 - y$$

ao qual associamos sua cúbica resolvente da forma $R_F(T) = T(T^2 - 2bT + b^2 + 4y)$. Pelo Teorema 2.9 temos que $G_F \cong C_4$ se $= y(b^2 + 4y)$ é um quadrado. Isto ultimo acontece, se $b = 0$ e $k = \mathbb{C}$.

Observação 2.29. Dados $f(x) = x^4 + ax^3 + bx^2 + d \in k[x]$ e um primo $p \neq 2$, temos seguinte comparação dos subgrupos de Galois G_F associados

	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{F}_q$, com $q = p^e$
$b = 0$	D_4	C_4	C_4 se, e somente se, $q \equiv 1 \mod 4$
$b \neq 0$	D_4	D_4	D_4

Exemplo 2.30. Seja $q = 2$. Para cada polinômio $f(x) \in M_s$ onde $M_s := \{f(x) \in \mathbb{F}_q[x] | f(x) = x^4 + ax^3 + bx^2 + cx + d$, com $a \neq 0$ ou $c \neq 0\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$, então o conjunto M_s é particionado da seguinte forma:

(i) Não existem elementos $f(x) \in M_s$ tais que $G_F \cong V$.

(ii) Os polinômios $x^4 + x + d$ tais que $G_F \cong D_4$.

(iii) Os polinômios $x^4 + x^2 + x + d$ tais que $G_F \cong A_4$, e outros 8 da forma $x^4 + x^3 + bx^2 + cx + d$ tais elementos para os quais $G_F \cong S_4$.

Observe que $Aut(\mathbb{F}_2(x)/\mathbb{F}_2) \cong S_3$, o qual não contem cada um dos G_F descritos acima.

Exemplo 2.31. Seja $q = 3$. Para cada $f(x) \in M := \{f(x) \in k[x] |$ f (x) é mônico de grau 4$\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$. Então o conjunto M é particionado da seguinte forma :

(i) Existem 54 elementos da forma $f(x) = x^4 + ax^3 + bx^2 + cx + d$, com $c \neq 0$, tais que $G_F \cong S_4$.

(ii) Existem 27 elementos da forma $f(x) = x^4 + ax^3 + bx^2 + d$ tais que $G_F \cong D_4$.

Exemplo 2.32. Seja $q = 4$. Para cada polinômio $f(x) \in M_s$ onde $M_s := \{f(x) \in \mathbb{F}_q[x] | f(x) = x^4 + ax^3 + bx^2 + cx + d$, com $a \neq 0$ ou $c \neq 0\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$, então o conjunto M_s é particionado da seguinte forma:

(i) Existem 4 elementos $f(x) \in M_s$ tais que $G_F \cong V$, os quais são: $x^4 + x, x^4 + x + 1, x^4 + x + \alpha$, $x^4 + x + \alpha + 1$, com $\alpha^2 + \alpha + 1 = 0$ e $\alpha \in \mathbb{F}_4$ não nulo.

(ii) Existem 24 elementos $f(x) \in M_s$ tais que $G_F \cong D_4$.

(iv) Existem 68 elementos $f(x) \in M_s$ tais que $G_F \cong A_4$ e outros 144 tais elementos para os quais $G_F \cong S_4$.

Se $G_F \cong S_4$ ou D_4, temos que esse grupos não estão em $Aut(\mathbb{F}_4(x)/\mathbb{F}_4) \cong A_5$.

Exemplo 2.33. Seja $q = 5$. Para cada polinômio $f(x) \in M_s$ onde $M_s := \{f(x) \in \mathbb{F}_q[x] | f(x) = x^4 + ax^3 + bx^2 + cx + d$, com $a \neq 0$ ou $c \neq 0\}$, seja G_F o grupo de Galois do fecho galoisiano de $\mathbb{F}_q(x)/\mathbb{F}_q(f(x))$, então o conjunto M_s é particionado da seguinte forma:

(i) Existem 500 elementos $x^4 + ax^3 + bx^2 + cx + d, c \neq 0$ tais que $G_F \cong S_4$.

(ii) 100 elementos $x^4 + ax^3 + bx^2 + d$ tais que $G_F \cong D_4$ e outros 25 da forma $x^4 + ax^3 + d$ tais elementos para os quais $G_F \cong C_4$.

Observação 2.34. Dado $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{F}_q[x]$ e o grupo $Aut(\mathbb{F}_q(x)/\mathbb{F}_q)$, temos as seguentes relações:

(i) Se $q = 2$, então $G_F \nsubseteq Aut(\mathbb{F}_2(x)/\mathbb{F}_2)$.

(ii) Se $q = 3$ ou 5, para $H = A_4$ ou V que estão em $Aut(\mathbb{F}_q(x)/\mathbb{F}_q)$, temos que não existe $t = f(x)$ com $G_F \cong H$.

(iii) Se $q = 4$, para $H = C_4$ ou D_4, temos que eles não estão em $Aut(\mathbb{F}_4(x)/\mathbb{F}_4)$, mas existe $t = f(x)$ com $G_F \cong H$.

Exemplo 2.35. Dados $t = \frac{x^4+1}{x}$. Temos que $\mathbb{F}_3(x)/\mathbb{F}_3(t)$ é de Galois, com grupo $G_F \cong A_4$. Neste caso temos o polinômio

$$F(T) = T^4 - tT + 1 \in \mathbb{F}_q(t)[T],$$

e sua cubica resolvente irredutível de $F(T)$ é $R_F(T) = T^3 - 4T + t^2$, pois a homogenização de $R_F(T)$ é $R_F(X,t,Z) = X^3 - 4XZ^2t^2Z$ la qual tem a suas derivadas:

$$\frac{\partial R_F}{\partial X} = 3X^2 - 4Z^2 = -4Z^2,\ \frac{\partial R_F}{\partial t} = 2tZ,\ \frac{\partial R_F}{\partial Z} = -8XZ + t^2$$

logo temos que $R_F(X,t,Z)$ é não singular em $\mathbb{F}_3[X,t,Z]$ (vide Proposição 1.26). Temos que $R_F(T)$ tem a sua vez associado sua quadrática resolvente $p(T) = T^2 + t^2T - 4^3 + t^4$. O discriminante deste ultimo é $\Delta_P = 4^4$. Assim $G_F \cong A_4$.
Se $p = 2$, então temos

$$\frac{\partial R_F}{\partial X} = 3X^2,\ \frac{\partial R_F}{\partial t} = 0,\ \frac{\partial R_F}{\partial X} = t^2 \neq 0.$$

a quadrática resolvente da forma

$$p(T) = T^2 + t^2T + t^4.$$

Assim, $P(T)$ se fatora se $q \equiv 1 mod 3$. Logo dados $t = \frac{x^4+1}{x}$ e $p = 2$.

(i) Temos que para $q \equiv 1 \mod 3$, a extensão de Galois $\mathbb{F}_q(x)/\mathbb{F}_q(t)$, com grupo $G_F \cong A_4$.

(ii) Temos que para $q \equiv 2 \mod 3$, a extensão de Galois $\mathbb{F}_q(x)/\mathbb{F}_q(t)$, com grupo $G_F \cong S_4$.

Exemplo 2.36. Dados $t = \frac{x^4+1}{x^2}$ e $q = 3$ ou 5. Temos que $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ é uma extensão de grau 4 com grupo de Galois $G_F \cong V$.
Usando os automorfismos

$$\begin{array}{ccc} \mathbb{F}_q(x) & \to & \mathbb{F}_q(x) \\ x & \mapsto & x \\ x & \mapsto & -x \\ x & \mapsto & 1/x \\ x & \mapsto & -1/x \end{array}$$

geramos o polinômio

$$F(T) = T^4 - ((x^4+1)/x^2)T^2 + 1,$$

o qual tem a sua cúbica resolvente da forma $R_F(T) = T(T^2 + 2(\frac{x^4+1}{x^2})T + ((\frac{x^4+1}{x^2})^2 - 4)$ que tem seu discriminante $\Delta_{R_F} = 16$. Se $q = 3$ ou 5, então Δ_{R_F} é um quadrado. Assim $G_F \cong V$.

Exemplo 2.37. Dados $t = \frac{x^4+1}{x^3}$. Temos que $\mathbb{F}_3(x)/\mathbb{F}_3(t)$ é de Galois, com grupo $G_F \cong A_4$. Neste caso temos o polinômio

$$F(T) = T^4 - tT^3 + 1 \in \mathbb{F}_q(t)[T],$$

e sua cubica resolvente irredutível de $F(T)$ é $R_F(T) = T^3 - 4T + t^2$, que a sua vez tem associado sua quadrática resolvente $p(T) = T^2 + t^2T - 4^3 + t^4$. O discriminante deste ultimo é $\Delta_P = 4^4$. Assim $G_F \cong A_4$. Dado $p = 2$, temos que $q \equiv 1 \mod 3$ se, e somente se, $G_F \cong A_4$.

Exemplo 2.38. Pelo Teorema (KORCHMáROS, 208, Pag. 643), temos que o grupo cíclico C_n com $n \mid (2^e \pm 1)$ é um subgrupo de $Aut(\mathbb{F}_{2^e}(x)/\mathbb{F}_{2^e})$. Em particular, temos que $C_4 \nsubseteq Aut(\mathbb{F}_{2^e}(x)/\mathbb{F}_{2^e})$. Logo não existe t tal que $G_F \cong C_4$.

APÊNDICE

A

SUBGRUPOS DO S_4

Lembremos que $H \leq S_n$ é subgrupo transitivo de S_n, se existe $\sigma \in S_n$ tal que $\sigma(i) = j$, para todo i, j distintos. Nosso interesse é listar cada um dos subgrupos do S_4. Uma importante ferramenta que associamos a f, é o polinômio R_f de grau 3, que é gerado com os elementos fixos pelo subgrupo V, veja as equações (2.1) e (2.2).

(i) O grupo simétrico de quatro elementos S_4.

(ii) O único subgrupo de 12 elementos A_4.

(iii) Os três subgrupos isomorfos a D_4, que são $\langle(1234),(13)\rangle$ $\langle(1243),(14)\rangle$ $\langle(1324),(12)\rangle$.

(iv) Os subgrupos de ordem 6, que são $\langle(123),(12)\rangle$ $\langle(124),(12)\rangle$ $\langle(134),(13)\rangle$ $\langle(234),(23)\rangle$.

(v) Os subgrupos de ordem 4, que são $\langle(1234)\rangle$ $\langle(1243)\rangle$ $\langle(1324)\rangle$ (cíclicos), $\langle(13),(24)\rangle$ $\langle(14),(23)\rangle$ $\langle(12),(34)\rangle$, $V = \langle(12)(34),(13)(24)\rangle$.

(vi) Os grupos cíclicos de ordem 3, que são $\langle(123)\rangle$ $\langle(124)\rangle$ $\langle(134)\rangle$ $\langle(234)\rangle$.

(vii) Todas as transposições $\langle(13)(24)\rangle$ $\langle(14)(23)\rangle$ $\langle(12)(34)\rangle$, $\langle(12)\rangle$ $\langle(13)\rangle$ $\langle(23)\rangle$ $\langle(14)\rangle$ $\langle(24)\rangle$ $\langle(34)\rangle$.

(viii) O subgrupo trivial.

Exemplo A.1. O subgrupo $S_3 \cong D_3$ é transitivo em S_3 pois para $i \neq j$ existe $\sigma \in G$ tal que $(i) = j$. $A_3 = \{id,(123),(132)\}$ também é transitivo em S_3, pois para cada elemento 1,2,ou 3 há permutação que associa a todos eles. O subgrupo trivial não é transitivo pois por exemplo não existe σ, tal que $\sigma(1) = 2$. O subgrupo $\{id,(12)\}$ não é transitivo em S_3, pois (por exemplo) não existe σ tal que $\sigma(2) = 3$.

Exemplo A.2. Os subgrupos S_3, A_3, são não transitivos en S_4, e aqueles da forma $\langle(12),(34)\rangle$, $\langle(12)(34)\rangle$ e análogos também são não transitivos em S_4. Logo os subgrupos transitivos de S_4 são S_4, A_4, C_4, D_4 e $V = \{e,(12)(34),(13)(24),(14)(23)\}$.

Observação A.3. Claramente o grupo klein-4 apresentado acima V é subgrupo de A_4.

REFERÊNCIAS

ARTIN, E. **Galois Teory**. [S.l.]: Notre Dame Mathematical Lectures Number 2, 1971. Citado 2 vezes nas páginas 29 e 30.

DUMMIT, D. S. **Abstract Algebra**. [S.l.]: John Wiley and Sons, 1994. Citado 10 vezes nas páginas 11, 13, 20, 22, 26, 27, 28, 29, 33 e 36.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. [S.l.]: Projeto Euclides, 2001. Citado na página 19.

KAPLANSKY, I. **Fields and Rings**. [S.l.]: Lectures in Mathematics Series, 1972. Citado 2 vezes nas páginas 17 e 34.

KAPPE, L.-C.; WARREN, B. **An Elementary Test for the Galois Group of a Quartic Polynomial**. Mathematical Association of America, 1989. Disponível em: <https://www.jstor.org/stable/pdf/2323198.pdf>. Citado 2 vezes nas páginas 34 e 35.

KORCHMáROS, P. H. G. **Algebraic Curves over a Finite Field**. [S.l.]: PRINCETON SERIES IN APPLIED MATHEMATICS, 208. Citado na página 48.

ROTMAN, J. J. **The theory of Groups**. [S.l.]: Allyn and Bacon, Inc, 1965. Citado na página 21.

VAINSENCHER, I. **Introdução a curvas algebricas planas**. [S.l.]: IMPA, 1979. Citado na página 25.

VALENTINI, R. C. Galois closures of quartic subfields of rational function fields. Elsevier, 2013. Citado na página 31.

-