Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Calculando Grupos de Galois sobre os Racionais

por

Carlos Alberto Marques dos Santos

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Fevereiro/1999

João Pessoa - Pb

Calculando Grupos de Galois sobre os Racionais

por

Carlos Alberto Marques dos Santos

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva

Prof. Dr. José Carmelo Interlando

Prof. Dr. Hélio Pires de Almeida

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática
Fevereiro/1999

Agradecimentos

- Ao Prof. Dr. Antônio de Andrade e Silva, que durante todo o desenrolar deste trabalho, contribuiu com sua orientação abalizada e dedicação exemplar para o sucesso do mesmo.

- Ao Prof. Dr. Aldo Bezerra Maciel, pelo incentivo ao prosseguimento das minhas atividades acadêmicas.

- A meu pai, Alberto, e a minha mãe, Francisca, razão maior da minha existência.

Dedicatória

Aos meus pais

Alberto e Francisca.

Sumário

Introdução

A teoria de Galois dá uma resposta elegante à questão de saber se uma equação polinomial

$$f(x) = 0$$

sobre um corpo adequado K(por exemplo, os racionais) é ou não solúvel por radicais. "Solúvel por radicais" significa que os zeros de $f(x)$ podem ser escritos como expressões finitas envolvendo os coeficientes de $f(x)$, onde as únicas operações permitidas são as operações do corpo e a extração de raízes. Na teoria de Galois, a cada polinômio $f(x) \in K[x]$, está associado um grupo G chamado o **grupo de Galois de** $f(x)$ **sobre** K. A estrutura deste grupo descreve a estrutura da menor extensão de K contendo todos os zeros de $f(x)$ e a equação $f(x) = 0$ é solúvel por radicais se, e somente se, G é um grupo solúvel.

Nesta dissertação estudaremos o problema do cálculo do grupo de Galois de um polinômio $f(x)$, com zeros distintos sobre um corpo K. Estaremos especialmente interessados no caso $K = \mathbb{Q}$, o corpo dos números racionais, e quando $f(x)$ é irredutível sobre K. Esta dissertação tem por objetivo ser uma contribuição ao domínio da computação simbólica e algébrica.

No Capítulo 2, apresentaremos algumas definições e resultados básicos que serão necessários para o entendimento dos capítulos subsequentes.

No Capítulo 3, discutiremos métodos computacionais usados para determinar invariantes de "$Gal(f/K)$", incluindo trabalho feito previamente. Discutiremos em detalhes o uso de "polinômios resolventes" e mostraremos como a "resolvente linear" pode ser usada na determinação de "$Gal(f/K)$".

No Capítulo 4, descreveremos um algoritmo prático e exato que usa "resultantes polinomiais" para calcular "resolventes lineares".Nosso algoritmo necessitará de algumas restrições sobre o corpo base K quando sua "característica" for não nula.

No Capítulo 5, implementaremos o algoritmo do Capítulo 4 sobre $K = \mathbb{Z}_p$, onde p é um número primo suficientemente grande, como um algoritmo modular que calcula "resolventes lineares" sobre $\mathbb{Z}$ para polinômios mônicos $f(x) \in \mathbb{Z}[x]$. Também no Capítulo 5, incluiremos exemplos que ilustram os métodos descritos nesta dissertação.

No Capítulo 6, são apresentadas algumas sugestões visando o prolongamento deste trabalho.

Capítulo 1

Conceitos Básicos

Neste capítulo estudaremos algumas definições e resultados básicos que serão necessários no decorrer dos capítulos subsequentes. O leitor interessado em mais detalhes deve consultar [5, 6, 8, 9, 11].

1.1 Grupos

Seja G um conjunto não-vazio munido de uma operação binária (denominada *produto*)

$$\begin{aligned} \bullet \ : \ G \times G &\rightarrow G \\ (a,b) &\mapsto a \bullet b. \end{aligned}$$

Dizemos que $(G, \bullet)$ é um *grupo* se $\bullet$ satisfaz:

(i) $a \bullet (b \bullet c) = (a \bullet b) \bullet c, \forall a, b, c \in G$ (associatividade);

(ii) $\exists e \in G$ tal que $a \bullet e = e \bullet a = a, \forall a \in G$ (elemento identidade);

(iii) Dado $a \in G, \exists a^{-1} \in G$ tal que $a \bullet a^{-1} = a^{-1} \bullet a = e$ (elemento inverso).

Se, além disso, $\bullet$ satisfaz:

(iv) $a \bullet b = b \bullet a, \forall a, b \in G$ (comutatividade)

dizemos que $(G, \bullet)$ é um *grupo abeliano* ou *comutativo*. Sejam $n \in \mathbb{N}, n \geq 2$ e $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ o conjunto das classes de equivalências obtidas da relação $\bmod n$. Então $(\mathbb{Z}_n, \oplus)$ é um grupo abeliano, onde $\oplus$ é definida por

$$\begin{aligned} \oplus \ : \ \mathbb{Z}_n \times \mathbb{Z}_n &\rightarrow \mathbb{Z}_n \\ (\overline{a}, \overline{b}) &\mapsto \overline{a+b}. \end{aligned}$$

$(\mathbb{Z}_n, \oplus)$ é chamado de *grupo aditivo dos inteiros modulo n.* Sejam $C = \{1, 2, ..., n\}$ e

$$S_n = \{f : C \to C; f \text{ é bijeção}\}.$$

Então $(S_n, \circ)$, onde $\circ$ denota a composição de funções, é um grupo finito, o qual é não abeliano para $n \geq 3$, chamado de *grupo das permutações* de n símbolos. Um elemento $\sigma \in S_n$ tal que

$$\sigma(1) = a_1, \sigma(2) = a_2, \ldots, \sigma(n) = a_n$$

será denotado por

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

Sejam $(G_1, \square)$, $(G_2, \triangle)$ grupos e $G = G_1 \times G_2$. Então $(G, \bullet)$ é um grupo, onde $\bullet$ é definida por

$$\begin{array}{rccc} \bullet & : & G \times G & \to & G \\ & & ((a,b),(c,d)) & \mapsto & (a \square c, b \triangle d). \end{array}$$

G é chamado de *produto direto de G_1 por G_2*. Tem-se que G é abeliano se, e somente se, G_1 e G_2 são abelianos. De modo análogo, define-se o produto direto de n grupos

$$(G_1, \underset{1}{\bullet}), (G_2, \underset{2}{\bullet}), \ldots, (G_n, \underset{n}{\bullet}).$$

A *ordem* de um grupo finito G é o número de elementos em G e denotada por $|G|$. Assim,

$$|S_n| = n!, |G_1 \times G_2| = |G_1|\,|G_2| \text{ e } |\mathbb{Z}_n| = n.$$

Se G é infinito, dizemos que a ordem de G é infinita e escrevemos $|G| = \infty$. Sejam $(G, \bullet)$ um grupo e H um subconjunto não-vazio de G. Dizemos que H é um *subgrupo* de G, denotado por $H \leq G$, quando $(H, \bullet)$ é um grupo. Claramente, $\{e\}$ e o próprio G são subgrupos de G, chamados de *subgrupos triviais de G.* Se $H_1, H_2, \ldots, H_n \leq G$, então $\bigcap_{i=1}^{n} H_i \leq G$. O conjunto de todos os subgrupos de G será denotado por $Sub(G)$. Se $H \in Sub(G)$ é tal que $H \neq G$ e $\forall K \in Sub(G)$ com $H \subsetneq K$, tem-se $K = G$, então H é denominado *subgrupo maximal* de G. Objetivando simplificar as notações, de agora em diante quando afirmarmos que G é um grupo, ficará implícita a operação $\bullet$ e dados $x, y \in G$, seu produto $x \bullet y$ será denotado por xy. Às vezes, operações distintas de grupos distintos serão denotadas da mesma maneira.

Proposição 1.1 *Sejam G um grupo e H um subconjunto não-vazio de G. Então $H \leq G$ se, e somente se, as seguintes condições são satisfeitas:*

1. $\forall x, y \in H$, *tem-se* $xy \in H$;

2. $\forall x \in H$, *tem-se* $x^{-1} \in H$. ■

Sejam G um grupo qualquer e

$$Z(G) = \{x \in G : xg = gx, \forall g \in G\}.$$

Tem-se que $Z(G) \leq G$ e, além disso, $Z(G)$ é abeliano. $Z(G)$ é chamado o *centro* de G. Se $x \in G$, o *centralizador* de x em G, denotado por $C_G(x)$, é o conjunto

$$C_G(x) = \{g \in G : g^{-1}xg = x\}.$$

Verifica-se que $C_G(x) \leq G$ e, além disso, G é abeliano se, e somente se, $C_G(x) = G, \forall x \in G$. Sejam G um grupo, $x \in G$ e $n \in \mathbb{Z}$. Define-se $x^n \in G$ da seguinte maneira:

$$x^n = \begin{cases} x^{n-1}x, & \text{se } n > 0 \\ e, & \text{se } n = 0 \\ (x^{-1})^{-n}, & \text{se } n < 0. \end{cases}$$

Sejam G um grupo e $x \in G$. Se existir $n \in \mathbb{Z}$ tal que $x^n = e$, definimos a *ordem* de x, em símbolos $o(x)$, como sendo

$$o(x) = \min\{n \in \mathbb{Z}_+ : x^n = e\}.$$

Caso contrário, dizemos que $o(x) = \infty$. Sejam G um grupo, S um subconjunto não-vazio de G e

$$\langle S \rangle = \{a_1 a_2 \cdots a_n : a_i \in S \text{ ou } a_i^{-1} \in S\}.$$

Tem-se que $\langle S \rangle \leq G$. $\langle S \rangle$ é chamado de *subgrupo gerado por* S. No caso em que $S = \{a\}$, então

$$\langle S \rangle = \langle a \rangle = \{\ldots, (a^{-1})^2, a^{-1}, e, a, a^2, \ldots\} = \{a^t : t \in \mathbb{Z}\}$$

é chamado de *grupo cíclico* gerado por a. É fácil ver que todo grupo cíclico é abeliano e que $o(x) = |\langle x \rangle|, \forall x \in G$. Sejam G grupo, $H \leq G$ e $x \in G$. Então $H^x \leq G$, onde

$$H^x = xHx^{-1} = \{xhx^{-1}; h \in H\}.$$

Se $H, K \leq G$, dizemos que H e K são *conjugados em* G se existir $x \in G$ tal que $H^x = K$. Verifica-se que conjugação é uma relação de equivalência em $Sub(G)$. Sejam G grupo, $H \leq G$ e $x \in G$. Definimos a *classe lateral à esquerda de* H *em* G *contendo* x como sendo o conjunto

$$xH = \{xh; h \in H\}.$$

Proposição 1.2 *Sejam G grupo finito e $H \leq G$. Valem as seguintes afirmações:*

1. $xH = yH \iff y \in Hx, \forall x, y \in G$;
2. $|xH| = |H|, \forall x \in G$;
3. $G = x_1 H \dot{\cup} x_2 H \dot{\cup} \cdots \dot{\cup} x_n H$. ■

O conjunto das classes laterais à esquerda de H em G será denotado por $\frac{G}{H}$. $\left|\frac{G}{H}\right| = (G : H)$ é chamado *índice de H em G*.

Teorema 1.1 (Lagrange) *Sejam G um grupo finito e $H \leq G$. Então*

$$|G| = (G : H)\,|H|\,.$$

■

Corolário 1.1 *Seja G um grupo finito. Vale o seguinte:*

1. *Se $|G| = n$, então $x^n = e, \forall x \in G$;*
2. *Se $|G| = p$, onde p é primo, então G é cíclico.* ■

Corolário 1.2 (Pequeno Teorema de Fermat) *Se $p \in \mathbb{N}$ é um número primo, então*

$$a^{p-1} \equiv 1 \bmod p, \forall a \in \mathbb{Z} - p\mathbb{Z}.$$

■

Sejam G um grupo e $H \leq G$. Dizemos que H é *normal* em G, em símbolos $H \trianglelefteq G$, se

$$H^g \subseteq H, \forall g \in G.$$

Claramente os subgrupos triviais de G são normais em G. Uma verificação simples mostra que $Z(G) \trianglelefteq G$. Se G é abeliano, então $H \trianglelefteq G, \forall H \in Sub(G)$. Um grupo é dito *simples* se seus únicos subgrupos normais são os triviais.

Proposição 1.3 *Seja G um grupo. As seguintes afirmações são verdadeiras*:

1. $N \trianglelefteq G \Leftrightarrow N^g = N, \forall g \in G$;
2. $N_1, N_2 \trianglelefteq G \Rightarrow N_1 \cap N_2 \trianglelefteq G$;

3. $H \leq G, N \trianglelefteq G \Rightarrow HN = \{hn; h \in H, n \in N\} \leq G$;

4. $N_1, N_2 \trianglelefteq G \Rightarrow N_1N_2 \trianglelefteq G$;

5. $H \leq G, N \trianglelefteq G \Rightarrow H \cap N \trianglelefteq H$. ■

Proposição 1.4 *Sejam G um grupo e $H \trianglelefteq G$. Então $(\frac{G}{H}, \odot)$ é um grupo, onde $\odot$ é definida por*

$$\begin{array}{rccc} \odot & : & \frac{G}{H} \times \frac{G}{H} & \rightarrow & \frac{G}{H} \\ & & (xH, yH) & \mapsto & xyH. \end{array}$$

$\frac{G}{H}$ é chamado grupo quociente de G por H. ■

Seja G um grupo. Definamos em G a seguinte relação:

$$x, y \in G, x \underset{G}{\tilde{}} y \Leftrightarrow \exists g \in G \text{ tal que } y = g^{-1}xg.$$

Prova-se que $\underset{G}{\tilde{}}$ é uma relação de equivalência em G. Se $x \underset{G}{\sim} y$, dizemos que x e y são *conjugados em G*. Dado $x \in G$, a classe de equivalência de x em G determinada por $\underset{G}{\sim}$ é

$$C_x = \{g^{-1}xg; g \in G\}$$

e é chamada de *classe de conjugação de x em G*;

Proposição 1.5 *Seja G um grupo finito. Então*:

1. $|C_x| \,|$*divide* $|G|$ *e* $C_x = \{x\} \Leftrightarrow x \in Z(G)$;

2. $|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|$ (*Equação das Classes*). ■

Um *homomorfismo* entre dois grupos G, G' é uma função $f : G \longrightarrow G'$ que é compatível com suas operações, isto é,

$$f(xy) = f(x)f(y), \forall x, y \in G.$$

No caso em que $G = G'$, dizemos que f é um *endomorfismo.* Se $f : G \longrightarrow G'$ é um homomorfismo bijetor, chamamos f de *isomorfismo* e dizemos que G e G' são *isomorfos* (notação:$G \cong G'$). No caso em que $G = G'$, dizemos que f é um *automorfismo.* O conjunto dos automorfismos de um grupo G será denotado por $Aut(G)$. Dado $g \in G$, a função $\Psi_g : G \longrightarrow G$ definida por $\Psi_g(x) = g^{-1}xg$ é um automorfismo. Ψ_g é chamado de *automorfismo interno de G*. Notação: $Inn(G)$ representará o conjunto de todos os automorfismos internos de um grupo G.

Proposição 1.6 *Seja G um grupo. Então $(Aut(G), \circ)$ é um grupo e, além disso, $Inn(G) \trianglelefteq Aut(G)$.* ■

Proposição 1.7 *Sejam G, G' grupos com identidades e, e', respectivamente e $\varphi : G \longrightarrow G'$ um homomorfismo. Vale o seguinte:*

1. $\mathrm{Im}(\varphi) = \varphi(G) = \{\varphi(g); g \in G\} \leq G'$;
2. $Ker(\varphi) = \{g \in G; \varphi(g) = e'\} \trianglelefteq G$ *($Ker(\varphi)$ é denominado* núcleo *do homomorfismo φ) e mais, φ é injetor se, e somente se, $Ker(\ \varphi) = \{e\}$.* ■

Teorema 1.2 (dos Homomorfismos) *Sejam G, G' grupos e $\varphi : G \longrightarrow G'$ um homomorfismo. Então*

$$\frac{G}{Ker(\varphi)} \cong \mathrm{Im}(\varphi).$$

■

Corolário 1.3 *Seja G um grupo qualquer.*

1. *Se G é um grupo cíclico, então $G \cong (\mathbb{Z}, +)$ se $|G| = \infty$ e $G \cong \mathbb{Z}_n$, se $|G| = n$;*
2. *$Inn(G) \cong \frac{G}{Z(G)}$;*
3. *Se $X = \{x_1, x_2, \ldots, x_n\}$, então $(\mathcal{P}(X), \circ) \cong S_n$, onde $\mathcal{P}(X)$ denota o conjunto das permutações dos elementos de X.* ■

Proposição 1.8 *Sejam m, n, s inteiros positivos tais que $s^m \equiv 1 \bmod(n)$. Então existe, a menos de isomorfismos, um único grupo G, com $|G| = nm$, gerado por dois elementos $a, b \in G$ satisfazendo às seguintes relações:*

$$\begin{cases} a^n = e \\ b^m = e \\ a = b^{-1}a^s b. \end{cases}$$

Neste caso, $G = \{a^i b^j; 0 \leq i \leq n-1, 0 \leq j \leq m-1\}$. ■

O grupo G tal que

$$|G| = 2n, n \in \mathbb{N}, G = \langle a, b\rangle, a^n = b^2 = e \text{ e } a = b^{-1}a^s b, n, s \in \mathbb{N}$$

é chamado de *grupo diedral de ordem* $2n$ e denotado por D_{2n}. O grupo G tal que

$$|G| = 2^n, n \in \mathbb{N}, G = \langle a, b \rangle, a^{2^{n-1}} = e, b^2 = a^{2^{n-2}} \text{ e } bab^{-1} = a^{-1}$$

é chamado de *grupo dos quatérnios de ordem* 2^n e denotado por Q_{2^n}. Sejam K, G, H grupos e $\varphi : K \longrightarrow G, \psi : G \longrightarrow H$ homomorfismos. Dizemos que o diagrama

$$K \xrightarrow{\varphi} G \xrightarrow{\psi} H$$

é uma *sequência exata em* G se $\text{Im}(\varphi) = Ker(\psi)$ ou, equivalentemente, $(\psi \circ \varphi)(x) = e_H, \forall x \in K$. Seja $\{\ldots, G_{i-1}, G_i, G_{i+1}, \ldots\}$ uma família, eventualmente infinita, de grupos e $\{\ldots, \varphi_i : G_i \longrightarrow G_{i+1}, \ldots\}$ uma família de homomorfismos. Dizemos que o diagrama

$$\cdots \longrightarrow G_{i-1} \xrightarrow{\varphi_{i-1}} G_i \xrightarrow{\varphi_i} G_{i+1} \xrightarrow{\varphi_{i+1}} \cdots$$

é uma *sequência exata*, se é exata em $G_i, \forall i \in I$, isto é, se $\text{Im}(\varphi_{i-1}) = Ker(\varphi_i), \forall i \in I$. Sejam G grupo e $H \trianglelefteq G$. Dizemos que G se *fatora* sobre H se existir $K \leq G$ tal que $G = HK$ e $H \cap K = \{e\}$. Neste caso, dizemos que K é um *complemento* de H. Sejam H, K dois grupos e

$$\begin{array}{rccc} \sigma : & K & \longrightarrow & Aut(H) \\ & k & \longmapsto & \sigma(k) \end{array}$$

um homomorfismo. O conjunto $G = H \times K$ equipado com a operação

$$(h, k)(h', k') = (h\sigma(k)(h'), kk')$$

é um grupo, onde o elemento neutro é (e_H, e_K) e o elemento inverso de (h, k) é $(\sigma(k^{-1})(h^{-1}), k^{-1})$. Tal grupo será denotado por $H \times_\sigma K$.

Teorema 1.3 *Sejam H, K grupos, $\sigma \in Aut(K)$ e $G = H \times_\sigma K$. As seguintes afirmações são verdadeiras:*

1. *Se σ é o homomorfismo trivial, isto é, se $\sigma(k) = Id_H, \forall k \in K$, então G é o produto direto usual $H \times K$; se σ não é o homomorfismo trivial, então G é não-abeliano, mesmo que H e K sejam abelianos;*

2. *Existem $H' \trianglelefteq G, K' \leq G$ com $H' \cong H, K' \cong K$ tais que G se fatora sobre H', com complemento K';*

3. *Existem* $\varphi : H' \longrightarrow G$ *homomorfismo injetor,* $\psi : G \longrightarrow K'$ *homomorfismo sobrejetor tais que a sequência abaixo é exata:*

$$\{e_{H'}\} \longrightarrow H' \xrightarrow{\varphi} G \xrightarrow{\psi} K' \longrightarrow \{e_{K'}\};$$

■

Em virtude do Teorema acima, o grupo $H \times_\sigma K$ será simplesmente denotado por HK e denominado *produto semi-direto de* H *por* K. Um *grupo de Frobenius* é um grupo finito G contendo um subgrupo normal não-trivial M tal que

$$C_G(x) \leq M, \forall x \in M^* = M - \{e\}.$$

M é chamado de *núcleo de Frobenius de* G. O grupo de Frobenius de ordem n será denotado por F_n.

Teorema 1.4 *Se* G *é um grupo de Frobenius com núcleo de Frobenius* M*, então:*

1. $\text{mdc}(|M|, (G : M)) = 1$;

2. $\exists H \leq G$ *tal que* $\text{mdc}(|H|, (G : H)) = 1$*,* G *fatora-se sobre* M *com complemento* H*,*

$$H \cap H^x = \{e\}, \forall x \in G - H \ \ e \ \ M = \{e\} \cup \{y : y \notin \bigcup_{x \in G} H^x\}.$$

■

Teorema 1.5 *Um grupo de Frobenius possui um único núcleo de Frobenius.* ■

Teorema 1.6 *Sejam* G *grupo finito e* $H \leq G$*. Se* $H \cap H^x = \{e\}, \forall x \in G - H$*, então* G *é um grupo de Frobenius com núcleo de Frobenius* M *tal que*

$$M = \{e\} \cup \{y : y \notin \bigcup_{x \in G} H^x\}.$$

Além disso, G *fatora-se sobre* M *com complemento* H*.* ■

Se $G \leq S_n$, então dizemos que o *grau* de G é n (notação: $\deg(G) = n$). O estudo dos grupos $S_n, n \in \mathbb{N}$, é importante, em virtude do seguinte teorema:

Teorema 1.7 (Cayley) *Se* G *é um grupo finito, com* $|G| = n$*, então* G *é isomorfo a um subgrupo do* S_n*.* ■

Uma permutação $\sigma \in S_n$ é chamada de *ciclo* se existem elementos distintos $i_1, ..., i_r \in \{1, ..., n\}, 1 \leq r \leq n$, tais que $\sigma(i_1) = i_2, \sigma(i_2) = i_3, ..., \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$ e $\sigma(j) = j$, $\forall j \in \{1, \ldots n\} - \{i_1, \ldots, i_r\}$. Tal ciclo será denotado por

$$(i_1, i_2, \ldots, i_r).$$

r é chamado de *comprimento* do ciclo. Os ciclos tais que $r = 2$ são também chamados de *transposições.* Dois ciclos

$$(i_1, i_2, \ldots, i_r), (j_1, j_2, \ldots, j_s) \in S_n$$

são ditos *disjuntos* se

$$\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset.$$

É fácil ver que se $\sigma, \tau \in S_n$ são ciclos disjuntos, então $\sigma\tau = \tau\sigma$.

Proposição 1.9 *Seja $\sigma \in S_n$, $\sigma \neq (1)$. Então σ é igual a um produto de ciclos disjuntos de comprimentos ≥ 2; tal fatoração é única, a menos da ordem.* ■

Seja $D = D(x_1, \ldots, x_n)$ a seguinte função nas variáveis $x_1, \ldots, x_n$, onde

$$x_i x_j = x_j x_i, \forall i, j \in \{1, \ldots, n\},$$

$$D(x_1, \ldots, x_n) = (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n)(x_2 - x_3) \cdots (x_2 - x_n) \cdots (x_{n-1} - x_n)$$

o qual denotaremos por

$$D = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Se $\sigma \in S_n$, denotamos por

$$D^\sigma = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Prova-se que $D^\sigma = (-1)^k D$, onde k é o número de fatores da forma $(x_j - x_i)$. Se $D^\sigma = D$, dizemos que σ é uma *permutação par.* Se $D^\sigma = -D$, dizemos que σ é uma *permutação ímpar.* Seja

$$A_n = \{\sigma \in S_n : D^\sigma = D\}.$$

Então $A_n \trianglelefteq S_n$. A_n é chamado de *grupo das permutaçõaes pares de S_n* ou *grupo alternado de grau n.* Além disso, $|A_n| = \frac{n!}{2}$. Um grupo G diz-se *solúvel* se existem subgrupos

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{n-1} \leq G_n = G$$

tais que

(i) $G_{i-1} \trianglelefteq G_i, \forall i \in \{1, \ldots, n\}$;

(ii) $\frac{G_i}{G_{i-1}}$ é abeliano, $\forall i \in \{1, \ldots, n\}$.

Proposição 1.10 *1. Todo subgrupo de um grupo solúvel é solúvel;*

2. Todo quociente de um grupo solúvel é solúvel;

3. Sejam G um grupo e $N \trianglelefteq G$. Se N e $\frac{G}{N}$ são solúveis, então G é solúvel. ■

Teorema 1.8 *Se $n \geq 5$, então S_n não é solúvel.* ■

Teorema 1.9 (Burnside) *Todo grupo finito cuja ordem é divisível no máximo por dois primos é solúvel.* ■

Teorema 1.10 (W. Feith e J. Thompson) *Todo grupo finito de ordem ímpar é solúvel.* ■

1.2 Anéis

Seja A um conjunto não-vazio, munido de duas operações binárias, denominadas *soma* e *produto* e denotadas, respectivamente por $+$ e $\bullet$. Assim

$$\begin{array}{rcccl} + & : & A \times A & \to & A \\ & & (x,y) & \mapsto & x+y \end{array} \quad \text{e} \quad \begin{array}{rcccl} \bullet & : & A \times A & \to & A \\ & & (x,y) & \mapsto & x \bullet y. \end{array}$$

Dizemos que $(A, +, \bullet)$ é um *anel* se as seguintes condições são satisfeitas:

(i) $(A, +)$ é um grupo abeliano;

(ii) $a \bullet (b \bullet c) = (a \bullet b) \bullet c, \forall a, b, c \in A$ (associatividade);

(iii) $a \bullet (b + c) = a \bullet b + a \bullet c, \forall a, b, c \in A$ (distributividade à esquerda);

(iv) $(a + b) \bullet c = a \bullet c + b \bullet c$, $\forall a, b, c \in A$ (distributividade à direita).

Dado $(A, +, \bullet)$ anel, denotaremos o elemento neutro da soma por 0 e dado $a \in A$, denotaremos por $-a$ seu elemento inverso com respeito à soma. De modo análogo àquele feito para grupos, dados $x, y \in A$, seu produto $x \bullet y$ será denotado simplesmente por xy. Às vezes, para efeito de simplificação, anéis distintos com soma e produto distintos,

serão denotados pelo mesmo símbolo, quando não houver perigo de confusão. Também ($A, +, \bullet$) será denotado simplesmente por A. Se um anel A satisfaz à propriedade:

$$\exists 1 \in A \text{ tal que } x1 = 1x = x, \forall x \in A,$$

dizemos que A é um *anel com unidade.* Se um anel A satisfaz à propriedade:

$$xy = yx, \forall x, y \in A,$$

dizemos que A é um *anel comutativo.* Se um anel A satisfaz à propriedade:

$$\forall x, y \in A \text{ tais que } xy = 0 \Rightarrow x = 0 \text{ ou } y = 0,$$

dizemos que A é um *anel sem divisores de zero.* Caso contrário, dizemos que A é um *anel com divisores de zero.* Um anel comutativo, com unidade e sem divisores de zero é chamado de *domínio de integridade* ou simplesmente *domínio.* Seja D um domínio. Um elemento $x \in D, x \neq 0$ é dito *invertível* (em D) se $\exists y \in D$ tal que $xy = yx = 1$. O elemento y é chamado de *inverso* de x. O conjunto dos elementos invertíveis de D será denotado por $U(D)$ e dado $x \in D, x \neq 0$, seu inverso será denotado por x^{-1}. Se $x, y \in D$, com $y \in U(D)$, então xy^{-1} será denotado por $\frac{x}{y}$. Um anel com unidade, onde todo elemento não-nulo possui inverso é denominado *anel de divisão.* Um *corpo* K é um domínio no qual todo elemento não-nulo é invertível, isto é,

$$\forall a \in K^*, \exists b \in K \text{ tal que } ab = ba = 1.$$

Isto é equivalente a dizer que $(K, +)$, $(K^*, \bullet)$ são grupos abelianos e vale a distributividade à esquerda e à direita. $(\mathbb{Z}_n, \oplus, \odot), n \in \mathbb{N}, n$ composto, é um anel finito, com divisores de zero, onde

$$\begin{array}{rccc} \oplus & : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & & (\overline{x}, \overline{y}) & \mapsto & \overline{x+y} \end{array} \quad \text{e} \quad \begin{array}{rccc} \odot & : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & & (\overline{x}, \overline{y}) & \mapsto & \overline{xy} \end{array}.$$

Já $(\mathbb{Z}_p, \oplus, \odot), p \in \mathbb{N}, p$ primo, é um corpo finito. $(\mathbb{Z}, +, \bullet)$ é um domínio infinito e mostra-se que todo domínio finito é corpo. Temos que $(\mathbb{Q}, +, \bullet)$, $(\mathbb{R}, +, \bullet)$ e $(\mathbb{C}, +, \odot)$ são corpos infinitos, onde

$$\begin{array}{rccc} \odot & : & \mathbb{C} \times \mathbb{C} & \to & \mathbb{C} \\ & & (a+bi, c+di) & \mapsto & (ac-bd)+(ad+bc)i. \end{array}$$

Sejam K corpo e K_1 um subconjunto não-vazio de K. Dizemos que K_1 é um *subcorpo* de K se $(K_1, +) \leq (K, +)$ e $(K_1^*, \bullet) \leq (K^*, \bullet)$. É fácil ver que se K_1, $K_2, \ldots, K_n$ são subcorpos

de K, então $K_1 \cap K_2 \cap \cdots \cap K_n$ também o é. Além disso, se S é um subconjunto não-vazio de K, então o conjunto $\langle S \rangle \subseteq K$ definido por

$$\langle S \rangle = \{x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n : n \in \mathbb{N}, x_i \in K, \alpha_i \in S, i = 1, \ldots, n\}$$

também é um subcorpo de K, chamado de *subcorpo de K gerado por S*. Dizemos que um corpo L é uma *extensão* de um corpo K se L contém K como subcorpo. Notação: L/K significa que L é uma extensão de K. Se L/K é uma extensão, prova-se que L possui uma estrutura de espaço vetorial sobre K. A dimensão de L, visto como um espaço vetorial sobre K é chamada de *grau de L sobre K* e denotada por $(L : K)$. Diz-se que L/K é uma *extensão finita* se $(L : K)$ é finito. O conjunto de todos os subcorpos de L contendo K será denotado por $Lat(L/K)$. Seja L/K uma extensão de corpos e $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. Então o conjunto

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = \{a_0 + a_1\alpha_1 + \cdots + a_n\alpha_n : a_i \in K, i = 0, \ldots, n\}$$

é um subcorpo de L contendo K e $\alpha_1, \alpha_2, \ldots, \alpha_n$. Além disso, é o "menor" subcorpo de L com esta propriedade, isto é, se L' é um subcorpo de L contendo K e $\alpha_1, \alpha_2, \ldots, \alpha_n$, então $K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq L'$. $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é chamado de *subcorpo gerado sobre K por $\alpha_1, \alpha_2, \ldots, \alpha_n$*. Uma extensão L/K é dita *simples* se existe $\alpha \in L$ tal que $L = K(\alpha)$. Se, além disso, $\exists m \in \mathbb{N}$ tal que $\alpha^m \in K$, dizemos que L/K é *pura.* Sejam A e A' anéis. Uma função $f : A \longrightarrow A'$ diz-se um *homomorfismo* se satisfaz às seguintes condições:

(i) $f(a + b) = f(a) + f(b), \forall a, b \in A$;

(ii) $f(ab) = f(a)f(b), \forall a, b \in A$.

Se $A = A'$, f é chamado de *endomorfismo.* O homomorfismo $f : A \longrightarrow A'$ tal que $f(x) = 0', \forall x \in A$, é chamado de *homomorfismo nulo.*

Proposição 1.11 *Sejam A, A' anéis e $f : A \longrightarrow A'$ um homomorfismo. Vale o seguinte*:

1. $f(0) = 0'$;

2. $f(-a) = -f(a), \forall a \in A$;

3. *Se A e A' são domínios e f não é o homomorfismo nulo, então* $f(1) = 1'$;

4. Se A e A' são corpos e f não é o homomorfismo nulo, então f é injetiva. ■

Se A e A' são anéis e f descrita acima é uma bijeção, dizemos que f é um *isomorfismo* de A em A'. Neste caso, dizemos que A e A' são *isomorfos* e escrevemos $A \cong A'$. No caso em que $A = A'$, dizemos que f é um *automorfismo.*

Proposição 1.12 *Seja A um anel e seja $Aut(A)$ o seguinte conjunto:*

$$Aut(A) = \{f : A \longrightarrow A; f \quad \text{é automorfismo}\}.$$

Então $(Aut(A), \circ)$ é um grupo. ■

Teorema 1.11 *Se K é um corpo finito, com $\mid K \mid = q$, então $q = p^n$, com p primo. Reciprocamente, dado $q = p^n$, existe, a menos de isomorfismos, um único corpo finito K tal que $\mid K \mid = q$.* ■

Seja K um corpo e seja $GL_n(K)$ o conjunto das matrizes $n \times n$ invertíveis com entradas em K. Temos que $(GL_n(K), \bullet)$ é um grupo, onde $\bullet$ denota o produto de matrizes. Temos ainda que $SL_n(K) = \{M \in GL_n(K); \det M = 1\} \trianglelefteq GL_n(K)$. No caso em que $\mid K \mid = q < \infty$, as notações para $GL_n(K)$ e $SL_n(K)$ são, respectivamente, $GL(n,q)$ e $SL(n,q)$ (*grupo linear geral* e *grupo linear especial*, respectivamente). Demonstra-se que

$$\mid GL(n,q) \mid = \prod_{0 \leq i \leq n-1} (q^n - q^i) \text{ e } \mid SL(n,q) \mid = \frac{\mid GL(n,q) \mid}{q-1}.$$

Seja K um corpo finito e seja $G = GL(n,q)$. O *grupo linear geral projetivo*, denotado por $PGL(n,q)$, é definido como sendo o grupo quociente $\frac{G}{Z(G)}$. Já o *grupo linear especial projetivo*, denotado por $PSL(n,q)$, é definido como sendo o grupo quociente $\frac{SL(n,q)}{Z(G) \cap SL(n,q)}$. Sejam D um domínio, $x \in D$ e $n \in \mathbb{Z}$. Define-se $nx \in D$ da seguinte maneira:

$$nx = \begin{cases} (n-1)x + x, & \text{se } n > 0 \\ 0, & \text{se } n = 0 \\ -n(-x), & \text{se } n < 0. \end{cases}$$

Prova-se que

$$m(x+y) = mx + my, \forall m \in \mathbb{Z}, \forall x, y \in D$$

e

$$(mn)x = m(nx), \forall m, n \in \mathbb{Z}, \forall x \in D.$$

Um domínio D é dito de *característica zero* (notação: $Char(D) = 0$) se, dados $m \in \mathbb{Z}, x \in D^*$ tais que $mx = 0$, então $m = 0$. Se existe $m \in \mathbb{Z}^*$ tal que $mx = 0$, com $x \in D^*$, dizemos que D é de *característica finita.* Neste caso, definimos $Char(D)$ como sendo

$$Char(D) = \min\{m \in \mathbb{N}; mx = 0, \text{ para algum } x \in D^*\}.$$

Proposição 1.13 *Seja K um corpo. Então as seguintes condições são satisfeitas:*

1. *Se $Char(K) = 0$, então $\mid K \mid = \infty$;*
2. *Se $\mid K \mid = p^n, p \in \mathbb{Z}_+^*, n \in \mathbb{N}^*$, p primo, então $Char(K) = p$ e $px = 0, \forall x \in D$.* ■

Seja A um anel comutativo e com unidade. Um *polinômio f sobre A* é uma sequência

$$f = (a_0, a_1, a_2, \ldots)$$

com $a_i \in A, \forall i \in \mathbb{Z}_+$ e $\exists n \in \mathbb{Z}_+$ tal que $a_{n+k} = 0, \forall k \in \mathbb{N}$. Assim sendo, f pode ser escrito da seguinte maneira:

$$f = (a_0, a_1, a_2, \ldots, a_{n,}\square)$$

onde o símbolo $\square$ significa que $a_{n+k} = 0, \forall k \in \mathbb{N}$. Se $g = (b_0, b_1, b_2, \ldots, b_m, \square)$ é outro polinômio sobre A, dizemos que $f = g$ se $a_i = b_i, \forall i \in \mathbb{Z}_+$. O conjunto dos polinômios sobre A, denotado por $\mathcal{A}$, é um anel, com soma $\oplus$ e produto $\odot$ definidos, respectivamente, por

$$(a_0, a_1, a_2, \ldots, a_n, \square) \oplus (b_0, b_1, b_2, \ldots, b_m, \square) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$

e

$$(a_0, a_1, a_2, \ldots, a_n, \square) \odot (b_0, b_1, b_2, \ldots, b_m, \square) = (\sum_{i+j=0} a_i b_j, \sum_{i+j=1} a_i b_j, \ldots).$$

Agora, identificando $(1, \square)$ com 1,o elemento $a_i \in A$ com $(a_i, \square)$ e $(0, 1, \square)$ com x, é fácil ver que $x^2 = (0, 0, 1, \square)$ e, por indução, que x^i é a sequência $(a_0, a_1, \ldots, a_i, \square)$ tal que $a_i = 1$ e $a_k = 0, \forall k < i, k \in \mathbb{Z}_+$ e que todo polinômio $f = (a_0, a_1, a_2, \ldots, a_n, \square) \in \mathcal{A}$ pode ser escrito da seguinte maneira (denominada *notação formal*):

$$f = f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

onde $a_{n+k} = 0, \forall k \in \mathbb{N}$, convencionando-se $x^0 = 1$ e $x^1 = x$. $(\mathcal{A}, \oplus, \odot)$ será, de agora em diante, denotado por $A[x]$ (*anel dos polinômios em uma "indeterminada" x sobre A*). Se

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in A[x],$$

os elementos $a_0, a_1, a_2, \ldots$ são denominados *coeficientes* de f. Quando $n = 0$ e $a_0 \neq 0$, então $f(x) = a_0$ é chamado de *polinômio constante sobre* A. Quando $n = 0$ e $a_0 = 0$, então $f(x)$ é chamado de *polinômio identicamente nulo sobre* A e denotado por $0(x)$. Assim, $f(x) = 0(x)$ se, e somente se, $a_i = 0, \forall i \in \mathbb{Z}_+$. Se

$$f(x) = \sum_{i=0}^{n} a_i x^i \in A[x],$$

então o *grau* de $f(x)$, denotado por $\partial f(x)$, é definido como sendo

$$\partial f(x) = \max\{r \in \mathbb{Z}_+; a_r \neq 0 \text{ e } a_{r+k} = 0, \forall k \in \mathbb{N}\}.$$

Observemos que $\partial 0(x)$ não está definido. Se

$$f(x) = \sum_{i=0}^{n} a_i x^i \in A[x],$$

com $\partial f(x) = n$, dizemos que a_n é o *coeficiente líder de* $f(x)$. No caso específico em que $a_n = 1$, $f(x)$ é dito *mônico.*

Proposição 1.14 *1. Se A é um domínio e $f(x), g(x) \in A[x]$, tais que $f(x)+g(x) \neq 0$, então*

$$\partial(f(x) + g(x)) = \max\{\partial f(x), \partial g(x)\} \text{ e } \partial(f(x)g(x)) = \partial(f(x)) + \partial(g(x)).$$

Neste caso, $A[x]$ é um domínio.

2. Se A é um corpo, então os únicos polinômios invertíveis sobre $A[x]$ são os polinômios constantes. Assim, $A[x]$ nunca é um corpo. ■

Se $A[x_1]$ é um domínio, definimos $A[x_1, x_2]$ como sendo $(A[x_1])[x_2]$, ou seja, o conjunto dos polinômios em uma indeterminada x_2 com coeficientes em $A[x_1]$. Temos, pela comutatividade de A, que $A[x_1, x_2] = (A[x_1])[x_2] = (A[x_2])[x_1]$. Fazendo identificações análogas àquelas feitas para $A[x]$, temos que todo polinômio

$$f(x_1, x_2) = (g_0(x_1), g_1(x_1), \ldots, g_n(x_1), \square) \in A[x_1, x_2]$$

pode ser escrito na notação formal

$$f = f(x_1, x_2) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_{ij} x_1^i x_2^j$$

onde $a_{ij} \in A, i, j \in \mathbb{Z}_+$ tais que $i + j \leq n$ e $a_{i+k,j+l} = 0, \forall k, l \in \mathbb{N}, \forall i, j \in \mathbb{Z}_+$ tais que $i + j = n$. Do mesmo modo, dado

$$f = f(x_1, x_2) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_{ij} x_1^i x_2^j \in A[x_1, x_2],$$

o *grau* de $f(x_1, x_2)$ é definido como sendo

$$\partial f(x_1, x_2) = \max\{r + s \in \mathbb{Z}_+; a_{rs} \neq 0 \text{ e } a_{ij} = 0, \forall i, j \in \mathbb{Z}_+ \text{ com } i + j > r + s \ \}.$$

Por indução, define-se $A[x_1, \ldots, x_n] = (A[x_1, \ldots, x_{n-1}])[x_n]$. Sejam D domínio, $\alpha \in D$, $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$ e o homomorfismo

$$\begin{array}{rccc} \varphi_\alpha : & D[x] & \longrightarrow & D \\ & \sum_{i=0}^{n} a_i x^i & \longmapsto & \sum_{i=0}^{n} a_i \alpha^i \end{array}$$

Define-se a *avaliação* de $f(x)$ em α, denotada por $f(\alpha)$, como sendo $f(\alpha) = \varphi_\alpha(f(x))$. No caso em que $f(\alpha) = 0$, dizemos que α é *raiz* ou *zero* de $f(x)$.

Proposição 1.15 *Se K é um corpo e $f(x) \in K[x], \partial f(x) = n > 0$, então $f(x)$ possui no máximo n raízes em K e em qualquer extensão de K .* ■

Seja $p \in \mathbb{N}$ primo. A função

$$\begin{array}{rccc} \varphi : & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}_p[x] \\ & \sum_{i=0}^{n} a_i x^i & \longmapsto & \sum_{i=0}^{n} \overline{a}_i x^i \end{array}$$

é um homomorfismo sobrejetor de anéis, onde $\overline{a}_i$ significa $a_i \bmod p$. Dado $f(x) \in \mathbb{Z}[x]$, então $\varphi(f(x))$ será denotado por $f(x) \bmod p$. Sejam D domínio e $a \in D$. Um elemento $b \in D$ é dito *divisor* ou *fator* de a (em D) se existir $c \in D$ tal que $a = bc$; dizemos também que b *divide* a ou que a é *múltiplo* de b e denotamos $b \mid a$. Se b não é um fator de a, dizemos que b *não divide* a e denotamos $b \nmid a$. Se existe $u \in U(D)$ tal que $a = ub$, dizemos que a e b são *associados*. Seja D domínio. Um elemento $a \in D^*$ é dito *irredutível* se

(i) $a \notin U(D)$;

(ii) $\forall b, c \in D$ tais que $a = bc$, então $b \in U(D)$ ou $c \in U(D)$.

Seja D domínio. Um elemento $p \in D^*$ é dito *primo* se

(i) $p \notin U(D)$;

(ii) $\forall a, b \in D$ tais que $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Mostra-se que, em D, todo elemento primo é irredutível, mas nem sempre a recíproca é verdadeira.

Proposição 1.16 *Sejam D domínio, $f(x) \in D[x]$, $\partial f(x) \neq 0$ e $\alpha \in D$. Tem-se $f(\alpha) = 0$ se, e somente se, $(x - \alpha)$ divide $f(x)$.* ■

Corolário 1.4 *Seja K corpo. Vale o seguinte*:

1. *Se $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, $\partial f = n > 0$, possui n raízes $v_1, v_2, \ldots v_n$ em K, então $f(x) = a_n(x - v_1)(x - v_2)\cdots(x - v_n)$;*

2. *Se $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, $\partial f = n > 0$ possui r raízes $v_1, v_2, \ldots v_r$ em K, com $r < n$, então $f(x) = a_n(x - v_1)(x - v_2)\cdots(x - v_r)t(x)$, onde $t(x)$ não possui raiz em K.* ■

Sejam K corpo, $f(x) \in K[x]$ e L uma extensão de K. Dizemos que L é o *corpo de decomposição* de $f(x)$ se:

(i) Todas as raízes $v_1, v_2, \ldots, v_n$ de $f(x)$ estão em L, isto é,

$$f(x) = a_n(x - v_1)(x - v_2)\cdots(x - v_n) \in L[x];$$

(ii) L é gerado sobre K por $v_1, v_2, \ldots, v_n$, isto é, $L = K(v_1, v_2, \ldots, v_n)$.

Vale salientar que dado um polinômio $f(x) \in K[x]$, seu corpo de decomposição é único, a menos de isomorfismos.

Teorema 1.12 (Kronecker) *Sejam K corpo, $f(x) \in K[x]$,$\partial f = n > 0$. Existe um corpo L tal que $K \subseteq L$ e L é o corpo de decomposição de $f(x)$.* ■

Sejam D domínio e $a_1, a_2, \ldots, a_n \in D$. Um elemento $d \in D$ é dito *máximo divisor comum* de $a_1, a_2, \ldots, a_n$ se ocorre:

(i) $d \mid a_1, d \mid a_2, \ldots, d \mid a_n$;

(ii) se $d' \in D$ é tal que $d' \mid a_1, d' \mid a_2, \ldots, d' \mid a_n$, então $d' \mid d$.

Notação: $d = MDC\{a_1, a_2, \ldots, a_n\}$. Em particular, se $d = 1$, dizemos que $a_1, a_2, \ldots, a_n$ são *relativamente primos.* Sejam D domínio e $a_1, a_2, \ldots, a_n \in D$. Um elemento $m \in D$ é dito *mínimo múltiplo comum* de $a_1, a_2, \ldots, a_n$ se ocorre:

(i) $a_1 \mid m, a_2 \mid m, \ldots, a_n \mid m$;

(ii) se $m' \in D$ é tal que $a_1 \mid m', a_2 \mid m', \ldots, a_n \mid m'$, então $m \mid m'$.

Notação: $m = MMC\{a_1, a_2, \ldots, a_n\}$. Se, num domínio D, para todo par de elementos $a, b \in D$, existe algum máximo divisor comum (mínimo múltiplo comum), diz-se que D é um domínio com máximo divisor comum (mínimo múltiplo comum). Um *domínio euclidiano* é um domínio D equipado com uma função

$$\Phi : D^* \longrightarrow \mathbb{Z}_+$$

que satisfaz às seguintes propriedades:

(i) $\forall a, b \in D, b \neq 0, \exists t, r \in D$ tais que $a = bt + r$, com $r = 0$ ou $\Phi(r) < \Phi(b)$;

(ii) $\forall a, b \in D^*$, tem-se $\Phi(a) \leq \Phi(ab)$.

Mostra-se que $(\mathbb{Z}, +, \bullet, |\ .\ |)$ e $(K[x], \oplus, \odot, \partial)$ são domínios euclidianos, onde K é um corpo e $|.|$ e ∂ são, respectivamente, as funções

$$\begin{array}{rccc} |.| : & \mathbb{Z}^* & \longrightarrow & \mathbb{Z}_+ \\ & n & \longmapsto & |n| \end{array}$$

e

$$\begin{array}{rccc} \partial : & K[x] - \{0\} & \longrightarrow & \mathbb{Z}_+ \\ & f(x) & \longmapsto & \partial(f(x)) \end{array} .$$

Proposição 1.17 (Algoritmo da Divisão) *Sejam D domínio,*

$$f(x) \in D[x] \ \ e \ \ g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \in D[x]$$

tal que $b_m \in U(D)$. Então:

1. *Existem $t(x), r(x) \in D[x]$ tais que $f(x) = g(x)t(x) + r(x)$, com $\partial r(x) < \partial g(x)$ ou $r(x) = 0(x)$;*

2. *Tais $t(x)$ e $r(x)$ são unicamente determinados.* ■

Um domínio D é dito *domínio fatorial* ou *domínio de fatoração única* se todo elemento não-invertível de D se escreve de "maneira única" como produto de elementos irredutíveis de D, isto é, de maneira precisa:

(i) Todo elemento não-invertível de D é um produto finito de fatores irredutíveis;

(ii) Se $\{p_i\}_{1\leq i\leq s}$ e $\{q_j\}_{1\leq j\leq t}$ são famílias finitas de elementos irredutíveis de D tais que $p_1\cdots p_s = q_1\cdots q_t$, então $s = t$ e, a menos de ordenação, p_i é associado a $q_i, \forall i = 1,\ldots,s$ (isto é, existe uma permutação σ de $\{1,\ldots,s\}$ tal que p_i é associado a $q_{\sigma(i)}, \forall i = 1,\ldots,s$).

É fácil ver que, em um domínio fatorial, todo elemento irredutível é primo e que todo domínio fatorial é um domínio com máximo divisor comum (domínio com mínimo múltiplo comum).

Teorema 1.13 *Seja D um domínio euclidiano. Então:*

1. *$\forall a, b \in D$, com $b \neq 0, \exists d = MDC\{a, b\}$ e $\exists r, s \in D$ tais que $d = ra + sb$;*

2. *Tais r e s podem ser efetivamente calculados quando a divisão em D é efetiva (isto é, existe um algoritmo que calcula r e s quando existe um algoritmo de divisão em D, similar ao Algoritmo de Euclides para os inteiros).* ■

Seja $(D, +, \bullet)$ um domínio. Um *corpo de frações* de D é um corpo $(K, \oplus, \odot)$ tal que:

(i) $(D, +, \bullet) \subseteq (K, \oplus, \odot)$, isto é, existe $D' \subseteq K$, D' domínio, tal que $D' \cong D$, a restrição de $\oplus$ para D' é igual a $+$ e a restrição de $\odot$ para D' é igual a $\bullet$;

(ii) $\forall \alpha \in D^*$, $\exists \xi \in K$ tal que $\alpha\xi = \xi\alpha = 1$, ou seja, todo elemento não-nulo de D possui um inverso em K.

Proposição 1.18 *Seja D um domínio qualquer. Vale o seguinte*:

1. *Existe um corpo de frações de D;*

2. *Se K_1 e K_2 são corpos de frações de D, então $K_1 \cong K_2$.* ■

Em particular, $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$.

Proposição 1.19 *Sejam D um domínio fatorial e K seu corpo de frações. Se $f(x) \in D[x]$ é irredutível sobre D, então $f(x)$ é irredutível sobre K.* ■

Teorema 1.14 (Gauss) *Se D é um domínio fatorial, então $D[x]$ também o é.* ■

Corolário 1.5 *Se D é um domínio fatorial, então $D[x_1, \ldots, x_n]$ também o é.* ■

Teorema 1.15 (Eisenstein) *Seja D um domínio fatorial com corpo de frações K e*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in D[x].$$

Se $p \in D$ é primo e satisfaz:

1. $p \mid a_i, \forall i < n$ *e* $p \nmid a_n$;
2. $p^2 \nmid a_0$;

Então, $f(x)$ é irredutível sobre K. ■

Seja A um anel comutativo com unidade. Dizemos que $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ é um *polinômio simétrico* se, dada qualquer permutação $\sigma \in S_n$, tem-se que $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$. Dado $i \in \{1, \ldots, n\}$, o *i-ésimo polinômio simétrico elementar* $s_i(x_1, \ldots, x_n)$ é definido como sendo

$$s_i(x_1, \ldots, x_n) = \sum_{k=0}^{N} a_k x_{j_1} \ldots x_{j_i}$$

onde $1 \leq j_1 < j_2 \ldots < j_i \leq n, a_k = 1$ e $N = \binom{n}{i}$.

Teorema 1.16 (Polinômios Simétricos) *Seja A um anel comutativo com unidade. Vale o seguinte:*

1. *Se $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ é um polinômio simétrico, pode-se construir um único polinômio $g(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ tal que $f(x_1, \ldots, x_n) = g(s_1, \ldots, s_n)$;*
2. *Se $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, com $\partial f(x) = n \geq 1, a_n$ invertível e raízes $v_1, v_2, \ldots, v_n$, então*

$$\frac{a_{n-1}}{a_n} = (-1)^i s_i(x_1, \ldots, x_n), \forall i \in \{1, \ldots, n\}.$$

■

Corolário 1.6 *Sejam A um anel comutativo com unidade,*

$$f(x) = \sum_{i=0}^{n} a_i x^i \in A[x],$$

com $\partial f(x) = n \geq 1, a_n$ invertível e $v_1, v_2, \ldots, v_n$ suas raízes. Se $g = g(v_1, v_2, \ldots, v_n)$ é simétrico, existe único $h = h(\frac{a_0}{a_n}, \cdots, \frac{a_{n-1}}{a_n})$ tal que $g = h$. ■

1.3 Extensões Algébricas

Seja L/K uma extensão. Um elemento $\alpha \in L$ é dito *algébrico* sobre K se $\exists\ f(x) \in K[x]\backslash\{0\}$ tal que $f(\alpha) = 0$. Já L/K é dita *algébrica* se todo elemento de L é algébrico sobre K. Prova-se que dados L/K algébrica e $\alpha \in L$, existe único $p(x) \in K[x]$ mônico, irredutível, tal que $p(\alpha) = 0$. Tal $p(x)$ é denotado por $irr(\alpha, K)$. Seja L/K uma extensão algébrica. Dizemos que $\alpha \in L$ é *separável* sobre K se α é raiz simples de $irr(\alpha, K)$ (para a definição de raiz simples, ver Cap. 4). Já L/K é dita separável se cada um dos seus elementos é separável sobre K. Um corpo K é dito *perfeito* se todas as suas extensões finitas são separáveis. Prova-se que corpos finitos e corpos de característica zero são perfeitos. Seja L/K uma extensão de corpos. O *grupo de Galois de* L/K, denotado por $G(L/K)$, é definido como sendo

$$G(L/K) = \{\sigma \in Aut(L); \sigma(a) = a, \forall a \in K\}.$$

Dizemos que uma extensão algébrica N/K é *normal* se $\forall\ p(x) \in K[x]$ irredutível tal que $\exists \alpha \in N$ raiz de p, então $p(x)$ se decompõe sobre $N[x]$. Sejam L um corpo e G um subconjunto não vazio de $Aut(L)$. Então, o conjunto $L^G \subseteq L$, definido por

$$L^G = \{\alpha \in L; \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

é um subcorpo de L, denominado de *subcorpo fixado por* G. Uma extensão algébrica N/K é dita *galoisiana* se $N^{G(N/K)} = K$. Prova-se que N/K finita é galoisiana se, e somente se, é normal e separável. Seja R um conjunto não-vazio. Uma relação $\leq$ entre pares de elementos de R diz-se uma *relação de ordem parcial em* R se:

1. $a \leq a, \forall a \in R$;
2. $a \leq b$ e $b \leq a \Rightarrow a = b, \forall a, b \in R$;
3. $a \leq b$ e $b \leq c \Rightarrow a \leq c, \forall a, b, c \in R$.

Neste caso, dizemos que $(R, \leq)$ é um *conjunto parcialmente ordenado*. Sejam $(R, \leq)$ um conjunto parcialmente ordenado e $a, b \in R$. Dizemos que $c \in R$ é *supremo de* a *e* b se:

1. $a \leq c$ e $b \leq c$;
2. Se $c' \in R$ é tal que $a \leq c'$ e $b \leq c'$, então $c \leq c'$.

O supremo de a e b se existir é único e será denotado por $a \vee b$. Sejam $(R, \leq)$ um conjunto parcialmente ordenado e $a, b \in R$. Dizemos que $d \in R$ é *ínfimo de a e b* se:

1. $d \leq a$ e $d \leq b$;

2. Se $d' \in R$ é tal que $d' \leq a$ e $d' \leq b$, então $d' \leq d$.

O ínfimo de a e b se existir é único e será denotado por $a \wedge b$. Um *reticulado* é um conjunto parcialmente ordenado $(R, \leq)$ no qual cada par de elementos $a, b \in R$ possui ínfimo $a \wedge b$ e supremo $a \vee b$. É fácil ver que se G é um grupo, então $(Sub(G), \subseteq)$ é um reticulado, com $H \vee H' = \langle H \cup H' \rangle$ e $H \wedge H' = H \cap H', \forall H, H' \in Sub(G)$. Também verifica-se que se N/K é uma extensão de corpos, então $(Lat(N/K), \subseteq)$ é um reticulado, com $L \vee M = \langle L \cup M \rangle$ e $L \wedge M = L \cap M, \forall L, M \in Lat(N/K)$.

Teorema 1.17 (Fundamental de Galois) *Seja N/K uma extensão normal com grupo de Galois $G = G(N/K)$.*

1. *A função*

$$\begin{array}{rccc} \gamma: & Sub(G) & \longrightarrow & Lat(N/K) \\ & H & \longmapsto & N^H \end{array}$$

   é uma bijeção que inverte ordem, com inversa

$$\delta : Lat(N/K) \longrightarrow Sub(G)$$

$$L \longmapsto G(N/L)$$

2. *$N^{H \vee H'} = N^H \cap N^{H'}$ e $N^{H \wedge H'} = N^H \vee N^{H'}$, $\forall H, H' \in Sub(G)$; $G(N/(L \vee M)) = G(N/L) \cap G(N/M)$ e $G(N/(L \cap M)) = G(N/L) \vee G(N/M), \forall L, M \in Lat(N/K)$;*

3. *$(L : K) = (G(N/K) : G(N/L)), \forall L \in Lat(N/K)$ e $(G : H) = (N^H : K), \forall H \in Sub(G)$. Além disso, se $\gamma(H) = L$, então $\mid H \mid = (N : L)$;*

4. *Se $b \in N$ é tal que $\sigma(b) = b, \forall \sigma \in G(N/K)$, então $b \in K$;*

5. *L/K é normal se, e somente se, $G(N/L) \trianglelefteq G(N/K)$.* ■

Corolário 1.7 *Toda extensão normal é simples.* ■

Uma *ação* de um grupo G sobre um conjunto não-vazio X é uma função

$$\begin{aligned} * : \ G \times X &\longrightarrow X \\ (g, x) &\longmapsto g * x \end{aligned}$$

que satisfaz:

(i) $e * x = x, \forall x \in X$;

(ii) $(gg') * x = g * (g' * x), \forall g, g' \in G, \forall x \in X$.

Neste caso, dizemos que G age sobre X. Todo grupo G age sobre si mesmo (aqui $X = G$) por conjugação: basta definir $g * x = g^{-1}xg, \forall g \in G, \forall x \in X$. Por outro lado, se $X = \{1, 2, \ldots, n\}$ e $G \leq S_n$, então a função

$$\begin{aligned} * : \ G \times X &\longrightarrow X \\ (\sigma, j) &\longmapsto \sigma(j) \end{aligned}$$

é uma ação de G sobre X. Sejam G um grupo, X um conjunto qualquer não-vazio e suponhamos que G age sobre X por $*$ e seja $x \in X$. A *órbita* contendo x (sob G), denotada por $G * x$, é definida como sendo

$$G * x = \{g * x; g \in G\}.$$

$\mid G * x \mid$ é chamado de *comprimento* da órbita contendo x. O conjunto das órbitas de X,

$$G * X = \{G * x; x \in X\}$$

particiona X. Esta partição de X induz uma partição de $\mid X \mid$, chamada de *partição do comprimento das órbitas* de X sob G. Esta partição de $\mid X \mid$ consiste dos comprimentos das órbitas distintas de X sob G. Dado um grupo G, uma *representação de* G é um homomorfismo φ de G em algum grupo G'. Se $Ker(\varphi) = \{e\}$, dizemos que a representação é *fiel.* No caso em que $G' \leq S_n$, dizemos que φ é uma *representação por permutações.*

Proposição 1.20 *A cada ação corresponde uma representação e vice-e-versa.* ■

Sejam G um grupo, X um conjunto qualquer não-vazio e suponhamos que G age sobre X por $*$. Dizemos que G *age transitivamente* sobre X se $G * x = X, \forall x \in X$. Isto é equivalente a dizer que a ação de G sobre X possui uma única órbita, ou seja, $G * X = \{X\}$. Dizemos também que a representação induzida pela última proposição é

transitiva. Sejam G um grupo, X um conjunto qualquer não-vazio e suponhamos que G age sobre X por $*$. Se $x \in X$, o *estabilizador* de x em G, denotado por $stab_G(x)$, é definido por

$$stab_G(x) = \{g \in G; g * x = x\}.$$

Sejam $g, g_1, g_2 \in G, x \in X$ e $H = stab_G(x)$. É fácil mostrar que os seguintes fatos são verdadeiros:

(1) $H \leq G$;

(2) $g_1 * x = g_2 * x$ se, e somente se, $g_1 H = g_2 H$;

(3) $stab_G(g * x) = gHg^{-1}$.

Sejam G um grupo, X um conjunto qualquer não-vazio e suponhamos que G age sobre X por $*$. Suponhamos ainda que $\mid X \mid = n < \infty$ e seja $\underline{X} = (x_1, x_2, \ldots, x_n)$ uma ordenação dos elementos de X. Então existe uma representação natural por permutações

$$\begin{array}{rccc} rep(G, \underline{X}, *): & G & \longrightarrow & S_n \\ & g & \longmapsto & \sigma_g \end{array}$$

onde $\sigma_g(i) = j$ se, e somente se, $g * x_i = x_j, \forall g \in G$ e $i, j \in \{1, 2, \ldots, n\}$. O núcleo de $rep(G, \underline{X}, *)$ é

$$\bigcap_{i=1}^{n} stab_G(x_i).$$

O subgrupo de S_n que é a imagem de $rep(G, \underline{X}, *)$ é denotado por

$$\mathrm{Im}(rep(G, \underline{X}, *)).$$

Seja $H = \mathrm{Im}(rep(G, \underline{X}, *))$ e seja σ uma permutação de S_n. Consideremos uma nova ordenação dos elementos de X :

$$\underline{X}' = (x'_1, x'_2, \ldots, x'_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Então $\mathrm{Im}(rep(G, \underline{X}, *)) = \sigma H \sigma^{-1}$. Dizemos que $G \leq S_n$ é *transitivo* se a ação de G sobre $X = \{1, 2, \ldots, n\}$ descrita anteriormente possui uma única órbita, ou seja, $G * j = X, \forall j \in X$. Isto equivale a dizer que $\forall j, k \in X, \exists \sigma \in G$ tal que $\sigma(j) = k$. Ou ainda, $\sigma(X) = X, \forall \sigma \in G$. Caso contrário, dizemos que G é *intransitivo.* De um modo geral, dizemos que $G \leq S_n$ é *r-transitivo* ($r \leq \deg(G), r \in \mathbb{N}$) se $\forall \{i_1, i_2, \ldots, i_r\}, \{j_1, j_2, \ldots, j_r\} \subseteq X, \exists \sigma \in G$

tal que $\sigma(i_1) = j_1, \sigma(i_2) = j_2, \ldots, \sigma(i_r) = j_r$. Assim, G é $1-$transitivo se, e somente se, G é transitivo. Seja $G \leq S_n$ e $X = \{1, 2, \ldots, n\}$. Um *bloco* B de G é um subconjunto próprio de X tal que:

(i) $\mid B \mid > 1$;

(ii) Se $\sigma \in G$, então ou $B = \sigma(B)$ ou $B \cap \sigma(B) = .$

$G \leq S_n$ transitivo é dito *imprimitivo* se possui blocos. Caso contrário, dizemos que G é *primitivo.*

Teorema 1.18 *Sejam $G \leq S_n$ transitivo e $X = \{1, 2, \ldots, n\}$.*

1. *Se $\deg(G) = p$ primo, então G é primitivo;*
2. *Se G é imprimitivo e B é um bloco, então $\sigma(B)$ é um bloco, $\forall \sigma \in G$. Além disso, $\mid B \mid$ divide n;*
3. *Se G é imprimitivo e B, B' são blocos, então $\mid B \mid = \mid B' \mid$;*
4. *Se G é imprimitivo e B é um bloco, então*

$$X = \dot{\bigcup_{\sigma \in G}} \sigma(B).$$

■

Sejam $G \leq S_n$ imprimitivo, $X = \{1, 2, \ldots, n\}$ e B um bloco. O conjunto

$$G(B) = \{\sigma(B); \sigma \in G\}$$

é chamado de *sistema de imprimitividade* de G. Um grupo imprimitivo pode possuir mais de um sistema de imprimitividade. Sejam K corpo, $f(x) \in K[x], N$ o corpo de decomposição de $f(x), G = G(N/K)$ e $\underline{V} = (v_1, v_2, \ldots, v_n)$ uma ordenação dos (distintos) zeros de $f(x)$. G leva zero de $f(x)$ em zero de $f(x)$ (ver Lema 2.6) e assim G age sobre o conjunto $V = \{v_1, v_2, \ldots, v_n\}$ por $*$, onde $\sigma * v_i = \sigma(v_i), \forall \sigma \in G$ e $i \in \{1, 2, \ldots, n\}$. Assim uma representação natural por permutações

$$rep(G(N/K), \underline{V}, *) : G(N/K) \longrightarrow S_n$$

como a descrita anteriormente. Esta representação é fiel no seguinte sentido: se um elemento τ está no núcleo de $rep(G(N/K), \underline{V}, *)$, então τ fixa cada um dos v_i, bem como

os elementos de K. Desde que V gera N sobre K, então τ é a identidade de $G(N/K)$. O *grupo de Galois de* $f(x)$ *sobre* K, com respeito à ordenação $\underline{V}$ dos zeros de $f(x)$, é definido como sendo $\mathrm{Im}(rep(G(N/K), \underline{V}, *))$. Se não for fixada uma ordenação dos zeros de $f(x)$, então $Gal(f/K)$ pode ser determinado, quando muito, por conjugação interna em S_n. Isto é mais forte do que isomorfismo interno e nesta dissertação, geralmente não estaremos interessados no problema da ordenação dos zeros de $f(x)$. Se não a especificarmos e estabelecermos que $Gal(f/K) = G$, queremos dizer que para alguma ordenação dos zeros de $f(x), Gal(f/K) = G$ com respeito àquela ordenação. Sejam G grupo, $H \leq G$ e $C = \frac{G}{H}$. Temos que a função

$$\begin{array}{rccc} * : & G \times C & \longrightarrow & C \\ & (g, xH) & \longmapsto & gxH \end{array}$$

é uma ação de G sobre C. Assim, temos em correspondência a representação

$$\begin{array}{rccc} T : & G & \longrightarrow & \mathcal{P}(C) \\ & g & \longmapsto & T_g \end{array},$$

onde

$$\begin{array}{rccc} T_g : & C & \longrightarrow & C \\ & xH & \longmapsto & g * (xH) \end{array}.$$

Note que se $H \trianglelefteq G$, então $Ker(T) = H$. O subgrupo $T(G)$ será denotado por $\mathrm{Im}(rep(G, \mathcal{P}(C)))$. Sejam K corpo e $f(x) \in K[x]$. Dizemos que $f(x)$ é *solúvel por radicais* sobre K se existe uma cadeia de corpos

$$K = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_{t-1} \subseteq B_t$$

onde cada B_{i+1}/B_i é uma extensão pura e B_t contém o corpo de decomposição de $f(x)$ sobre K. A extensão B_t/K é chamada de *extensão radical.*

Teorema 1.19 (Galois) *Sejam K corpo, com $Char(K) = 0$ e $f(x) \in K[x]$. Tem-se que $f(x)$ é solúvel por radicais sobre K se, e somente se, $Gal(f/K)$ é solúvel.* ■

Seja $F = F(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ e seja $\sigma \in S_n$. Definimos o *polinômio conjugado de F com respeito à σ*, denotado por $\sigma * F$ como sendo

$$\sigma * F = F(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Deste modo, qualquer subgrupo de S_n age sobre $K[x_1, \ldots, x_n]$ como um grupo de automorfismos de um anel. Sejam $F \in K[x_1, \ldots, x_n], f(x) \in K[x], n = \partial f > 0$ e $v_1, \ldots, v_n$ os zeros de $f(x)$. O *polinômio resolvente* (ou a *resolvente*) associado(a) a F e $f(x)$, denotado(a) por $R(F, f)$, é definido(a) por

$$R(F, f) = \prod_{i=1}^{k} \left(x - F_i(v_1, \ldots, v_n)\right),$$

onde

$$\{F_1, \ldots, F_k\} = S_n * F, \text{ com } F_i \neq F_j, \text{ para } i \neq j.$$

Podemos tomar $F_i = \sigma_i * F, i = 1, \ldots, k$, onde $\{\sigma_1, \ldots, \sigma_k\}$ é um conjunto de representantes das classes laterais de $stab_{S_n}(F)$ em S_n. Os coeficientes de $R(F, f)$ são polinômios simétricos sobre K em $v_1, \ldots, v_n$ e daí, pelo Teorema dos Polinômios Simétricos, podem ser expressos como polinômios sobre K nos coeficientes de $f(x)$. Também nota-se que $R(F, f)$ é independente da ordenação dos zeros de $f(x)$. Sejam $f(x) \in K[x], n = \partial f > 1, e_1, \ldots, e_r \in K, 0 < r \leq n$ e o multiconjunto $M = [e_1, \ldots, e_r]$. O *polinômio resolvente linear* (ou a *resolvente linear*) associado(a) a M e $f(x)$, denotado(a) por $LR(M, f)$, é definido(a) como sendo o polinômio associado a $F = F(x_1, \ldots, x_n)$ e $f(x)$, onde $F = e_1x_1 + \cdots + e_rx_r$. Sejam $f(x) \in K[x], n = \partial f > 1$ e $v_1, \ldots, v_n$ os zeros de $f(x)$. O *discriminante* de $f(x)$, denotado por $disc(f)$, é definido por

$$disc(f) = \prod_{i<j} (v_i - v_j)^2$$

Note que $disc(f) = 0$ se, e somente se, os zeros de $f(x)$ não são distintos. O discriminante do polinômio mônico $f(x)$ pode ser calculado eficientemente usando a relação

$$disc(f) = (-1)^{n(n-1)/2} res(f, f'),$$

onde $res(f, f')$ é a *resultante* de $f(x)$ e sua *derivada formal* $f'(x)$. A resultante e a derivada formal serão discutidas na Seção 4.2. Seja $f(x) \in \mathbb{Q}[x]$ um polinômio mônico separável, com $n = \partial f > 0$. Vamos, primeiramente, admitir que o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$ é um subcorpo dos complexos. Em segundo lugar, podemos assumir que os coeficientes de $f(x)$ são inteiros pois, caso contrário, podemos aplicar a seguinte transformação a $f(x)$: Seja c o mínimo múltiplo comum dos denominadores dos coeficientes de $f(x)$. Então

$$g(x) = c^n f(x/c)$$

é um polinômio mônico em $\mathbb{Z}[x]$. Se $v_1, v_2, \ldots, v_n$ são os zeros de $f(x)$,então $cv_1, cv_2, \ldots, cv_n$ são os zeros de $g(x)$ e, com respeito a estas ordenações, $Gal(g/\mathbb{Q}) \cong Gal(f/\mathbb{Q})$. Seja $X = \{x_1, x_2, \ldots, x_n\}$. Um *r-conjunto de* X, com $1 \leq r \leq n$, é qualquer subconjunto de X com r elementos e será denotado por $\{y_1, y_2, \ldots, y_r\}$. Já uma *r-seqüência de* X, com $1 \leq r \leq n$, é qualquer r-upla formada por elementos de X e será denotada por $(y_1, y_2, \ldots, y_r)$. Vale salientar que dois r-conjuntos de X diferem entre sí pela natureza de seus elementos, enquanto que duas r-seqüências de X diferem entre sí pela ordem de seus elementos. Por exemplo, se $X = \{1, 2, 3\}$, então os possíveis 2-conjuntos e 2 -seqüências de X são, respectivamente

$$\{1, 2\}, \{1, 3\}, \{2, 3\}$$

e

$$(1, 1), (1, 2), (1, 3), (2, 1)(2, 2), (2, 3), (3, 1), (3, 2), (3, 3).$$

Para referências futuras, enunciaremos o

Teorema 1.20 (Chinês dos Restos) *Sejam* $n_1, n_2, \ldots, n_r \in \mathbb{N}$, *com* $n_i \geq 2$, *relativamente primos dois a dois,* $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$ *e* $z_1, z_2, \ldots, z_r$ *inteiros quaisquer. Então o sistema de congruências*

$$z \equiv z_i (\mathrm{mod}\, n_i^{\alpha_i}), 1 \leq i \leq r$$

admite solução em $\mathbb{Z}$, *que é única módulo* $n = \prod_{i=1}^{r} n_i^{\alpha_i}$. ■

Capítulo 2

Métodos de determinação do grupo de Galois

Neste capítulo, discutiremos algoritmos para determinar propriedades do grupo de Galois de um polinômio. O objetivo é determinar com eficiência a informação necessária para especificar representantes das classes de conjugação do grupo de Galois. Incluiremos neste capítulo trabalhos feitos previamente e nossa discussão centrar-se-á no polinômio resolvente.

2.1 Determinação do grupo de Galois em um número finito de etapas

Seja $f(x) \in K[x], n = \partial f > 0$. Além disso, suponha que $f(x)$ tem zeros distintos $v_1, \ldots, v_n$, no corpo de decomposição de $f(x)$ sobre K. Se existe um algoritmo para fatorar polinômios em duas ou mais variáveis sobre K, então podemos determinar $Gal(f/K)$ em um número finito de etapas usando um método detalhado por van der Warden [14]. Notemos que tal algoritmo de fatoração existe quando existe um algoritmo para a fatoração de polinômios em uma variável sobre K. Para encontrar $Gal(f/K)$ por este algoritmo, procede-se da seguinte maneira: Forme a expressão

$$t = x_1v_1 + x_2v_2 + \cdots + x_nv_n$$

onde $x_1, x_2, \ldots, x_n$ são indeterminadas. Sejam $t_1, t_2, \ldots, t_{n!}$ as expressões distintas obtidas de t pela aplicação de todas as possíveis permutações para os índices dos x_i. Ponha

$$F = F(z, x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} (z - t_i).$$

F tem coeficientes simétricos nos v_i, daí podem ser expressos em termos dos coeficientes de $f(x)$ e dos x_i. Seja a fatoração de F em fatores irredutíveis sobre $K[z, x_1, x_2, \ldots, x_n]$:

$$F = F_1 F_2 \cdots F_r.$$

As permutações dos x_i que deixam invariante qualquer fator, digamos F_1, formam um grupo G.

Teorema 2.1 *Se assumirmos que os zeros de $f(x)$ estão ordenados de modo que $x_1v_1 + x_2v_2 + \cdots + x_nv_n$ é um zero de F_1, então $Gal(f/K) = G$.* ■

Este método é claramente impraticável do ponto de vista computacional. Apesar disso, o resultado do Teorema 2.1 é usado para provar um resultado útil computacionalmente para o caso $K = \mathbb{Q}$. Este resultado é estabelecido no Teorema 2.2.

2.2 A determinação dos tipos ciclos em $Gal(f/\mathbb{Q})$

Sejam $f(x) \in \mathbb{Z}[x]$ um polinômio mônico e separável, $n = \partial f > 1$ e $p \in \mathbb{N}$ um primo. Definimos o *tipo ciclo* de uma permutação $\sigma \in S_n$ como sendo a partição de n induzida pelos comprimentos dos ciclos disjuntos de σ. O *tipo fator* de $f(x) \bmod p$ é definido como sendo a partição de n induzida pelos graus dos fatores irredutíveis de $f(x) \bmod p$ sobre $\mathbb{Z}_p$. Um método útil para descobrir informação sobre $Gal(f/\mathbb{Q})$ é determinar tipos ciclos de suas permutações, por fatoração de $f(x) \bmod p$ sobre $\mathbb{Z}_p$, p primo, com $p \nmid disc(f)$. Este método tem sido discutido por muitos autores, incluindo van der Warden, Zassenhaus e McKay [10, 14, 15].

Teorema 2.2 *Para todo primo p tal que $p \nmid disc(f)$, o tipo fator de $f(x) \bmod p$ é tipo ciclo de alguma permutação em $Gal(f/\mathbb{Q})$.* ■

O próximo resultado, que segue do Teorema da Densidade de Chebotarev, também pode ser usado:

Teorema 2.3 *Seja T uma partição de n. Então, quando $k \to \infty$, a proporção de ocorrência de T como tipo fator de $f(x) \bmod p_i, i = 1, 2, \ldots, k$ ($p_1, p_2, \ldots, p_k$ primos distintos), tende à proporção de permutações em*
$Gal(f/\mathbb{Q})$ tendo tipo ciclo T . ■

Podemos fatorar $f(x) \bmod p$ sobre $\mathbb{Z}_p$ usando o Algoritmo de Berlekamp. Contudo, como estamos interessados apenas no tipo fator de $f(x) \bmod p$, podemos usar o método de fatoração parcial descrito em [7], que nos fornece a informação necessária. As tabelas A.2, A.4, A.6, A.8 do Apêndice contêm a distribuição de tipos ciclos dos subgrupos transitivos de $S_3, \ldots, S_6$, respectivamente. Já as tabelas A.10 e A.11 do Apêndice contêm a distribuição de tipos ciclos dos subgrupos transitivos de S_7. Essas tabelas são usadas quando aplicamos os teoremas 2.2 e 2.3. Aplicando o Teorema 2.2, podemos determinar tipos ciclos de permutações em $Gal(f/\mathbb{Q})$. Feito isso, aqueles grupos de permutações pertencentes às tabelas que não contêm tais tipos ciclos são excluídos como candidatos a $Gal(f/\mathbb{Q})$. Aplicando o Teorema 2.3, podemos conjecturar adequadamente sobre $Gal(f/\mathbb{Q})$ após uma fatoração de $f(x) \bmod p$ para um número "suficiente" de primos p. Se $Gal(f/\mathbb{Q}) = S_n$ ou A_n podemos, na maioria dos casos, determinar rapidamente $Gal(f/\mathbb{Q})$ pela aplicação do Teorema 2.2 e usando o fato de que $Gal(f/\mathbb{Q}) \leq A_n$ se, e somente se, $disc(f) = r^2 \in \mathbb{N}$ (cf. Proposição 2.3).

Exemplo 2.1 *Seja $f(x) = x^7 - 14x^5 + 56x^3 - 56x + 22$. Temos que $disc(f) = 2^6 7^{10}$. $f(x) \bmod p$ foi fatorado sobre $\mathbb{Z}_p$ para os 42 primos p no intervalo $[2, 193]$ tais que $p \nmid disc(f)$. Para um primo o tipo fator é (1^7), para trinta primos o tipo fator é $(3^2, 1)$ e para onze primos o tipo fator é (7). Recorrendo às tabelas A.10 e A.11 do Apêndice, conjecturamos (pelas evidências) que $Gal(f/\mathbb{Q}) = 7T3$, o grupo de Frobenius de ordem 21. De fato, podemos mostrar que $Gal(f/\mathbb{Q}) = 7T3$ (cf. Seção 4.3, Exemplo 4.1). Note que $disc(f) = r^2 \in \mathbb{N}$, daí $Gal(f/\mathbb{Q}) \leq A_7$. Isto, junto com os tipos ciclos de $Gal(f/\mathbb{Q})$ que determinamos, limita $7T3, 7T5$ e $7T6$ $(= A_7)$ como candidatos.*

Conjugação complexa é um automorfismo de qualquer subcorpo dos complexos. Se $f(x)$ é separável sobre $\mathbb{Q}$,então conjugação complexa induz um elemento em $Gal(f/\mathbb{Q})$ com tipo ciclo $(2^c, 1^r)$, onde c é o número de pares de conjugados complexos que são zeros de $f(x)$ e r é o número de zeros reais de $f(x)$. O número de zeros reais de um polinômio sobre $\mathbb{Q}$ pode ser determinado pela seqüência dos restos do Polinômio de Sturm. Note que

o polinômio $f(x)$ do Exemplo 2.1 tem todos os zeros reais. Isto é uma condição necessária para que $\mid Gal(f/\mathbb{Q}) \mid$ seja ímpar.

2.3 O polinômio resolvente

Sejam $f(x) \in K[x]$ separável, $n = \partial f > 0$ e $\underline{V} = (v_1, v_2, \ldots, v_n)$ uma ordenação dos zeros de $f(x)$. Resolventes são ferramentas clássicas e úteis, do ponto de vista computacional, para determinar $Gal(f/K)$ e é neste método que nos concentraremos. Para $F \in K[x_1, x_2, \ldots, x_n]$, usaremos a resolvente $R(F, f)$ (com zeros distintos) para determinar a partição do comprimento das órbitas de $S_n * F$ sobre $Gal(f/K)$. Seja N o corpo de decomposição de $f(x)$ sobre K. Então $G(N/K)$ age sobre N de modo natural como um grupo de automorfismos. Mostraremos agora que qualquer órbita dos elementos de N, sob a ação de $G(N/K)$, consiste precisamente dos zeros de um polinômio mônico irredutível sobre K. Primeiramente, provaremos o seguinte:

Lema 2.1 *Sejam* $W = \{\omega_1, \omega_2, \ldots, \omega_k\} \subset N$ *(com os* ω_i *distintos) e*

$$g(x) = \prod_{i=1}^{k}(x - \omega_i).$$

$G(N/K)$ *leva* W *em* W *se, e somente se,* $g(x) \in K[x]$.

Prova. Sejam

$$g(x) = \sum_{i=0}^{k} a_i x^i, \omega \in W, \sigma \in G(N/K)$$

e suponhamos que $g(x) \in K[x]$. Como σ é um automorfismo de N fixando K, temos:

$$0 = g(\omega) = \sigma(g(\omega)) = \sum_{i=0}^{k} \sigma(a_i)\sigma(\omega^i) = \sum_{i=0}^{k} a_i \sigma(\omega)^i = g(\sigma(\omega)).$$

Assim, $\sigma(\omega) \in W, \forall \omega \in W, \forall \sigma \in G(N/K)$, ou seja, $G(N/K)$ leva W em W. Reciprocamente, suponhamos que $G(N/K)$ leva W em W. Então qualquer elemento $\sigma \in G(N/K)$ induz uma permutação de W. Assim, $\sigma(a_i) = a_i$, para todo coeficiente a_i de $g(x)$, pois a_i é uma função simétrica de $\omega_1, \omega_2, \ldots, \omega_k$. Isto implica que $a_i \in K, \forall i = 1, \ldots, k$, ou seja, $g(x) \in K[x]$. ■

Proposição 2.1 *Sejam* $G = G(N/K)$ *e* $\omega \in W = \{\omega_1, \ldots, \omega_k\} \subset N$ *(com os* ω_i *distintos). Denotemos por* $G(\omega)$ *o conjunto* $\{\sigma(\omega); \sigma \in G\}$. *Tem-se* $W = G(\omega)$ *se, e somente se,* $g(x) = \prod_{i=1}^{k}(x - \omega_i)$ *é um polinômio irredutível sobre* K.

Prova. Se $G(\omega) = W$ então, pelo Lema 2.1 , $g(x) \in K[x]$. Suponhamos, por absurdo, que $g(x)$ é redutível. Então, $g(x)$ possui um fator $h(x) \in K[x]$, onde $h(x) = \sum_{i\in I}(x-\omega_i)$, para algum $I \subset \{1,\ldots,k\}$. Daí, pelo Lema 2.1, G leva $W' = \{\omega_i; i \in I\}$ em W' e isto contradiz o fato de que $G(\omega) = W$. Reciprocamente, suponhamos que $g(x) \in K[x]$ é um polinômio irredutível. Pelo Lema 2.1, sabemos que G leva W em W. Assim, $G(\omega) \subseteq W$. Se não fosse $W \subseteq G(\omega)$, existiria $I \subset \{1,\ldots,k\}$ tal que $G(\omega) = \{\omega_i; i \in I\}$. Então, pelo Lema 2.1, $h(x) = \sum_{i\in I}(x-\omega_i) \in K[x]$, ou seja, $g(x)$ possuiria um divisor próprio em $K[x]$, o que é uma contradição. ■

Corolário 2.1 *Se $f(x) \in K[x]$ é irredutível e separável, então $Gal(f/K)$ é transitivo.*

Prova. Suponhamos que $\partial f = n$. Sejam $v_1,\ldots,v_n$ os zeros(distintos) de $f(x)$, $\underline{V} = (v_1,\ldots,v_n)$ uma ordenação dos mesmos e $\varphi = rep(G(N/K),\underline{V},*)$ a representação fiel. Como $f(x)$ é irredutível temos, Proposição 2.1, que $G = G(N/K)$ é transitivo. Pelo Teorema Fundamental dos Homomorfismos,

$$\frac{G}{Ker(\varphi)} = G \simeq \mathrm{Im}(\varphi) = Gal(f/K)$$

e assim $Gal(f/K)$ é transitivo. ■

Aplicaremos o resultado precedente para determinar uma informação útil no que diz respeito à fatoração de uma resolvente. Seja $F \in K[x_1,\ldots,x_n]$. Recordemos que a resolvente sobre K associada com F e $f(x)$ é

$$R(F,f) = \prod_{i=1}^{k}(x - F_i(\underline{V})),$$

onde $\{F_1,\ldots,F_k\} = S_n * F$ (com os F_i distintos). Para $\tau \in G(N/K)$, seja $\tau \longmapsto \sigma_\tau$ sob a representação fiel de $G(N/K)$ sobre $Gal(f/K)$. Seja $\underset{1}{*}$ a ação de $G(N/K)$ sobre $K[\underline{V}]$ definida por $\tau \underset{1}{*} F(v_1,\ldots,v_n) = F(\tau(v_1),\ldots,\tau(v_n))$. Provaremos o seguinte lema:

Lema 2.2 $\tau \underset{1}{*} F(\underline{V}) = \sigma_\tau(\underline{V}) * F$.

Prova.

$$\begin{aligned}\tau \underset{1}{*} F(v_1,\ldots,v_n) &= F(\tau(v_1),\ldots,\tau(v_n)) \\ &= F(v_{\sigma_\tau(1)},\ldots,v_{\sigma_\tau(n)}) = \sigma_\tau(v_1,\ldots,v_n) * F.\end{aligned}$$

■ Assim, $Gal(f/K)$ age sobre polinômios nos zeros de $f(x)$ do mesmo modo que $G(N/K)$ o faz.

Proposição 2.2 *Seja* $t \in I \subset \{1, \ldots, k\}$.

(1) Se $Gal(f/K) * F_t = \{F_i; i \in I\}$ *e os* $F_i(\underline{V})$ *são distintos,* $\forall i \in I$, *então* $g(x) = \prod_{i \in I}(x - F_i(\underline{V}))$ *é um polinômio irredutível sobre* K;

(2) Se $g(x) = \prod_{i \in I}(x - F_i(\underline{V}))$ *é um fator irredutível não repetido de* $R(F, f)$, *então* $Gal(f/K) * F_t = \{F_i; i \in I\}$.

Prova. *(1)* Basta aplicar o Lema 2.1 e a Proposição 2.1. *(2)* Como N é separável sobre $K, g(x)$ deve ter zeros distintos. Usando a Proposição 2.1 e o Lema 2.2, temos que

$$\{F_i(\underline{V}); i \in I\} = \{\sigma(\underline{V}) * F; \sigma \in Gal(f/K)\}.$$

Como $g(x)$ é um fator não repetido de $R(F, f), \forall i \in I$ e $j = 1, \ldots, k$, $F_i(\underline{V}) = F_j(\underline{V})$ se, e somente se, $i = j$. Daí, segue o resultado. ■

Corolário 2.2 *Suponhamos que* $R(F, f)$ *tem zeros distintos. Então a partição do comprimento das órbitas de* $S_n * F$ *sob a ação de* $Gal(f/K)$ *é igual à partição de* $\partial(R(F, f))$ *induzida pelos fatores irredutíveis de* $R(F, f)$ *sobre* K. ■

Um método para lidar com a ocorrência de zeros repetidos de $R(F, f)$ é o uso de uma transformação apropriada de Tschirnhaus aplicada a $f(x)$. Agora suponhamos que $R(F, f)$ tem zeros distintos $\sigma_1(\underline{V}) * F, \ldots, \sigma_k(\underline{V}) * F$, onde $\{\sigma_1, \ldots, \sigma_k\}$ é um conjunto de representantes das classes laterais à esquerda de $stab_{S_n}(F)$ em S_n. Note que $Gal(f/K)$ age sobre os zeros de $R(F, f)$ por permutação dos σ_i. Assim,

$$Gal(R(F, f)/K) = \mathrm{Im}(rep(Gal(f/K), \underline{\sigma}, *)),$$

onde $\underline{\sigma} = \{\sigma_1, \ldots, \sigma_k\}$ e a ação $*$ é definida por $\tau * \sigma_i = \tau\sigma_i, \forall \tau \in Gal(f/K)$ e $i \in \{1, \ldots, k\}$. Notemos que a partição do comprimento das órbitas de $S_n * F$ sob a ação de $Gal(f/K)$ depende apenas de $stab_{S_n}(F)$.

Lema 2.3 *Seja* $F_t(\underline{V})$ *um zero de um fator irredutível não repetido da resolvente* $R(F, f)$. *Então* $K(F_t(\underline{V}))$ *é o corpo fixo correspondente a* H, *onde* $H \leq G(N/K)$ *é levado sobrejetivamente em* $stab_{Gal(f/K)}(F_t)$ *sob*
$rep(G(N/K), \underline{V}, *)$.

Prova. Temos que $\tau F_t(\underline{V}) = F_t(\underline{V}), \forall \tau \in H$. Se fosse $\tau F_t(\underline{V}) = F_t(\underline{V})$, para algum $\tau \notin H$, então $F_t(\underline{V})$ seria um zero repetido de $R(F, f)$, uma contradição. ■

A resolvente $R(F, f)$ pode ser construída pela sua expansão simbolicamente nos zeros de $f(x)$. Daí, com o auxílio do Teorema Fundamental dos Polinômios Simétricos, seus coeficientes são determinados em termos dos coeficientes de $f(x)$. Infelizmente, a não ser que $\partial R(F, f)$ seja pequeno ou $f(x)$ seja esparso (possua poucos coeficientes não-nulos), isto leva a uma manipulação simbólica demasiadamente extensa. Entretanto, se usamos este método, obtemos uma fórmula explícita para os coeficientes de $R(F, f)$ em termos dos coeficientes de $f(x)$. No Capítulo 4, descreveremos um algoritmo exato para construir resolventes lineares. Este algoritmo não expande a resolvente simbolicamente nos zeros de $f(x)$. Sejam $K = \mathbb{Q}$, $f(x) \in \mathbb{Z}[x]$ mônico e $F \in \mathbb{Z}[x_1, \ldots, x_n]$. Então os coeficientes de f são inteiros. Assim, se formarmos $R(F, f)$ usando aproximações
números para os zeros de $f(x)$ e soubermos que a exatidão dessas aproximações é tal que os coeficientes de $R(F, f)$ são calculados com um erro absoluto menor que $1/2$, então podemos determiná-los exatamente por arredondamento. Stauduhar usa este método logo abaixo. Na Seção 5.1 discutiremos uma aproximação modular para o cálculo de $R(F, f)$ quando F e $f(x)$ são como no parágrafo precedente. Assumiremos que existe um algoritmo de fatoração sobre $K[x]$. Na prática, para $K = \mathbb{Q}$, $f(x) \in \mathbb{Z}[x]$ mônico e $F \in \mathbb{Z}[x_1, \ldots, x_n]$, pode-se determinar candidatos a fatores de $R(F, f)$ por uso de aproximações números para os zeros de $f(x)$.

2.4 Funções pertencentes a grupos

Sejam $F \in K[x_1, \ldots, x_n]$ e $G = stab_{S_n}(F)$. Neste caso, dizemos que F *pertence* a G. Em particular, a função alternada $D[x_1, \ldots, x_n]$ pertence a A_n. Note que para $\sigma \in S_n$, $\sigma * F$ pertence a $\sigma^{-1}G\sigma$ e, além disso, $\sigma(\underline{V}) * F$ é um zero de $R(F, f)$. Aplicando a Proposição 2.2, vemos que se $Gal(f/K) \leq \sigma^{-1}G\sigma$, para algum $\sigma \in S_n$, então $R(F, f)$ possui um fator linear. Reciprocamente, se $R(F, f)$ possui um fator linear não repetido, então $Gal(f/K)$ está contido em algum conjugado de G. Embora fatores lineares sejam fáceis de se encontrar, os mesmos podem fornecer informação apenas sobre a inclusão de $Gal(f/K)$ em um grupo e seus conjugados. A fatoração completa de uma resolvente escolhida adequadamente muitas vezes distingue $Gal(f/K)$ dentre muitos possíveis can-

didatos.

Proposição 2.3 *Sejam K corpo, com $Char(K) \neq 2, f(x) \in K[x]$ um polinômio irredutível, separável, com $\partial f = n > 0$, zeros distintos $v_1, \ldots, v_n$ e $\underline{V} = (v_1, \ldots, v_n)$ uma ordenação dos mesmos. Tem-se $Gal(f/K) \leq A_n$ se, e somente se, $disc(f) = k^2$, com $k \in K^*$.*

Prova. Considere $R(D, f)$, onde $D = D(\underline{V})$ é a função alternada. Tem-se

$$R(D, f)(x) = (x - D(\underline{V}))(x + D(\underline{V})) = x^2 - (D(\underline{V}))^2 = x^2 - disc(f).$$

Como os v_i são distintos, então $disc(f) \neq 0$ e como $Char(K) \neq 2$ temos que $R(D, f)$ possui zeros distintos. Por hipótese,

$$Gal(f/K) \leq A_n = stab_{S_n}(D)$$

e sabemos que $A_n = \sigma^{-1} A_n \sigma, \forall \sigma \in S_n$. Assim, $R(D, f)$ possui um fator linear não repetido e então $h(x) = x - \sqrt{disc(f)} \in K[x]$. Logo, $\sqrt{disc(f)} \in K^*$, ou seja, $disc(f) = k^2, k \in K^*$. Reciprocamente, considere novamente $R(D, f) = x^2 - disc(f)$. Por hipóte-se, $disc(f) = k^2$, com $k \in K^*$. Daí, $R(D, f) = (x - k)(x + k)$. Como $Char(K) \neq 2$ temos que $h_1(x) = x - k \neq x + k = h_2(x)$ e assim $R(D, f)$ possui um fator linear não repetido sobre K. Logo, $Gal(f/K) \leq \sigma^{-1} stab_{S_n}(D)\sigma$, para algum $\sigma \in S_n$. Mas $stab_{S_n}(D) = A_n$ e $\sigma^{-1} A_n \sigma = A_n, \forall \sigma \in S_n$. Daí, temos o resultado desejado. ■

2.5 O método de Stauduhar

Stauduhar em [12] descreve um método eficaz para a determinação do grupo de Galois sobre $\mathbb{Q}$ de um polinômio mônico irredutível $f(x) \in \mathbb{Z}[x]$. Ele descreve a implementação deste método para $n = \partial f \leq 8$ e fornece tabelas com informações necessárias para esta implementação. Seja $\underline{V} = (v_1, \ldots, v_n)$ uma ordenação dos zeros de $f(x)$ e suponha que com respeito a esta ordenação, sabemos que $Gal(f/\mathbb{Q}) \leq G$ (inicialmente sabemos que $Gal(f/\mathbb{Q}) \leq S_n$). Se G não possui subgrupos próprios transitivos, então $Gal(f/\mathbb{Q}) = G$. Caso contrário, verificamos se $Gal(f/\mathbb{Q}) \leq H$, para cada subgrupo maximal transitivo H de G. Para H um subgrupo maximal transitivo de G, verificamos se $Gal(f/\mathbb{Q}) \leq \sigma H \sigma^{-1}$, para algum $\sigma \in G$. Escolha (de uma tabela) um polinômio $F \in \mathbb{Z}[x_1, \ldots, x_n]$ tal que

$stab_G(F) = H$ e considere o fator de $R(F, f)$:

$$R_G(F, f) = \prod_{i=1}^{k} (x - F_i(\underline{V})),$$

onde $F_i = \sigma_i * F$ $(i = 1, \ldots, k, F_1 \neq \cdots \neq F_k)$, $\{\sigma_1, \ldots, \sigma_k\}$ um conjunto de representantes das classes laterais à esquerda de H em G (obtidos de uma tabela). Como $Gal(f/\mathbb{Q}) \leq G$ temos que cada elemento de $Gal(f/\mathbb{Q})$ induz uma permutação dos F_i. Daí, os coeficientes de $R_G(F, f)$ são inteiros, os quais são determinados por expansão de $R_G(F, f)$ usando aproximações de alta precisão para os zeros de $f(x)$ e depois arredondando os coeficientes aproximados de $R_G(F, f)$. Se $Gal(f/\mathbb{Q})$ está contido em algum conjugado de H em G, então $R_G(F, f)$ possui um zero inteiro. Reciprocamente, se $R_G(F, f)$ possui um zero inteiro não repetido, então $Gal(f/\mathbb{Q})$ está contido em algum conjugado de H em G. Testamos cada zero aproximado z de $R_G(F, f)$ que aparenta ser inteiro para determinar se $R_G(F, f)(round(z)) = 0$. Suponha que $R_G(F, f)$ possui um zero inteiro não repetido $\sigma(\underline{V}) * F, \sigma \in G$. Então $Gal(f/\mathbb{Q}) \leq \sigma^{-1} H \sigma$. Podemos reordenar os zeros de $f(x)$ pela troca de $\underline{V}$ por $(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$ e, com respeito a esta ordenação, $Gal(f/\mathbb{Q}) \leq H$. Se $Gal(f/\mathbb{Q})$ não está contido em nenhum subgrupo maximal transitivo de G, então $Gal(f/\mathbb{Q}) = G$. Caso contrário, temos determinado que $Gal(f/\mathbb{Q}) \leq H$ com respeito à ordenação $\underline{V}$, onde H é um subgrupo maximal transitivo de G. Podemos então trocar G por H e repetir o processo inteiro. O método de Stauduhar é prático e direto. Entretanto, aproximações altamente precisas dos zeros de $f(x)$ são necessárias e deve-se ter muitas informações úteis tabeladas. Outrossim, uma inspeção no reticulado de $Sub(S_n)$ deve ser feita, pois se uma função F pertence a G, então F é fixada pelos elementos de qualquer subgrupo de G.

2.6 O uso de resolventes lineares

Seja $f(x) \in K[x]$ um polinômio separável, com $\partial f = n > 1$ e zeros $v_1, \ldots, v_n$ e corpo de decomposição N. Seja o multiconjunto $M = [e_1, \ldots, e_r]$, onde $e_i \in K$ e $0 < r \leq n$. Denominamos r de *comprimento* de M. Podemos também escrever

$$M = [a_1^{m_1}, \ldots, a_k^{m_k}],$$

onde $a_1 \neq \cdots \neq a_k$ e $m_i > 0$ é a *multiplicidade* de a_i em M, com $i = 1, \ldots, k$. Lembremos que a resolvente linear $LR(M, f)$ associada a M e $f(x)$ é a resolvente $R(F, f)$, onde

$F = e_1x_1 + \cdots + e_rx_r$. Se, por acaso, algum e_i é nulo, será considerado como simbólico ocupante da posição i. Temos que $\partial(LR(M,f))$ é o número de maneiras de escolher r objetos dentre n vezes o número de permutações distintas dos elementos de M. Assim,

$$\partial(LR(M,f)) = \binom{n}{r}\frac{r!}{m_1!\cdots m_k!} = \frac{n!}{(m_1!\cdots m_k!)(n-r)!}. \tag{2.1}$$

Resolventes lineares formam uma classe geral de resolventes úteis, para qualquer grau de $f(x)$. Freqüentemente, a fatoração de resolventes lineares de grau relativamente baixo, pode ser usada para determinar $Gal(f/K)$ exatamente. Um grupo de permutações $G \leq S_n$ age sobre os $r-$conjuntos contidos em $\{1,\ldots,n\}$, onde a ação é definida por $\sigma * \{i_1,\ldots,i_r\} = \{\sigma(i_1),\ldots,\sigma(i_r)\}, \forall\sigma \in G$. É claro que a ação de G sobre $S_n * F$, onde $F = x_1 + \cdots + x_n$, é equiva-lente à ação de G sobre os $r-$conjuntos de $\{1,\ldots,n\}$. Assim, a fatoração de $LR([1^r,f])$ (com zeros distintos) determina a partição do comprimento das órbitas de $S_n * \{1,\ldots,r\}$ sob a ação de $Gal(f/K)$. McKay e Erbach em [4, 10] sugerem o uso de resolventes desta forma a fim de determinar a transitividade sobre os $r-$ conjuntos de $Gal(f/K)$. A seguinte observação é de interesse: Suponhamos que $f(x)$ é irredutível (nesse caso, $Gal(f/K)$ é transitivo) e $n = rs, s \in \mathbb{N}, s \neq 1, n$. Então $LR([1^r,f])$ (com zeros distintos) tem t fatores irredutíveis de grau s se, e somente se, $Gal(f/K)$ tem t sistemas de imprimitividade de s blocos de tamanho r. Um grupo de permutações $G \leq S_n$ age sobre o conjunto das $r-$ seqüências $(i_1,\ldots,i_r)$, com $i_j \in \{1,\ldots,n\}$ e os i_j distintos $(j = 1,\ldots,r)$. Esta ação é definida por

$$\sigma * (i_1,\ldots,i_r) = (\sigma(i_1),\ldots,\sigma(i_r)), \forall\sigma \in G.$$

É claro que a ação de G sobre $S_n * F$, onde $F = e_1x_1 + \cdots + e_nx_r$, com $e_1 \neq \cdots \neq e_r$, é equivalente à ação de G sobre as r-seqüências de $\{1,\ldots,n\}$. Agora, suponhamos que

$$LR(M,f) = LR([e_1,\ldots,e_r],f)$$

tem zeros distintos e $e_1 \neq \cdots \neq e_r$. Tem-se $LR(M,f)$ redutível se, e somente se, $Gal(f/K)$ não é $r-$transitivo. Também existe uma interpretação referente à teoria dos corpos simples para a fatoração deste $LR(M,f)$. Seja $z = e_1v_{\sigma(1)} + \cdots + e_rv_{\sigma(r)}$ um zero de $LR(M,f)$ $(\sigma \in S_n)$. Vemos que

$$stab_{G(N/K)}(z) = \bigcap_{i=1}^{r} stab_{G(N/K)}v_{\sigma(i)}$$

e daí, pelo Lema 2.3, $K(z) = K(v_{\sigma(1)},\ldots,v_{\sigma(r)})$. Os graus dos fatores irredutíveis de $LR(M,f)$ correspondem aos graus sobre K dos subcorpos não-conjugados de N gerados

pelos $r-$conjuntos dos zeros de $f(x)$. Em particu-lar, note que se $r = 2$ e $f(x)$ é irredutível, então $LR(M, f)$ tem todos os fatores irredutíveis de grau n se, e somente se, $N = K(v_i)$, para cada v_i zero de $f(x)$, pois, neste caso, $K(v_i) = K(v_j), \forall i, j = 1, \ldots, n$. Também note que se $r = n$, então $\partial(LR(M, f)) = n!$ e $N = K(z)$, para cada z zero de $LR(M, f)$. As partições dos comprimentos das órbitas de $r-$conjuntos e $2-$seqüências sob a ação dos grupos de permutações transitivos de graus $3, 4, 5, 6, 7$, encontram-se, respectivamente, abaixo das tabelas A.2, A.4, A.6, A.8, A.11 do Apêndice. Para $f(x)$ irredutível, essas tabelas são usadas para determinar candidatos a $Gal(f/K)$, dada a fatoração de uma resolvente linear que determina o comprimento das órbitas de $Gal(f/K)$ sobre $r-$conjuntos ou $2-$seqüências.

2.7 A diferenciação de todos os grupos transitivos de grau ≤ 7

Suponhamos $Char(K) \neq 2$. Se $Gal(f/K)$ é transitivo e sabemos de $disc(f)$ se o mesmo é ou não subgrupo de A_n, então para $n = 3, 4, 5, 7$ as classes de conjugação de $Gal(f/K)$ são determinadas completamente pelo comprimento das órbitas da ação de $Gal(f/K)$ sobre $2-$conjuntos, $3-$conjuntos e $2-$ seqüências, com a excessão da distinção entre os grupos $5T3$ e $5T5$ (cf abaixo da Tabela A.6 do Apêndice). O grupo $5T3$ pode ser distinguido do grupo $5T5(= S_5)$ da seguinte maneira. Tome

$$f = (x_1 + x_2 - x_3 - x_4)^2$$

e note que

$$R(F, f)(x^2) = LR([1^2, -1^2], f)(x).$$

Use esta resolvente linear para calcular $R(F, f)$. Para $\partial f = 5$, tem-se $\partial(R(F, f)) = 15$ e a partição do comprimento das órbitas de $S_5 * F$ sob a ação de $5T3$ é $(10, 5)$. Para $n = 6$, todos os grupos transitivos podem ser diferenciados por $disc(f)$ e pela ação sobre $2-$conjuntos, $3-$conjuntos e $2-$ seqüências, exceto a distinção entre os grupos $T8$ e $T11$, $T9$ e $T13$, $T14$ e $T16$ (cf. após geradores de grupos para a Tabela A.7 do Apêndice). Para distinguir estes grupos, pode-se usar técnicas ad hoc ou o Método de Stauduhar, se $K = \mathbb{Q}$. Esboçaremos resumidamente uma técnica ad hoc adequada. Assumiremos que todos os polinômios em discussão têm zeros distintos. Seja $D = disc(f)$, com $\sqrt{D} \notin K$

e $d(x) = x^2 - D$. Se estivermos trabalhando sobre $\mathbb{Z}$, podemos tomar D como sendo a parte livre de quadrado (D não é divisível por nenhum primo ao quadrado) de $disc(f)$. Seja $r(x) \in K[x]$ um fator mônico irredutível de uma resolvente $R(F, f)$. Suponhamos $r(F_t(\underline{V})) = 0$ para alguma ordenação $\underline{V}$ dos zeros de $f(x)$ e $F_t \in S_n * F$. As seguintes condições são equivalentes:

(1) $stab_{Gal(f/K)}(F_t) \leq A_n$;

(2) $K(\sqrt{D}) \subseteq K(F_t(\underline{V}))$;

(3) $SZ(r(x), d(x))$ tem um fator sobre K de grau ∂r (cf. Seção 4.2 para uma explanação de SZ).

Agora, suponhamos $n = 6$. Suponhamos $Gal(f/K) = T8$ ou $T11$. Seja $r(x) \in K[x]$ o fator mônico irredutível de $LR([1^3], f)$, com $\partial r = 12$. Então $Gal(f/K) = T8$ se, e somente se, $SZ(r(x), d(x))$ tem um fator (sobre K) de grau 12. Suponhamos $Gal(f/K) = T9$ ou $T13$. Seja $r(x) \in K[x]$ o fator mônico de $LR([1^3], f)$, com $\partial r = 2$. Então $Gal(f/K) = T9$ se, e somente se, $SZ(r(x), d(x))$ tem um fator de grau 2. Suponhamos $Gal(f/K) = T14$ ou $T16$. Seja $r(x) = LR([1^3], f)$. Então $Gal(f/K) = T14$ se, e somente se, $SZ(r(x), d(x))$ tem um fator de grau 20.

Capítulo 3

Construção de resolventes lineares

Neste capítulo descreveremos um algoritmo para construir qualquer resolvente linear sobre um corpo K sujeito às restrições da Seção 4.1. O algoritmo é exato, usa resultantes de polinômios e não expande a resolvente simbolicamente nos zeros de $f(x)$. Este avanço foi inspirado em Trager [13], que usou resultantes polinomiais de maneira semelhante para fatorar polinômios sobre corpos de extensões algébricas.

A utilidade da resolvente linear na calculação de $Gal(f/K)$ quando temos um algoritmo de fatoração sobre $K[x]$ foi discutida na Seção 3.3.5.

3.1 Restrições sobre o corpo

O algoritmo da resolvente linear tem o propósito de trabalhar sobre um corpo K que obedeça às seguintes restrições:

Se $Char(K) \neq 0$, então exige-se que $Char(K) > D$, onde D é o grau máximo de qualquer polinômio usado ou construído pelo algoritmo principal ou qualquer sub-algoritmo. Se $Char(K) \neq 0$, então $Char(K) > D$ se, e somente se, $Char(K) \nmid D!$.

Se K é finito, precisamos de $|K|$ grande o suficiente para construir os polinômios exigidos por interpolação. Para esta exigência, $|K| > 2D$ é suficiente. Note que o nosso interesse não é encontrar o grupo de Galois de um polinômio sobre um corpo finito (tal grupo de Galois é sempre cíclico) e sim o de podermos usar resolventes sobre corpos finitos em um algoritmo modular (cf. Capítulo 5).

3.2 Operações polinomiais

Nesta seção descreveremos nossas operações básicas nos polinômios sobre K. Usaremos estas operações no algoritmo da resolvente linear.

Definição 3.1 *Sejam $f = f(x), g = g(x) \in K[x] - \{0\}$. O $MDC(f, g)$ é definido como sendo o polinômio mônico em $K[x]$ de maior grau que divide $f(x)$ e $g(x)$.*

Se $\partial g > 0$, então, pelo Algoritmo da Divisão, existem únicos $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x)g(x) + r(x), \text{ onde } r = 0 \text{ ou } \partial r < \partial g.$$

Denotaremos este $r(x)$ por $f \mod g$. Como qualquer divisor comum de f e g divide $f \mod g$, podemos usar a seguinte formulação recursiva para encontar $MDC(f, g)$:

Se $f \mod g$ é o polinômio nulo, então $MDC(f, g) = \frac{1}{c}g(x)$, onde c é o coeficiente líder de $g(x)$; se $\partial g = 0$, então $MDC(f, g) = 1$; caso contrário, $MDC(f, g) = MDC(g, f \mod g)$.

Seja e um inteiro não-negativo e seja N o corpo de decomposição de $f(x)$ sobre K. Dizemos que $f(x)$ possui um zero v de *multiplicidade* e se $(x - v)^e \mid f(x)$ mas $(x - v)^{e+1} \nmid f(x)$ em $N[x]$. Escrevemos $e = mult(v, f)$. No caso em que $e = 1$, dizemos que v é *raiz simples* de $f(x)$.

Note que $MDC(f, g)$ sobre qualquer extensão L de K é o mesmo que $MDC(f, g)$ sobre K. Isto ocorre porque o algoritmo para calcular $MDC(f, g)$ sobre K é exatamente o mesmo sobre L. Em particular, para L o corpo de decomposição de $f(x)g(x)$, os zeros de $MDC(f, g)$ são os zeros comuns a f e g e se v é um zero de $MDC(f, g)$, então

$$mult(v, MDC(f, g)) = \min\{mult(v, f), mult(v, g)\}.$$

3.3 A resultante

Sejam $f = f(x)$, $g = g(x)$ polinômios em $K[x]$. Sejam

$$f(x) = a(x - v_1) \cdots (x - v_n) \text{ e } g(x) = b(x - w_1) \cdots (x - w_m)$$

sobre o corpo de decomposição de $f(x)g(x)$. Além disso, assumimos que $n = \partial f > 0$ e $m = \partial g$.

Discorreremos sobre a resultante de maneira semelhante a Childs [2, p. 283]. Confira também Collins [3].

Definição 3.2 *A* resultante *de* $f(x)$ *e* $g(x)$*, denotada por* $res(f,g)$*, é dada por*

$$res(f,g) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(v_i - w_j).$$

A resultante é uma função simétrica dos v_i e w_j, daí $res(f,g)$ é um elemento de K. Os seguintes fatos são conseqüências imediatas da definição:

(1) $res(f,g) = (-1)^{mn} res(g,f)$;

(2) $res(f,g) = a^m \prod_{i=1}^{n} g(v_i)$;

(3) Se $m = 0$, então $res(f,g) = b^n$.

Para nossos propósitos, é conveniente assumir que $\partial 0 = 0$, de modo que em (3) não excluímos a possibilidade de que $b = 0$. Usaremos (1) e (2) para provar o lema seguinte.

Lema 3.1 *Suponhamos* $m > 0$ *e seja* $r(x) = f \mod g$*. Então*

$$res(f,g) = (-1)^{mn} b^{n-\partial r} res(g,r).$$

Prova.

$$\begin{aligned} res(f,g) &= (-1)^{mn} res(g,f) = (-1)^{mn} b^n \prod_{i=1}^{n}(g(w_i)q(w_i) + r(w_i)) \\ &= (-1)^{mn} b^n \prod_{i=1}^{n} r(w_i) = (-1)^{mn} b^{n-\partial r} res(g,r). \end{aligned}$$

■

Combinando (3) e o Lema 3.1, temos uma formulação recursiva de $res(f,g)$ semelhante à formulação recursiva de $MDC(f,g)$. Esta formulação é usada para calcular $res(f,g)$ eficientemente. Pode-se também calcular $res(f,g)$ ou $MDC(f,g)$ não recursivamente por uso de uma seqüência de restos polinomiais.

3.4 A derivada formal e seus zeros

A derivada formal de um polinômio sobre um corpo K é semelhante à derivada usual de um polinômio real, possuindo muitas propriedades análogas a esta.

Definição 3.3 *Seja* $f(x) = \sum_{i=0}^{n} a_i x^i$ *um polinômio sobre* K. *A* derivada formal de $f(x)$, *denotada por* f' *ou* $f'(x)$, *é dada por*

$$f' = f'(x) = \sum_{i=1}^{n} i a_i x^{i-1},$$

onde ia_i *significa* $a_i + \cdots + a_i$ (i *vezes*).

Existe uma importante relação entre a multiplicidade dos zeros de $f(x)$ e os zeros de $f'(x)$, a qual estabeleceremos na seguinte proposição:

Proposição 3.1 *Suponhamos que* $f(x)$ *possui um zero* v *de multiplicidade* $e > 0$. *Se* $Char(K) \nmid e$, *então* $mult(v, f') = e - 1$.

Prova. Por hipótese, $f(x) = (x-v)^e h(x)$. Então, $f'(x) = e(x-v)^{e-1}h(x) + (x-v)^e h'(x)$. Assim, $mult(v, f') \geq e - 1$. Agora, se $(x - v)^e \mid f'(x)$, então $(x - v) \mid eh(x)$. Isto não pode acontecer pois, como $Char(K) \nmid e$, então $e \neq 0$ e pela definição de multiplicidade, $(x - v) \nmid h(x)$. Daí, $mult(v, f') < e$. Portanto, $mult(v, f') = e - 1$. ■

Corolário 3.1 *Suponhamos* $Char(K) > n$. *Para todo zero* v *de* $f(x)$ *de multiplicidade* $e > 1, v$ *é um zero de* $MDC(f, f')$ *de multiplicidade* $e-1$ *e* $MDC(f, f')$ *não possui outros zeros.* ■

3.5 Polinômios "zeros múltiplos" e "zeros da soma"

Sejam $f(x) \in K[x]$ um polinômio mônico, $n = \partial f$, $v_1, \ldots, v_n$ seus zeros e $d \in K$. Queremos encontrar o polinômio mônico de grau n com zeros $dv_1, \ldots, dv_n$. Tal polinômio é denotado por $MZ(d, f)$ (Múltiplos de Zeros) e é dado pela seguinte expressão:

$$MZ(d, f) = \begin{cases} d^n f(\frac{x}{d}), & \text{se } d \neq 0 \\ x^n, & \text{se } d = 0. \end{cases}$$

Sejam $f = f(x)$, $g = g(x) \in K[x]$ polinômios mônicos tais que

$$f(x) = (x - v_1) \cdots (x - v_n) \text{ e } g(x) = (x - w_1) \cdots (x - w_m)$$

sobre o corpo de decomposição de $f(x)g(x)$. Queremos encontrar o polinômio mônico em $K[x]$ de grau mn com zeros

$$v_i + w_j, i = 1, \ldots, n, j = 1, \ldots, m.$$

Tal polinômio é denotado por $SZ(f,g)$ (Somas de Zeros).

Note que na equação 3.1 abaixo, tanto o membro esquerdo quanto o membro direito são polinômios mônicos de grau mn tendo os mesmos zeros:

$$SZ(f,g) = \prod_{i=1}^{n} g(x - v_i) \tag{3.1}$$

Assim, para qualquer $y \in K$, conhecemos o valor de $SZ(f,g)(y)$. O mesmo é dado por:

$$SZ(f,g)(y) = (-1)^{mn} res(f(x), g(y-x)). \tag{3.2}$$

Se $|K|$ é suficientemente grande, podemos calcular $z_i = SZ(f,g)(y_i)$, usando 3.2, para $i = 1, 2, \ldots, mn+1$ e $y_i \in K$ distintos. Então podemos determinar $SZ(f,g)$ por interpolação. Isto é, encontramos o polinômio $t(x) = SZ(f,g)$, com $\partial t \leq mn$ tal que $t(y_i) = z_i$, $i = 1, 2, \ldots, mn+1$. Para algoritmos de interpolação, o leitor interessado deve consultar [3, 7].

3.6 Raiz polinômio

Finalmente, precisamos de um algoritmo para resolver o seguinte problema. Sejam $k \in \mathbb{N}$ e $u(x) \in K[x]$ um polinômio mônico com $\partial u > 0$. Se existir $r(x) \in K[x]$ mônico tal que $u(x) = r(x)^k$, denotamos este $r(x)$, que é único, por $PR(k,u)$ (raiz polinômio). Encontramos $PR(k,u)$ usando o algoritmo POLYROOT, que segue. Assumimos que $Char(K) > \partial u$ ou $Char(K) = 0$.

Algoritmo POLYROOT

Entrada:

$k \in \mathbb{N}$ e $u(x) \in K[x]$ mônico, $\partial u > 0$, tal que $u(x) = r(x)^k$, para algum polinômio mônico $r(x) \in K[x]$.

Saída:

$PR(k,u)$ $(= r(x))$.

(1) Se $k = 1$, então $PR(k,u) = u(x)$ e Fim.

(2) Faça $t(x) \leftarrow \frac{u(x)}{MDC(u(x),u'(x))}$, $t(x)$ é separável e seus zeros são precisamente os zeros distintos de $u(x)$, pelo Corolário 3.1.

(3) Faça $r(x) \leftarrow t(x)$ e $s(x) \leftarrow u(x)$;

(4) Quando $\partial r < \frac{\partial u}{k}$, execute os seguites passos:

(4.1) Faça $s(x) \leftarrow \frac{s(x)}{t(x)^k}$;

(4.2) Faça $t(x) \leftarrow MDC(s,t)$; até a i-ésima iteração deste "loop", os zeros de $t(x)$ são precisamente os zeros distintos v de $u(x)$ tais que $mult(v,u) > i$;

(4.3) Faça $r(x) \leftarrow t(x)r(x)$;

(5) Retorne $r(x)$ e Fim.

3.7 Operações com multiconjuntos

Definiremos as operações $+$ e $-$ para multiconjuntos. Elas são semelhantes, respectivamente, à união e diferença de conjuntos, exceto o fato de que as multiplicidades são contadas. Usaremos estas operações na prova seguinte e no algoritmo da resolvente linear. A multiplicidade do elemento e no multiconjunto M será denotada por $mult(e, M)$.

Sejam M, N multiconjuntos e seja e um elemento do conjunto "universo" do qual M e N extraem seus elementos. Então $M + N$ é um multiconjunto e

$$mult(e, M + N) = mult(e, M) + mult(e, N).$$

Também $M - N$ é um multiconjunto e

$$mult(e, M - N) = mult(e, M) - mult(e, N),$$

se $mult(e, M) > mult(e, N)$ e $mult(e, M - N) = 0$, caso contrário.

3.8 Prova construtiva

Sejam K um corpo satisfazendo às restrições descritas na Seção 3.1, $f(x) \in K[x]$ um polinômio mônico, com $n = \partial f > 0$ e zeros $v_1, \ldots, v_n$. Sejam $e_1, \ldots, e_r \in K, 0 < r \leq n$ e $M = [e_1, \ldots, e_r]$ um multiconjunto. Nós agora provaremos a

Proposição 3.2 *A resolvente linear $LR(M, f)$ pode ser construída sobre K usando apenas as operações MZ, SZ e PR.*

Prova. Usaremos indução sobre r, o comprimento de M.

i) Se $r = 1$, então $LR(M, f) = MZ(e_1, f)$;

ii) Suponhamos $r > 1$ e que o resultado seja válido para todo s, com $1 \leq s < r$. Seja

$$\overline{M} = [e_1, \ldots, e_{r-1}] = [a_1^{m_1}, \ldots, a_k^{m_k}],$$

onde $a_1, \ldots, a_k$ são distintos e $m_i = mult(a_i, \overline{M}) > 0$, para $i = 1, \ldots, k$. Por hipótese de indução, podemos calcular

$$t(x) = SZ(LR(\overline{M}, f), MZ(e_r, f)).$$

Para cada zero w de $LR(\overline{M}, f)$, $t(x)$ tem precisamente os zeros $w+e_rv_1, \ldots, w+e_rv_n$. Assim, temos que

$$t(x) = (\prod_{i=1}^{k} LR(M_i, f)^{c_i}) LR(M, f)^c,$$

onde

$$M_i = (\overline{M} - [a_i]) + [a_i + a_r], c_i = m_i \partial(LR(\overline{M}, f))/\partial(LR(M_i, f))$$

e

$$c = (n - r + 1)\partial(LR(\overline{M}, f))/\partial(LR(M, f)).$$

Podemos calcular c_i e c usando a expressão 2.1 para o grau de uma resolvente linear. De fato, por cálculos diretos envolvendo estas expressões, vê-se que $c_i = mult(a_i + e_r, M_i)$ e $c = mult(e_r, M)$. Por hipótese, podemos construir

$$s(x) = \prod_{i=1}^{k} LR(M_i, f)^{c_i}.$$

Então a resolvente linear desejada pode ser obtida por

$$LR(M, f) = PR(c, t(x)/s(x)).$$

3.9 Algoritmo LINRESOLV

Sejam K um corpo satisfazendo às restrições estabelecidas na Seção 4.1, $f(x) \in K[x]$ um polinômio mônico, com $n = \partial f > 0$ e zeros $v_1, \ldots, v_n$. Sejam $e_1, \ldots, e_r \in K, 0 < r \leq n$ e $M = [e_1, \ldots, e_r]$ um multiconjunto.

A prova indutiva da Seção precedente motiva nosso algoritmo recursivo para construir $LR(M, f)$, a resolvente linear associada a M e $f(x)$. Algumas mudanças, com relação ao

método da prova, foram feitas, por considerações de eficiência. O algoritmo é denominado LINRESOLV e é detalhado a seguir:

Algoritmo LINRESOLV

Entrada:

Um polinômio mônico $f(x) \in K[x]$, com $\partial f = n > 0$ e um multiconjunto $M = [e_1, \ldots, e_r]$, $0 < r \leq n$, onde $e_1, \ldots, e_r \in K$.

Saída:

$LR(M, f)$, a resolvente linear associada a M e $f(x)$.

(1) Se qualquer um dos elementos de M é igual a 0 (a identidade aditiva de K) então estes zeros são significativos como simbólicos ocupantes de posição. Entretanto, esta peculiaridade nos permite que $LR(M, f)$ seja determinada considerando apenas o submulticonjunto maximal que contém apenas elementos não-nulos:

(1.1) Faça $m \leftarrow mult(0, M)$;

(1.2) Se $m = 0$, então vá ao passo (2);

(1.3) Se $m = r$, então faça $t(x) \leftarrow$ "x" e vá ao passo (1.6);

(1.4) Faça $\overline{M} \leftarrow M - [0]^m$;

(1.5) Faça $t(x) \leftarrow LR(\overline{M}, f)$ (aplicação recursiva deste algoritmo);

(1.6) Faça $d \leftarrow \binom{n-r+m}{m}$, retorne $t(x)^d$ e Fim.

(2) Se $r = 1$, retorne $t(x)^d$ e Fim.

(3) Arranje os elementos de M de modo que $mult(e_r, M) \leq mult(e_i, M)$, para $i = 1, \ldots, r$. Isto assegura que o grau do polinômio construído no passo (4.2) seja o menor possível.

(4.1) Faça $\overline{M} \leftarrow [e_1, \ldots, e_{r-1}]$, $(= [a_1^{m_1}, \ldots, a_k^{m_k}]$, onde $a_1, \ldots, a_k$ são distintos e $m_i > 0$, para $i = 1, \ldots, k.)$;

(4.2) Faça $u(x) \leftarrow LR(\overline{M}, f)$ (uso recursivo deste algoritmo);

(5) Faça $s(x) \leftarrow \prod_{i=1}^{k} \Pi LR(M_i, f)^{c_i}$, onde $M_i = (\overline{M} - [a_i]) + [a_i + e_r]$ e $c_i = mult(a_i + e_r, M_i)$ (uso recursivo deste algoritmo);

(6.1) Faça $c \leftarrow mult(e_r, M), g(x) \leftarrow MZ(e_r, f)$;

(6.2) Tome d como sendo um inteiro positivo tal que para todo $b = a^c$, para algum $a \in K$,

i. a^d é único em K, para todas as soluções $a \in K$ de $b = a^c$ e

ii. podemos calcular eficientemente este a^d.

iii. Podemos sempre tomar $d = c$. Entretanto, é mais eficiente escolher d tanto menor quanto possível. Por exemplo, quando $K = \mathbb{Q}$: se c é ímpar, então tome $d = 1$ e a^d é a única c-ésima raiz em $\mathbb{Q}$ de b; se c é par, então tome $d = 2$ e a^d é a única $(c/2)$-ésima raiz em $\mathbb{Q}$ de b;

(6.3) Faça $m \leftarrow d(\partial u \partial g - \partial s)/(c+1)$, $m = \partial(LR(M,f)^d) + 1$;

(6.4) Para m distintos $y_i \in K$, $i = 1, \ldots, m$, tais que $s(y_i) \neq 0$, faça $z_i \leftarrow res(u(x), g(y_i - x))/s(y_i)$. Aqui é onde precisamos assumir que $|K|$ é "grande o suficiente" $z_i = SZ(u,g)(y_i)/s(y_i) = (LR(M,f)(y_i))^c$;

(6.5) Para cada z_i, sabemos que $z_i = a_i^c$, para algum $a_i \in K$. $a_i = LR(M,f)(y_i)$. Para $i = 1, \ldots, m$, faça $z_i = a_i^d$. Podemos fazer isto devido à escolha de d como explanado no passo (6.2);

(7) Tome $t(x)$ como sendo o polinômio de grau $m-1$ tal que $t(y_i) = z_i$, para $i = 1, \ldots, m$, usando um algoritmo de interpolação;

(8) Retorne $PR(d,t)$ e Fim.

3.10 Observações

À medida que r cresce, a eficiência do algoritmo LINRESOLV decresce notadamente. Entretanto, na prática, r é geralmente pequeno; freqüentemente $r \leq 3$. Para um corpo K dado, obsrevações empíricas podem ser feitas a fim de determinar o tamanho prático para r e n.

Quando o algoritmo LINRESOLV é usado para calcular uma certa resolvente linear, o mesmo deve, geralmente, calcular outras resolventes acessórias, recursivamente. Se estas são úteis, deveriam ser salvas. Por exemplo, para calcular $LR([1^3], f)$, LINRESOLV tem que calcular também $LR([1^2], f)$ e $LR([1,2], f)$.

Capítulo 4

Implementação e Exemplos

Ao longo deste capítulo, vale o seguinte:

$$f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i} \in \mathbb{Z}[x],$$

com zeros $v_1, \ldots, v_n$ e $M = [e_1, \ldots, e_r]$, com $e_i \in \mathbb{Z}$, $0 < r \leq n$.

Discutiremos nosso algoritmo modular para calcular $LR(M, f)$ e a implementação deste algoritmo no computador. Damos exemplos de determinação de grupos de Galois sobre $\mathbb{Q}$, usando esta implementação.

4.1 Uma aproximação modular para o cálculo de resolventes

Seja $S(x_1, \ldots, x_n)$ um polinômio simétrico sobre $\mathbb{Z}$ e $p \in \mathbb{N}$ primo. Pelo Teorema dos Polinômios Simétricos,

$$S = T(s_1, \ldots, s_n),$$

para um único $T \in \mathbb{Z}[x_1, \ldots, x_n]$, onde s_i, $i = 1, \ldots, n$, é o i-ésimo polinômio simétrico elementar. Suponhamos que

$$f(x) \mod p = x^n + \sum_{i=1}^{n} \overline{a}_i x^{n-i}$$

possui zeros $\overline{v}_1, \ldots, \overline{v}_n$ e sejam

$$\overline{S} = S \mod p, \overline{T} = T \mod p.$$

Então, sobre $\mathbb{Z}_p$:

$$\overline{S}(\overline{v}_1, \ldots, \overline{v}_n) = \overline{T}(-\overline{a}_1, \overline{a}_2, \ldots, (-1)^n \overline{a}_n).$$

Assim,

$$S(v_1, \ldots, v_n) \bmod p = \overline{S}(\overline{v}_1, \ldots, \overline{v}_n). \tag{4.1}$$

Vemos que, para qualquer $F \in \mathbb{Z}[x_1, \ldots, x_n]$ tal que $stab_{S_n}(F) = stab_{S_n}(F \bmod p)$:

$$R(F, f) \bmod p = R(F \bmod p, f \bmod p), \tag{4.2}$$

onde a última resolvente é calculada sobre $\mathbb{Z}_p$. Para calcular $R(F, f)$ sobre $\mathbb{Z}$, usando 4.2, podemos calcular $R(F, f) \bmod p_i$, para primos distintos p_i tais que $\Pi\ p_i > 2C$, onde C é uma cota superior para o módulo dos coeficientes de $R(F, f)$. $R(F, f)$ é então reconstruída sobre $\mathbb{Z}$ usando o Algoritmo do Resto Chinês (cf. Knuth [7, pp. 268-276]).

Calculamos C pela cotação dos módulos dos zeros de $f(x)$, o que nos permite calcular uma cota para o módulo dos zeros de $R(F, f)$. Se B é uma cota superior para o módulo dos zeros de $R(F, f)$ e $d = \partial(R(F, f))$, então

$$C = \max\{\binom{d}{i} B^i : 1 \leq i \leq d\}$$

é uma cota superior para o módulo dos coeficientes de $R(F, f)$.

4.2 Uma cotação para os zeros de $f(x)$

Precisamos calcular uma cota A tal que $A \geq |v_i|$, para todo v_i zero de $f(x)$. Zassenhaus em [15] sugere

$$A = \max\{\frac{\left|\frac{a_i}{\binom{d}{i}}\right|^{\frac{1}{i}}}{(2^{\frac{1}{n}} - 1)} : 1 \leq i \leq n\}.$$

Sugerimos o método seguinte para calcular uma cota conveniente. Sejam

$$g(x) = x^n - \sum_{i=1}^{n} |a_i|\, x^{n-i}$$

e $R > 0$ uma cota estritamente superior para o módulo dos zeros reais de $g(x)$ (pela Regra dos Sinais de Descartes, $g(x)$ tem pelo menos um zero real positivo, daí podemos tomar

R como sendo o menor inteiro positivo tal que $g(R) > 0$). Agora note que para qualquer número complexo z tal que $|z| > R$:

$$|f(z)| \geq g(|z|) \geq g(R) > 0.$$

Assim, $R > |v_i|$, para todo v_i zero de $f(x)$.

O método acima é melhor do que aquele sugerido por Zassenhaus e usamos o mesmo nos exemplos da Seção 5.3.

4.3 A implementação

É usada a linguagem PASCAL a fim de elaborar o algoritmo LINRESOLV sobre $K = \mathbb{Z}_{p_i}$. Assim, calculamos $LR(M, f) \bmod p_i$, para primos distintos p_i. $LR(M, f)$ é reconstruída sobre $\mathbb{Z}$ usando o Algoritmo do Resto Chinês e então $LR(M, f)$ é fatorada, usando a fatoração de Hensel (cf. [7, 15]). Para estas duas últimas operações, usa-se a linguagem ALGEB, que foi elaborada por D. Ford e permite a computação com inteiros de tamanho arbitrário.

4.4 LINRESOLV sobre $K = \mathbb{Z}_p$

O corpo $\mathbb{Z}_p$ satisfaz às restrições da Seção 3.1, se $p > 2D$, onde D é o grau máximo de qualquer polnômio usado no programa. Na prática nós escolhemos p tal que p^2 é aproximadamente igual ao maior inteiro que podemos trabalhar ($10^7 < p < 2^{24}$ na nossa implementação).

Adição, subtração e multiplicação sobre $\mathbb{Z}_p$ são implementadas fazendo primeiramente estas operações sobre os inteiros e aplicando o operador PASCAL mod para o resultado. Para dividir precisamos de inversos multiplicativos em $\mathbb{Z}_p$. Dado $a \in \mathbb{Z}$ tal que $p \nmid a$, precisamos determinar $b \in \mathbb{Z}$ tal que $ab \equiv 1 \bmod p$. Sabemos que existem $b, t \in \mathbb{Z}$ tais que

$$1 = MDC(a, p) = ab + tp$$

Daí, b pode ser calculado usando o Algoritmo de Euclides (cf. [7, p. 325]).

O problema principal, que é dependente do corpo base na implementação do LINRESOLV, é a escolha de d no passo (6.2). Usando a notação do passo (6) do Algoritmo LINRESOLV, afirmamos que $d = MDC(c, p-1)$ é apropriado. Note que

$$d = MDC(c, p-1) = sc + t(p-1),$$

para algum $s, t \in \mathbb{Z}$. Seja $b = a^c$, para algum $a \in \mathbb{Z}_p$. Então, $b^s = a^{cs} = a^d$ pois, pelo Pequeno Teorema de Fermat,

$$y^{p-1} = 1, \forall y \in \mathbb{Z}_p, y \neq 0.$$

Agora precisamos mostrar que $y^d = z^d$, $\forall y, z \in \mathbb{Z}_p$, tais que $b = y^c = z^c$. Temos

$$y^c = z^c \Rightarrow y^{cs} = z^{cs} \Rightarrow y^d = z^d.$$

Quando usamos o Algoritmo LINRESOLV sobre $\mathbb{Z}_{p_i}$ a fim de calcularmos $LR(M, f)$ sobre $\mathbb{Z}$, escolhemos primos p_i tais que $j \nmid (p_i - 1)$, para $j = 3, \ldots, n$. Neste caso, d nunca é maior que 2 no passo (6.2).

4.5 Exemplos

Exemplo 5.1. Seja $f(x) = x^7 - 14x^5 + 56x^3 - 56x + 22$ (discutido no Exemplo 3.5). Calculamos e fatoramos $L(x) = LR([1^3], f)$, de grau 35, para provar que $Gal(f/\mathbb{Q})$ é o grupo $7T3$, o grupo de Frobenius de ordem 21.

Uma cota superior para o módulo dos zeros de $f(x)$ é 5, daí 15 é uma cota superior para o módulo dos zeros de $L(x)$. Uma cota superior para o módulo dos coeficientes de $L(x)$ é $\frac{1}{2}10^{42}.L(x) \mod p_i$ foi calculada para seis primos $p_i > 10^7.L(x)$ foi então construída sobre $\mathbb{Z}$ usando o Algoritmo do Resto Chinês. Fatorando $L(x)$ em fatores irredutíveis sobre $\mathbb{Q}$, encontramos $L(x) = L_1(x)L_2(x)L_3(x)$, onde

$$
\begin{aligned}
L_1(x) &= x^7 - 28x^5 + 224x^3 - 448x + 94, \\
L_2(x) &= x^7 - 28x^5 + 224x^3 - 448x + 192 \text{ e} \\
L_3(x) &= x^{21} - 84x^{19} + 2436x^{17} - 31136x^{15} + 6358x^{14} + 203840x^{13} - \\
&\quad -84392x^{12} - 733824x^{11} + 420728x^{10} + 1480192x^9 - 988064x^8 - \\
&\quad -1652036x^7 + 1138368x^6 + 986496x^5 - 620928x^4 - 284032x^3 + \\
&\quad +137984x^2 + 27104x - 10648.
\end{aligned}
$$

$L(x)$ possui zeros distintos e sua fatoração mostra que a partição do comprimento das órbitas de 3−conjuntos sob a ação de $Gal(f/\mathbb{Q})$ é $(7^2, 21)$. Da tabela logo abaixo da Tabela A.11 do Apêndice, vemos que $Gal(f/\mathbb{Q})$ é $7T3$.

Exemplo 5.2. Seja $f(x) = x^5 + 15x + 12$. Temos que $disc(f) = 2^{10}3^45^5$ e $f(x)$ é irredutível sobre $\mathbb{Q}$. Desde que $disc(f)$ não é um quadrado, da Tabela A.5 e da tabela situada logo abaixo da Tabela A.6 do Apêndice, vemos que $Gal(f/\mathbb{Q})$ é $5T3$ (o grupo de Frobenius de ordem 20) ou $5T5(= S_5)$.

Seja $F = (x_1 + x_2 - x_3 - x_4)^2$. Calculamos e fatoramos $R(x) = R(F, f)$, de grau 15, para saber qual dos candidatos é $Gal(f/\mathbb{Q})$ ($R(F, f)(x^2) = LR([1^2, -1^2], f)(x)$; cf. Seção 3.3, 5.2).

Uma cota superior para o módulo dos zeros de $f(x)$ é 3, daí 144 é uma cota superior para os zeros de $R(x)$. Uma cota superior para o módulo dos coeficientes de $R(x)$ é 10^{33}. $R(x) \bmod p_i$ foi calculada para cinco primos $p_i > 10^7$.$R(x)$ foi então construída sobre $\mathbb{Z}$ usando o Algoritmo do Resto Chinês. Fatorando $R(x)$ em fatores irredutíveis sobre $\mathbb{Q}$, encontramos $R(x) = R_1(x)R_2(x)$,onde $\partial(R_1(x)) = 5$ e $\partial(R_2(x)) = 10$. $R(x)$ possui zeros distintos e sua fatoração mostra que que $Gal(f/\mathbb{Q})$ age intransitivamente sobre $S_5 * F$, daí $Gal(f/\mathbb{Q})$ é $5T3$.

Capítulo 5

Conclusões

Este trabalho é deveras importante, do ponto de vista algébrico e computacional, pois fornece algoritmos que aceleram consideravelmente o processo para a obtenção do grupo de Galois de um polinômio sobre os racionais, grupo este que desempenha papel fundamental na questão de solubilidade por radicais de um polinômio, que é objeto de estudo da Álgebra desde os tempos antigos.

A seguir, listamos alguns itens que podem ser considerados como uma continuação deste trabalho:

- A elaboração, através dos algoritmos fornecidos, de programas em uma linguagem computacional adequada, a fim de calcular o grupo de Galois de um polinômio irredutível sobre os racionais, com coeficientes inteiros, de grau inferior ou igual a 7.

- A obtenção do grupo de Galois de qualquer polinômio com coeficientes inteiros, de grau inferior ou igual a 7, já que sabemos como calcular o grupo de Galois de seus fatores irredutíveis.

- Fornecer algoritmos que calculem o grupo de Galois de um polinômio irredutível sobre os racionais, com coeficientes inteiros, de grau superior ou igual a 8.

- A obtenção de algoritmos que, implementados em computador, calculam eficientemente resolventes polinomiais quaisquer, as quais são importantes para o cálculo dos grupos de Galois, como foi visto ao longo deste trabalho.

Apêndice A

Tabelas dos grupos transitivos de grau n , com $3 \leq n \leq 7$

Para cada grau apresentamos informações sobre todos os grupos transitivos que possuem tal grau em um conjunto de tabelas. Os grupos são denominados $T1$, $T2$, etc, por conveniência e para evitar confusões escrevemos nTi para identificar o $i-$ésimo grupo de grau n. Todas as tabelas abaixo encontram-se em [1].

Nas tabelas A.1, A.3, A.5, A.7, A.9 listamos a ordem do grupo, se o mesmo é ou não constituído apenas de permutações pares, os possíveis tipos de sistemas de imprimitividade(caso o mesmo seja imprimitivo) e o número de suas classes de conjugação. Se o grupo possui uma representação fiel de menor grau, isto é dado na coluna denominada "Outra Representação" e abreviada por "O. R.". Se o grupo é conhecido por um nome comum, este é apresentado na coluna intitulada "Nome". Para cada tabela acima citada, é dado um conjunto de geradores para cada grupo, bem como a partição do comprimento das órbitas de r-conjuntos e 2-seqüências (com elementos distintos) sob a ação de cada grupo.

As tabelas A.2, A.4, A.6, A.8, A.10, A.11 apresentam os elementos distintos de cada grupo, especificando os seus tipos ciclos.

Grupo	Ordem	Par	Nº de Classes	Nome
$T1$	3	+	3	A_3
$T2$	6		3	S_3

Tabela A.1: grupos de grau 3

	2		
	1^3	1	3
$T1$	1	-	2
$T2$	1	3	2

Tabela A.2: Distribuição de tipos ciclos para a Tabela A.1

Geradores de grupos para a Tabela A.1

$$a = (1, 2, 3) \qquad b = (1, 2)$$
$$T1 = \langle a \rangle \qquad T2 = \langle a, b \rangle$$

Partições dos comprimentos das órbitas de r-conjuntos e 2-seqüências sob a ação de G para a Tabela A.1

G	2-conjuntos	2-seqüências
$G \leq A_3$		
$T1$	3	3^2
$G \not\leq A_3$		
$T2$	3	6

Grupo	Ordem	Par	Imprimitivo $[2^2]$	Nº de Classes	Nome
$T1$	4		⌋	4	$\mathbb{Z}_4$
$T2$	4	+	⌋	4	$\mathbb{Z}_2 \times \mathbb{Z}_2$
$T3$	8		⌋	5	D_8
$T4$	12	+		4	A_4
$T5$	16			5	S_4

Tabela A.3: grupos de grau 4

Geradores de grupos para a Tabela A.3

$$a = (1,3,4) \qquad c = (2,4)$$
$$b = (1,3) \qquad d = (1,2)(3,4)$$

$$T1 = \langle ac \rangle \qquad T4 = \langle a, d \rangle$$
$$T2 = \langle bc, d \rangle \qquad T5 = \langle ac, d \rangle$$
$$T3 = \langle ac, bc \rangle$$

		2		3	
	1^4	1^2	2^2	1	4
$T1$	1	–	1	–	2
$T2$	1	–	3	–	–
$T3$	1	2	3	–	2
$T4$	1	–	3	8	–
$T5$	1	6	3	8	6

Tabela A.4: Distribuição de tipos ciclos para a Tabela A.3

Partições dos comprimentos das órbitas de r-conjuntos e 2-seqüências sob a ação de G para a Tabela A.3

G	2-conjuntos	2-seqüências
$G \leq A_4$		
$T2$	2^3	4^3
$T4$	6	12
$G \not\leq A_4$		
$T1$	$2, 4$	4^3
$T3$	$2, 4$	$4, 8$
$T5$	6	12

Grupo	Ordem	Par	Nº de Classes	Nome
$T1$	5	+	5	$\mathbb{Z}_5$
$T2$	10	+	4	D_{10}
$T3$	20		5	F_{20}
$T4$	60	+	5	A_5
$T5$	120		7	S_5

Tabela A.5: grupos de grau 5

Geradores de grupos para a Tabela A.5

$$a = (1, 2, 3, 4, 5) \qquad c = (2, 3, 5, 4)$$
$$b = (1, 2)$$

$$T1 = \langle a \rangle \qquad T4 = \langle a, bab \rangle$$
$$T2 = \langle a, c^2 \rangle \qquad T5 = \langle a, b \rangle$$
$$T3 = \langle a, c \rangle$$

		2	2^2	3	3	4	
	1^5	1^3	1	2	1^2	1	5
$T1$	1	–	–	–	–	–	4
$T2$	1	–	5	–	–	–	4
$T3$	1	–	5	–	–	10	4
$T4$	1	–	15	–	20	–	24
$T5$	1	10	15	20	20	30	24

Tabela A.6: Distribuição de tipos ciclos para a Tabela A.5

Partições dos comprimentos das órbitas de r-conjuntos e 2-seqüências sob a ação de G para a Tabela A.5

G	2-conjuntos	2-seqüências
$G \leq A_5$		
$T1$	5^2	5^4
$T2$	5^2	10^2
$T4$	10	20
$G \not\leq A_5$		
$T3$	10	20
$T5$	10	20

Grupo	Ordem	Par			Nº de Classes	O. R.	Nome
$T1$	6		⌟	⌟	6		$\mathbb{Z}_6$
$T2$	6		⌟	⌟	3	$3T2$	S_3
$T3$	12		⌟	⌟	6		D_{12}
$T4$	12	+	⌟		4	$4T4$	A_4
$T5$	18			⌟	9		$\mathbb{Z}_3 \times S_3$
$T6$	24		⌟		8		$\mathbb{Z}_2 \times A_4$
$T7$	24	+	⌟		5	$4T5$	$\mathrm{Im}(rep(S_4, \mathcal{P}(\frac{S_4}{\mathbb{Z}_2^2})))$
$T8$	24		⌟		5	$4T5$	$\mathrm{Im}(rep(S_4, \mathcal{P}(\frac{S_4}{\mathbb{Z}_4})))$
$T9$	36			⌟	9		$\mathbb{Z}_3^2\mathbb{Z}_2^2$
$T10$	36	+		⌟	6		$\mathbb{Z}_3^2\mathbb{Z}_4$
$T11$	48		⌟		10		$\mathbb{Z}_2 \times S_4$
$T12$	60	+			5	$5T4$	$PSL(2,5)$
$T13$	72			⌟	9		$\mathbb{Z}_3^2 D_8$
$T14$	120				7	$5T5$	$PGL(2,5)$
$T15$	360	+			7		A_6
$T16$	720				11		S_6

Tabela A.7: Grupos de grau 6

Geradores de grupos para a Tabela A.7

$a = (1, 2, 3)$ $\quad$ $i = (1, 3)(2, 4)$

$b = (1, 4)(2, 5)(3, 6)$ $\quad$ $j = (1, 6)(2, 5)(3, 4)$

$c = (1, 5, 2, 4)(3, 6)$ $\quad$ $k = (1, 2, 3, 4, 5)$

$d = ab$ $\quad$ $l = (1, 6)(2, 5)$

$e = bc^2$ $\quad$ $m = (2, 3, 5, 4)$

$f = (1, 2)$

$g = (1, 3, 5)(2, 4, 6)$

$h = fgfg^2$

$T1 = \langle d \rangle$ $\quad$ $T11 = \langle f, g, i \rangle$

$T2 = \langle e, j \rangle$ $\quad$ $T12 = \langle k, l \rangle$

$T3 = \langle d, e \rangle$ $\quad$ $T13 = \langle a, b, c \rangle$

$T4 = \langle g, h \rangle$ $\quad$ $T14 = \langle k, l, m \rangle$

$T5 = \langle a, b \rangle$ $\quad$ $T15 = \langle c, k \rangle$

$T6 = \langle g, f \rangle$ $\quad$ $T16 = \langle d, k \rangle$

$T7 = \langle g, h, i \rangle$

$T8 = \langle g, h, j \rangle$

$T9 = \langle a, b, e \rangle$

$T10 = \langle a, c \rangle$

						3					
		2	2^2		3	2		4	4	5	
	1^6	1^4	1^2	2^3	1^3	1	3^2	1^2	2	1	6
$T1$	1	–	–	1	–	–	2	–	–	–	2
$T2$	1	–	–	3	–	–	2	–	–	–	–
$T3$	1	–	3	4	–	–	2	–	–	–	2
$T4$	1	–	3	–	–	–	8	–	–	–	–
$T5$	1	–	–	3	4	–	4	–	–	–	6
$T6$	1	3	3	1	–	–	8	–	–	–	8
$T7$	1	–	9	–	–	–	8	–	6	–	–
$T8$	1	–	3	6	–	–	8	6	–	–	–
$T9$	1	–	9	6	4	–	4	–	–	–	12
$T10$	1	–	9	–	4	–	4	–	18	–	–
$T11$	1	3	9	7	–	–	8	6	6	–	8
$T12$	1	–	15	–	–	–	20	–	–	24	–
$T13$	1	6	9	6	4	12	4	–	18	–	12
$T14$	1	–	15	10	–	–	20	30	–	24	20
$T15$	1	–	45	–	40	–	40	–	90	144	–
$T16$	1	15	45	15	40	120	40	90	90	144	120

Tabela A.8: Distribuição de tipos ciclos para a Tabela A.7

Partições dos comprimentos das órbitas de r-conjuntos e 2-seqüências sob a ação de G para a Tabela A.7

G	2-conjuntos	3-conjuntos	2-seqüências
$G \leq A_6$			
$T4$	$3, 12$	$4^2, 6^2$	$6, 12^2$
$T7$	$3, 12$	$4^2, 12$	$6, 24$
$T10$	$6, 9$	$2, 18$	$12, 18$
$T12$	15	10^2	30
$T15$	15	20	30
$G \not\leq A_6$			
$T1$	$3, 6^2$	$2, 6^3$	6^5
$T2$	$3^2, 6$	$2, 6^3$	6^5
$T3$	$3, 6^2$	$2, 6, 12$	$6, 12^2$
$T5$	$6, 9$	$2, 18$	$6^2, 18$
$T6$	$3, 12$	$6^2, 8$	$6, 12^2$
$T8$	$3, 12$	$8, 12$	$6, 24$
$T9$	$6, 9$	$2, 18$	$12, 18$
$T11$	$3, 12$	$8, 12$	$6, 24$
$T13$	$6, 9$	$2, 18$	$12, 18$
$T14$	15	20	30
$T16$	15	20	30

Grupo	Ordem	Par	Nº de Classes	Nome
$T1$	7	+	7	$\mathbb{Z}_7$
$T2$	14		5	D_{14}
$T3$	21	+	5	F_{21}
$T4$	42		7	F_{42}
$T5$	168	+	6	$PSL(3,2)$
$T6$	2520	+	9	A_7
$T7$	5040		15	S_7

Tabela A.9: Grupos de grau 7

Geradores de grupos para a Tabela A.9

$$a = (1,2,3,4,5,6,7) \qquad c = (2,3)(4,7)$$
$$b = (2,4,3,7,5,6) \qquad d = (1,2,3)$$

$$T1 = \langle a \rangle \qquad T6 = \langle a, d \rangle$$
$$T2 = \langle a, b^3 \rangle \qquad T7 = \langle b, d \rangle$$
$$T3 = \langle a, b^2 \rangle$$
$$T4 = \langle a, b \rangle$$
$$T5 = \langle a, c \rangle$$

						3		
		2	2^2	2^3	3	2	3	3^2
	1^7	1^5	1^3	1	1^4	1^2	2^2	1
$T1$	1	–	–	–	–	–	–	–
$T2$	1	–	–	7	–	–	–	–
$T3$	1	–	–	–	–	–	–	14
$T4$	1	–	–	7	–	–	–	14
$T5$	1	–	21	–	–	–	–	56
$T6$	1	–	105	–	70	–	210	280
$T7$	1	21	105	105	70	420	210	280

Tabela A.10: Distribuição de tipos ciclos para a Tabela A.9

Partições dos comprimentos das órbitas de r-conjuntos e 2-seqüências sob a ação de G para a Tabela A.9

G	2-conjuntos	3-conjuntos	2-seqüências
$G \leq A_7$			
$T1$	7^3	7^5	7^6
$T3$	21	$7^2, 21$	21^2
$T5$	21	$7, 28$	42
$T6$	21	35	42
$G \not\leq A_7$			
$T2$	7^3	$7^3, 14$	14^3
$T4$	21	$14, 21$	42
$T7$	21	35	42

		4					
	4	2	4	5	5	6	
	1^3	1	3	1^2	2	1	7
$T1$	–	–	–	–	–	–	6
$T2$	–	–	–	–	–	–	6
$T3$	–	–	–	–	–	–	6
$T4$	–	–	–	–	–	14	6
$T5$	–	42	–	–	–	–	48
$T6$	–	630	–	504	–	–	720
$T7$	210	630	420	504	504	840	720

Tabela A.11: Continuação da Tabela A.10

Referências Bibliográficas

[1] G. Butler and J. McKay, "The Transitive Groups of Degree up to 11," *Comm. Algebra*, pp. 863-911, 1983.

[2] L. Childs, *A Concrete Introduction to Higher Algebra*, Springer-Verlag, New York, 1979.

[3] G.E. Collins, "The Calculation of Multivariate Polynomial Resultants", *JACM*, 18, pp. 515-532, 1971.

[4] D.W. Erbach, J. Fischer and J. McKay, "Polynomials with PSL(2,7) as Galois Group", *J. Number Theory*, 11, pp. 69-75, 1979.

[5] A. Garcia e Y. Lequain, *Álgebra: Uma Introdução*, Projeto Euclides, Rio de Janeiro, 1983.

[6] A. Gonçalves, *Introdução à Álgebra*, Projeto Euclides, Rio de Janeiro, 1979.

[7] D.E. Knuth, *The Art of Computer Programing*, Vol 2, 2-ed. Addison-Wesley, 1981.

[8] S. Lang, *Algebra*, Addison-Wesley,

[9] P.J. McCarthy, *Algebraic Extensions of Fields*, Blaisdell Publishing Co., 1966.

[10] J. McKay, "Some Remarks on Computing Galois Groups", *SIAN J. Comput.*, 8, pp. 344-347, 1979.

[11] W.R. Scott, *Group Theory*, Dover Publications, 1987.

[12] R.P. Stauduhar, "The determination of Galois Groups", *Math. Comput.*, 27, pp. 981-996, 1973.

[13] B.M. Trager, "Algebraic Factoring and Rational Function Integration," *Proc. 1976, ACM Symp. on Symbolic and Algebraic Comput.*, pp. 219-226.

[14] B.L. van der Waerden, *Modern Algebra*, Vol. 1, tr. Blum, F., Ungar, New York, 1953.

[15] H. Zassenhaus, "On Hensel Factorization", *I. J. Number Theory*, 1, pp. 291-311, 1969.