Cálculo do Grupo de Galois

Danilo Elias Castro – nUSP 3100230

3 de dezembro de 2007

Sumário

Parte I

Parte Objetiva

Capítulo 1

Introdução

> Si l'équation proposée a tous ses coefficients rationnels, l'équation auxiliaire qui donne cette fonction les aura tous aussi, et il suffira de reconnaître si cette équation auxiliaire du degré $1.2.3...(n-2)$ a ou non une racine rationnelle, ce que l'on sait faire.
>
> Évariste Galois

1.1 Teoria de Galois

Em 1831 Évariste Galois resolveu, em seu artigo, "Mémoire: Sur les conditions de résolubilité des équations par radicaux", o problema de solubilidade por radicais de polinômios irredutíveis de grau primo e encontrou condições para um polinômio ser ou não solúvel por radicais.

Na epígrafe acima Galois escreve "Se a equação proposta tiver seus coeficientes racionais, sua equação auxiliar também terá, e será suficiente determinar se a equação auxiliar de grau $(n-2)!$ tem ou não uma raiz racional. E isso sabe-se como fazer."

A equação proposta é, obviamente, dada pelo polinômio cujas raízes Galois queria saber se eram solúveis ou não, por radicais. A equação auxiliar é o que nós chamaremos de polinômio resolvente, e a última frase refere-se ao fato já conhecido na época que sempre que temos polinômios com coeficientes em $\mathbb{Z}$, suas raízes racionais são do tipo $\pm q/p$ onde p e q são os coeficientes do primeiro termo e do termo independente respectivamente. Na citação do Galois aparece a palavra "racional"que não tem exatamente o mesmo significado que para nós, mas isso deixaremos de lado.

Galois, em seu trabalho, utilizou uma estrutura associada ao polinômio original que faz o serviço de nos contar se o dado polinômio é ou não solúvel por radicais. Essa estrutura era chamada de "grupo de permutações"(groupe de permutations) que, possuindo certas propriedades, indicava se o polinômio era de fato solúvel por radicais. Esse grupo será justamente chamado de *Grupo de Galois* e é sempre um subgrupo do grupo de permutações do conjunto $\{1, 2, \ldots, n\}$ chamado de $\mathfrak{S}_n$ onde n é o grau do polinômio dado.

Na verdade, o que foi descoberto é que existe uma correspondência bijetora entre o reticulado de subcorpos do corpo das raízes do polinômio original e o reticulado de subgrupos do grupo de Galois. Dentre outras coisas, essa correspondência nos traz informações sobre a natureza algébrica das raízes e isso permitiu a Galois inferir sobre sua construção(das raízes) pela utilização de radicais.

1.2 O Trabalho proposto

No contexto acima, este trabalho visa estudar o algoritmo que fornece o grupo de Galois de qualquer polinômio mônico irredutível com coeficientes inteiros de grau menor ou igual a 7.

Para isso, se utiliza fortemente do "Teorema Fundamental da Teoria de Galois", que trata da correspondência mencionada acima, e também de polinômios resolventes que nos dão informações sobre qual é o grupo de Galois. Em suma, para cada grau, há um resolvente particular que, sob certas condições, determina qual é o grupo em questão.

O método utilizado aqui chama-se "método do resolvente"que foi exposto por Henry Cohen em [5].

Os capítulos 2 e 3 tratam da teoria de Galois do ponto de vista moderno. O capítulo 4 dá a teoria por trás dos algoritmos e demonstra a validade dos algoritmos para se encontrar o grupo de Galois dos polinômios do 3^o,4^o e 5^o graus. Para os outros casos a demonstração é análoga e depende apenas das particularidades do reticulado de subgrupos do $\mathfrak{S}_n$.

Além do algoritmo, este trabalho deve produzir um pacote na linguagem do programa Mathematica que recebe um polinômio irredutível com coeficientes racionais e devolve uma representação do grupo de Galois correspondente. Como o algoritmo deve receber um polinômio mônico com coeficientes inteiros, então uma transformação no polinômio original deve ser feita.

No apêndice A, há uma tabela que relaciona as representações do grupo de Galois com sua respectiva descrição.

Capítulo 2

Extensões de Corpos e Morfismos

2.1 Preliminares

Nesta primeira seção, pretendo expor conhecimentos básicos de álgebra abstrata que serão frequentemente usados neste trabalho. Apesar disso, supomos que o leitor já possua nesse momento alguns conhecimentos prévios adquiridos em algum curso introdutório de álgebra abstrata, como por exemplo na disciplina Álgebra II do IME-USP.

Tais conhecimentos prévios são:

- Estrutura de anéis, domínios de integridade e corpos.
- Homomorfismos de anéis e anéis quociente.
- Ideais primos e maximais.
- Espaço Vetorial sobre um corpo.
- Grupos.
- Ações de grupos.

Usaremos frequentemente o seguinte resultado, que trata da avaliação de um polinômio de um anel $F[x]$ no elemento $\alpha \in$ corpo E.

Teorema 2.1.1 (Avaliação)**.** *Seja F um subcorpo de um corpo E e seja α elemento de E. A função $\varepsilon_\alpha : F[x] \to E$ definida por:*

$$\varepsilon_\alpha(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

*com $a_i \in F$ é um homomorfismo de anéis de $F[x]$ em E. O homomorfismo ε_α é uma **avaliação** em α.*

Demonstração. ε_α está claramente bem definida e agora vamos mostrar que ε_α é de fato um homomorfismo de anéis. Considere então $f(x) = a_0+a_1x+\cdots+a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$ com $m \leq n$. Assim:

$$\varepsilon_\alpha(f(x) + g(x)) =$$

$$\varepsilon_\alpha((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n) =$$

$$(a_0 + b_0) + (a_1 + b_1)\alpha + \cdots + (a_m + b_m)\alpha^m + a_{m+1}\alpha^{m+1} + \cdots + a_n\alpha^n =$$

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n + b_0 + b_1\alpha + \cdots + b_m\alpha^m =$$

$$f(\alpha) + g(\alpha) = \varepsilon_\alpha(f(x)) + \varepsilon_\alpha(g(x))$$

E também:

$$\varepsilon_\alpha(f(x)g(x)) =$$

$$\varepsilon_\alpha(d_0 + d_1x + \cdots + d_nx^n) =$$

$$d_0 + d_1\alpha + \cdots + d_n\alpha^n =$$

$$(a_0 + a_1\alpha + \cdots + a_n\alpha^n)(b_0 + b_1x + \cdots + b_mx^m) =$$

$$f(\alpha)g(\alpha) = \varepsilon_\alpha(f(x))\varepsilon_\alpha(g(x))$$

onde $d_i = \sum_{j=0}^{i} a_jb_{i-j}$

E pela definição $\varepsilon_\alpha(a) = a$ e isso termina a prova. □

Neste trabalho, utilizaremos o tempo todo, principalmente a partir de extensões de morfismos, o conceito de homomorfismos de corpos. Esses morfismos mostram o que há de mais importante por trás da teoria de Galois que é a relação entre a simetria algébrica das raízes de um polinômio e a solubilidade por radicais.

Definição 2.1.2 (Morfismo de Corpos)**.** Se F e L são corpos, uma função $\sigma : F \to L$ é um **homomorfismo de corpos** se valem, para todo $x, y \in F$:

1. $\sigma(x + y) = \sigma(x) + \sigma(y)$

2. $\sigma(xy) = \sigma(x)\sigma(y)$

Note que o ideal de um corpo é ou nulo, ou todo o corpo. Assim o kernel da σ é um ideal de F e portanto todo morfismo de corpos é ou o morfismo nulo, ou é injetor. Daqui para frente sempre vamos considerar o segundo caso.

2.2 Extensões de Corpos

Definição 2.2.1 (Extensão de Corpos)**.** Um corpo E é uma extensão de um corpo F se $F \subset E$.

Precisamos mostrar que todo polinômio tem uma raiz em algum lugar, ou seja, se F é um corpo e $f(x)$ um polinômio em $F[x]$, então existe uma extensão de F onde esse polinômio tenha uma raiz. Temos assim o seguinte teorema:

Teorema 2.2.2 (Kronecker)**.** *Seja F um corpo e seja $f(x)$ um polinômio não constante em $F[x]$. Então existe uma extensão E de F e um $\alpha \in E$ tal que $f(\alpha) = 0$.*

Demonstração. Sabemos que $f(x)$ se fatora em $F[x]$ num produto de polinômios que são irredutíveis. Seja $p(x)$ um polinômio irredutível em tal fatoração. Basta então encontrar uma extensão E de F que contém um elemento α tal que $p(\alpha) = 0$. Como $\langle p(x)\rangle$ é um ideal maximal em $F[x]$, então $F[x]/\langle p(x)\rangle$ é um corpo. Queremos mostrar que F pode ser identificado como um subcorpo de $F[x]/\langle p(x)\rangle$ através da inclusão natural $\psi : F \to F[x]/\langle p(x)\rangle$ dada por

$$\psi(a) = a + \langle p(x)\rangle$$

para $a \in F$. Esta função é injetora, pois, se $\psi(a) = \psi(b)$, ou seja, se $a+\langle p(x)\rangle = b + \langle p(x)\rangle$ para certos $a, b \in F$, então $(a - b) \in \langle p(x)\rangle$, portanto, $a - b$ deve ser múltiplo do polinômio $p(x)$, de grau ≥ 1. Mas $a, b \in F$ implica que $a - b$ está em F. Assim, devemos ter $a - b = 0$ e, então $a = b$. Podemos escolher a como sendo um elemento da classe $(a + \langle p(x)\rangle)$. Assim ψ é um isomorfismo de F em um subcorpo de $F[x]/\langle p(x)\rangle$. Assim, identificamos F como sendo $\{a + \langle p(x)\rangle \mid a \in F\}$ por meio de ψ. Agora podemos ver $E = F[x]/\langle p(x)\rangle$ como uma extensão de F. Tendo já criado a extensão E de $\psi(F)$, cópia isomorfa de F, pode-se então produzir uma extensão E' de F por um argumento conjuntista. Falta mostrar que E contém um zero de $p(x)$. Definimos

$$\alpha = x + \langle p(x)\rangle,$$

com $\alpha \in E$. Considere agora a avaliação $\phi_\alpha : F[x] \to E$ tal que $\phi_\alpha(p(x)) = p(\alpha)$. Se $p(x) = a_0 + a_1x + \cdots + a_nx^n$, onde $a_i \in F$, então temos

$$\phi_\alpha(p(x)) = a_0 + a_1(x + \langle p(x)\rangle) + \cdots + a_n(x + \langle p(x)\rangle)^n$$

em $E = F[x]/\langle p(x)\rangle$.

$$\phi_\alpha(p(x)) = p(\alpha) = (a_0 + a_1x + \cdots + a_nx^n) + \langle p(x)\rangle = p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0$$

em $F[x]/\langle p(x)\rangle$. Encontramos um elemento α em $E = F[x]/\langle p(x)\rangle$ tal que $p(\alpha) = 0$, e ,portanto, $f(\alpha) = 0$. □

Provamos acima que sempre existe um corpo E, contento F, e contendo a raiz de um polinômio qualquer $f(x) \in F[x]$ dado, mas se E for um corpo qualquer, nem sempre acontece de todo elemento de E ser uma raiz de algum polinômio em $F[x]$. Podemos agora definir elementos algébricos e transcendentes.

Definição 2.2.3. Um elemento α de uma extensão E de um corpo F é dito **algébrico** sobre F se $f(\alpha) = 0$ para algum polinômio não nulo $f(x)$ de $F[x]$. Se α não for algébrico, dizemos que α é **transcendente** sobre F.

Como exemplo considere a extensão $\mathbb{R}$ de $\mathbb{Q}$. Sabemos que $\sqrt{3}$ é algébrico sobre $\mathbb{Q}$ sendo raiz de $x^2 - 3$. Claramente $\sqrt{3}$ também é raiz de $x^3 - 3x$ e de $x^4 - 3x^2 + 2$. Assim é razoável imaginar que todos os polinômios em $\mathbb{Q}[x]$ que tenham $\sqrt{3}$ como raiz sejam múltiplos de $x^2 - 3$. Temos então:

Teorema 2.2.4. *Seja E uma extensão de F, e seja $\alpha \in E$, algébrico sobre F. Então existe um polinômio irredutível $p(x) \in F[x]$ tal que $p(\alpha) = 0$. Esse polinômio é univocamente determinado a menos de uma constante multiplicativa em F e é um polinômio de grau mínimo ≥ 1 em $F[x]$ tendo α como raiz. Se $f(\alpha) = 0$ com $f(x) \neq 0 \in F[x]$, então $p(x)$ divide $f(x)$.*

Demonstração. Seja ϕ_α a avaliação de $F[x]$ em E. Sabemos que o kernel de ϕ_α é um ideal principal gerado por algum $p(x) \in F[x]$. Assim o ideal $\langle p(x) \rangle$ consiste precisamente de todos os elementos de $F[x]$ que tem α como raiz. Assim, se $f(\alpha) = 0$ com $f(x) \neq 0 \in F[x]$, então $f(x) \in \langle p(x) \rangle$ e portanto $p(x)$ divide $f(x)$. Portanto, $p(x)$ é de grau mínimo e qualquer outro polinômio de mesmo grau tendo α como raiz deve ser da forma $ap(x)$ para algum $a \in F$.

Falta provar que $p(x)$ é irredutível. Para isso Suponha que $p(x) = r(x)s(x)$ onde os graus de r e s devem ser maiores ou iguais a 1 e menores que o grau de p. Então se $p(\alpha) = 0$, $r(\alpha)s(\alpha) = 0$ implicando que ou $r(\alpha) = 0$ ou $s(\alpha) = 0$, pois E é um corpo e não tem divisores de zero. Mas isso é um absurdo pois $p(x)$ é de grau mínimo. Concluímos que $p(x)$ é irredutível. □

Sempre podemos escolher um polinômio tal que o coeficiente do termo de maior grau é 1. Tal polinômio é chamado polinômio mônico.

Definição 2.2.5 ($irr(\alpha, F)$)**.** Seja E uma extensão do corpo F, e seja $\alpha \in E$ algébrico sobre F. O único polinômio mônico $p(x)$ do teorema anterior é o **polinômio irredutível de α sobre** F e será denotado por $irr(\alpha, F)$.

Seja E uma extensão de F, seja $\alpha \in E$. Seja ε_α a avaliação de $F[x]$ em E como já definimos antes.

Suponha que α é algébrico sobre F. Então como no teorema 2.2.4, o kernel de ε_α é $\langle irr(\alpha, F) \rangle$ que já sabemos que é ideal maximal de $F[x]$. Portanto, $F[x]/\langle irr(\alpha, F) \rangle$ é corpo e é isomorfo a imagem $\varepsilon_\alpha(F[x])$ em E. Pode-se mostrar que este subcorpo $\varepsilon_\alpha(F[x])$ em E é o menor subcorpo de E contendo F e α e será denotado por $F(\alpha)$.

Definição 2.2.6 (Extensões Simples)**.** Uma extensão E de um corpo F é dita uma **extensão simples** de F se $E = F(\alpha)$ para algum $\alpha \in E$.

Teorema 2.2.7. *Seja $E = F(\alpha)$ uma extensão simples de um corpo F, e seja α algébrico sobre F. Se o grau do $irr(\alpha, F)$ é $n \geq 1$, então todo elemento β de E se escreve de modo único como:*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

onde os b_j estão em F.

Demonstração. Considerando a avaliação ϕ_α, todo elemento de $F(\alpha)$ é da forma $\phi_\alpha(f(x)) = f(\alpha)$, ou seja, é um polinômio em α com coeficientes em F. Seja:

$$irr(\alpha, F) = p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

E então como $p(\alpha) = 0$, temos

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$$

Esta equação mostra que podemos expressar todo monômio α^m para $m \geq n$ em termos de potências de α menores ou iguais a n. Assim é claro que todo β pode ser expresso na forma desejada. Para verificar a unicidade basta ver que se:

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b_0^{'} + b_1^{'}\alpha + \cdots + b_{n-1}^{'}\alpha^{n-1}$$

para $b_j^{'} \in F$, então

$$g(x) = (b_0 - b_0^{'}) + (b_1 - b_1^{'})x + \cdots + (b_{n-1} - b_{n-1}^{'})x^{n-1}$$

é um polinômio em $F[x]$ que tem α como raiz. Mas como o grau de g é menor que o grau do $irr(\alpha, F)$ que é por sua vez o polinômio minimal, então $g(x) = 0$. Assim $b_j = b_j^{'}$ e a representação é única. □

2.3 Extensões Algébricas

Definição 2.3.1 (Extensão Algébrica)**.** Uma extensão E de um corpo F é uma **extensão algébrica** se todo elemento de E for algébrico sobre F.

Definição 2.3.2 (Extensão Finita)**.** Se uma extensão E de um corpo F tem dimensão finita n como espaço vetorial sobre F, então E é uma **extensão finita de grau n sobre** F. Esse grau será denotado por $[E : F]$.

Teorema 2.3.3. *Se considerarmos a torre de corpos $F \subset K \subset E$, então:*

$$[E : F] = [E : K][K : F]$$

Demonstração. Sejam $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ e $\{\beta_1, \beta_2, \ldots, \beta_m\}$ bases de E/K e K/F respectivamente. Vamos provar que o conjunto:

$$\{\alpha_i\beta_j\}_{(i,j)}$$

é uma base de E/F. Primeiro vamos mostrar que esses vetores geram E sobre F. Seja então $\gamma \in E$. Como $\{\alpha_i\}$ é a base de E sobre K então:

$$\gamma = \sum_{i=1}^{n} a_i \alpha_i$$

para $a_i \in K$. E como $\{\beta_j\}$ é a base de K sobre F então:

$$a_i = \sum_{j=1}^{m} \lambda_{ij} \beta_j$$

para $\lambda_{ij} \in F$. Então finalmente:

$$\gamma = \sum_{i=1}^{n} (\sum_{j=1}^{m} \lambda_{ij} \beta_j) \alpha_i = \sum_{i,j} \lambda_{ij} (\beta_j \alpha_i)$$

e portanto $\{\alpha_i \beta_j\}_{(i,j)}$ geram E sobre F. Falta agora mostrar que esses vetores são todos l.i.

Assim se por contradição $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ para certos $\lambda_{ij} \in F$ não todos nulos, então podemos escrever:

$$\sum_i (\sum_j \lambda_{ij} y_j) x_i = 0$$

Como $\sum_j \lambda_{ij} y_j$ está em K, e pela hipótese dos x_i serem l.i temos:

$$\sum_j \lambda_{ij} y_j = 0 \text{ para todo i}$$

e novamente pela hipótese dos y_i serem l.i, então $\lambda_{ij} = 0$ para todo par (i, j).

Os elementos $\{\alpha_i \beta_j\}_{(i,j)}$ são linearmente independentes sobre F e, como já vimos, geram E sobre F. □

$$\begin{array}{l} \\ Base\{\alpha_i\} \left\{ \right. \\ \\ Base\{\beta_j\} \left\{ \right. \\ \\ \end{array} \begin{array}{c} E \\ | \\ K \\ | \\ F \end{array}$$

Corolário 2.3.4. *Se $F \subset F_1 \subset F_2 \subset \cdots \subset F_n$ é uma torre de corpos, então:*

$$[F_n : F] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_2 : F_1][F_1 : F_0]$$

Demonstração. A prova sai direto do teorema 2.3.3 por indução. □

Corolário 2.3.5. *Se $F \subset K \subset E$ é uma torre de corpos, então E/F é uma extensão finita se e somente se E/K e K/F forem extensões finitas. Além disso, se E/F for finita, então os graus de E/K e K/F dividem o grau de E/F.*

Demonstração. A prova sai novamente do teorema 2.3.3. □

Se E é uma extensão de um corpo F e α_1 elemento de E, já vimos que o corpo obtido pela adjunção de α_1 a F é denotado por $F(\alpha_1)$. Da mesma forma, podemos adjuntar α_2 a $F(\alpha_1)$ tomando a avaliação $\varepsilon_{\alpha_2} : F(\alpha_1)[x] \to E$ obtendo como imagem $F(\alpha_1)(\alpha_2)$. $F(\alpha_1)(\alpha_2)$ é o menor corpo contendo $F(\alpha_1)$ e α_2 e será denotado por $F(\alpha_1, \alpha_2)$.

Definição 2.3.6. E/F é uma extensão finitamente gerada se existirem $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ tais que $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Lema 2.3.7. *E/F é uma extensão finita se, e somente se, for algébrica e finitamente gerada.*

Demonstração. ($\Rightarrow$) Se E/F é uma extensão finita e $\{\alpha_1, \ldots, \alpha_m\}$ é uma base de E como espaço vetorial sobre F, então se $\gamma \in E$ temos:

$$\gamma = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m$$

com $a_i \in F$. E, portanto, $E \subset F(\alpha_1, \ldots, \alpha_m)$. Como os α_i estão em E, é claro que $F(\alpha_1, \ldots, \alpha_m) \subset E$ e, assim, E/F é uma extensão finitamente gerada. Além disso E/F é algébrica pois se $\alpha \in E$, o conjunto $\{1, \alpha, \alpha^2, \ldots\}$ não pode ser l.i pois $dim E_F < \infty$ e, portanto α deve ser algébrico sobre F.

($\Leftarrow$) Suponhamos que E/F seja algébrica e finitamente gerada. Então $E = F(\alpha_1, \ldots, \alpha_m)$ para certos α_i. Assim:

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \ldots, \alpha_m)$$

E pelo corolário 2.3.5 como cada extensão intermediária é finita, então E/F é finita. □

Algumas propriedades serão úteis daqui pra frente e devo expô-las agora:

Lema 2.3.8. *Considere a torre de corpos $F \subset K \subset E$, então E/F é algébrica se, e somente se, E/K e K/F forem algébricas.*

Demonstração. ($\Rightarrow$) Se E/F é algébrica então se $\gamma \in E$ é raiz de um polinômio com coeficientes em F, é claro que é raiz de um polinômio com coeficientes em K, assim E/K é algébrica, e, se os elementos de E são algébricos sobre F, é claro que os elementos de K são também algébricos sobre F.

($\Leftarrow$) Se E/K e K/F são extensões algébricas, então se $\alpha \in E$ é algébrico sobre K, então existe um polinômio em K que tem α como raiz a saber $k(x) = k_0 + k_1x + k_2x^2 + \cdots + k_nx^n$ com os k_i em K. Assim, considere a torre de corpos:

$$F \subset F(k_0, k_1, \ldots, k_n) \subset F(\alpha, k_0, k_1, \ldots, k_n)$$

Sendo assim como K/F é algébrica, $F(k_0, k_1, \ldots, k_n)/F$ é algébrica e finitamente gerada, e portanto finita pelo lema 2.3.7. Da mesma forma como E/K é algébrica, $F(\alpha, k_0, k_1, \ldots, k_n)/F(k_0, k_1, \ldots, k_n)$ é também finita.

$$\begin{array}{c} F(\alpha, k_0, k_1, \ldots, k_n) \subset E \\ \Big| {<}\infty \\ F(k_0, k_1, \ldots, k_n) \subset K \\ \Big| {<}\infty \\ F \end{array}$$

E portanto $[F(\alpha, k_0, k_1, \ldots, k_n) : F] < \infty$ e, logo α é algébrico sobre F. □

2.4 Existência do Fecho Algébrico

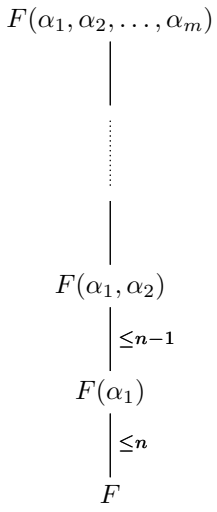
Do corolário 2.3.5 seque que se E é uma extensão de um corpo F e $\alpha, \beta \in E$ são algébricos sobre F, então $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$ e $\frac{\alpha}{\beta}, \beta \neq 0$ também são algébricos.

Já vimos no teorema 2.2.2 que sempre existe uma extensão que possui uma raiz de um polinômio dado. Precisamos mostrar que dado um corpo F, então também existe uma extensão que possui todas as raízes de seus polinômios em $F[x]$. Essa extensão será chamada de fecho algébrico.

Corolário 2.4.1. *Se F é um corpo e $f \in F[x]$ é um polinômio de grau $n \geq 1$, então existe um corpo L contendo F onde f possui todas as suas raízes.*

Demonstração. Para provar, basta utilizar o resultado do Kronecker repetidas vezes. Assim, se $f(x) \in F[x]$, então existe uma extensão de F que possui uma raiz α_1 de f, e já vimos que esta extensão é (a menos de isomorfismo) $F(\alpha_1)$. Agora fazemos o seguinte; fatoramos f em $F(\alpha_1)[x]$ e tomamos o resultado digamos $f_{(1)}(x)$ e sabemos que possui grau no máximo $n - 1$.

Assim, basta repetir o procedimento a fim de encontrar uma extensão que tenha uma raiz de $f_{(1)}(x)$, digamos α_2, e tomarmos a extensão $F(\alpha_1, \alpha_2)$ e assim por diante. É fácil perceber que no máximo em n passos construímos a extensão $F(\alpha_1, \alpha_2, \ldots, \alpha_m)$, cujo grau é, no máximo, $n!$.



□

Corolário 2.4.2. *Se F é um corpo e $f_1, f_2, \ldots, f_n \in F[x]$ são polinômios de grau ≥ 1, então existe um corpo L contendo F onde $f_1, f_2, \ldots, f_n$ possuem todas as suas raízes.*

Demonstração. Construímos da mesma maneira que no corolário anterior $F^{(1)}$ que tenha todas as raízes de f_1. Assim, basta repetir o procedimento $n-1$ vezes para $f_i, i = 2, ..., n$ e assim obter uma extensão que tenha todas as raízes desejadas. □

Definição 2.4.3. Um corpo E diz-se **algebricamente fechado** se todo polinômio $f(x) \in E[x]$ possui raiz em E e, portanto, possui todas as raízes em E.

Definição 2.4.4 (Fecho Algébrico)**.** Uma extensão E de um corpo F é chamada de **fecho algébrico** de F se E/F for algébrica e E for um corpo algebricamente fechado.

Definição 2.4.5 (Corpo de Decomposição)**.** Uma extensão E de um corpo F é chamada de **corpo de decomposição** para um polinômio $f \in F[x]$ se E contém todas as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ de f e é da forma $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Teorema 2.4.6. *Seja F um corpo. Então existe uma extensão de corpos E/F com E algebricamente fechado. Podemos também escolher E de modo que E/F seja algébrica e contruir assim o fecho algébrico de F denotado $\overline{F}$.*

Demonstração. A prova pode ser encontrada em [1]. □

2.5 Extensões de Morfismos

Na seção 2.2 definimos uma extensão de corpos como sendo simplesmente um corpo que contém outro corpo dado. A partir de agora precisamos definir extensões de homomorfismos de corpos.

Definição 2.5.1. Sejam $\sigma : F \to L$ e $\tau : E \to L$ homomorfismos de corpos tais que $F \subset E \subset L$ e τ restrito a F é σ ($\tau|_F = \sigma$), ou seja, se $x \in F$, então $\tau(x) = \sigma(x)$. Além disso, se σ for a identidade, então diremos que τ está sobre F.

Nesse caso diremos então que τ é uma **extensão** de σ.

Lema 2.5.1. *Se E/F for uma extensão algébrica e $\tau : E \to E$ um morfismo de corpos cuja restrição a F é a identidade (τ está sobre F), então τ é um isomorfismo.*

Demonstração. O ponto importante é que, como τ está sobre F, se $g \in F[x]$ for um polinômio e $\alpha \in E$, então τ vai fixar os coeficientes que estão em F. Assim:

$$\tau(g(\alpha)) = \tau(f_0 + f_1\alpha + \cdots + f_n\alpha^n) =$$

$$= f_0 + f_1\tau(\alpha) + \cdots + f_n\tau(\alpha)^n = g(\tau(\alpha))$$

temos então a seguinte equação:

$$\tau(g(\alpha)) = g(\tau(\alpha)) \tag{2.1}$$

Seja $\gamma \in E$ um elemento qualquer e $g(x) = irr(\gamma, F)(x)$. Seja $R = \{\beta \in E : g(\beta) = 0\}$ o conjunto das raízes de g e assim é claro que $\gamma \in R$. Vamos então utilizar 2.1 para ver o que o morfismo τ faz com γ.

$$\tau(g(\gamma)) = 0 = g(\tau(\gamma))$$

E portanto τ leva uma raiz de g em outra raiz de g.

Temos então que $\tau(R) \subset R$, e, como R é finito e τ é injetora, pois todo homomorfismo de corpos é injetor, $\tau(R) = R$, o que prova o lema. □

Se E for o corpo de decomposição de um polinômio irredutível $f \in F[x]$, então o isomorfismo de corpos $\tau : E \to E$ sobre F é, essencialmente, uma permutação das raízes de f.

Teorema 2.5.2. *Sejam F e L dois corpos, com L algebricamente fechado, se $E = F(\alpha)$, com α algébrico sobre F e $\sigma : F \to L$ um morfismo de corpos. Então existe uma extensão τ de σ, ou seja, existe um morfismo $\tau : E \to L$ tal que $\tau|_F = \sigma$.*

Demonstração. Seja $f(x) = Irr(\alpha, F)(x) \in F[x]$. Denotaremos por $f^\sigma \in L[x]$ o polinômio obtido pela aplicação de σ coeficiente a coeficiente. Como L é algebricamente fechado, existe $\beta \in L$ raiz de f^σ. Defino $\tau : F(\alpha) \to L$ assim:

$$\tau(g(\alpha)) := g^\sigma(\beta)$$

onde $g(x) \in F[x]$. Primeiro, vamos mostrar que τ está de fato bem definida.

Se $g(\alpha) = h(\alpha)$ para certo $h(x) \in F[x]$, então α é raiz de $t(x) = g(x) - h(x)$, pois $g(\alpha) - h(\alpha) = 0$ e, portanto, o polinômio irredutível $f(x)$ deve dividir $t(x)$.

Portanto, temos, para um certo $h(x) \in F[x]$:

$$t(x) = f(x)h(x)$$

$$t(x) - f(x)h(x) = 0$$

aplicando τ como definida.

$$t^\sigma(x) - f^\sigma(x)h^\sigma(x) = \sigma(0)$$

e como σ é um homomorfismo temos.

$$t^\sigma(x) = f^\sigma(x)h^\sigma(x)$$

Assim, $f^\sigma(x)$ divide $t^\sigma(x)$. o que prova que a definição de τ independe do particular polinômio g escolhido. Para mostrar que τ é homomorfismo de corpos basta ver que:

$$\tau(g(\alpha)h(\alpha)) = \tau(gh(\alpha))$$

$$gh^\sigma(\beta) = g^\sigma(\beta)h^\sigma(\beta)$$

$$= \tau(g(\alpha))\tau(h(\alpha))$$

e fazendo o mesmo para a soma vemos que claramente τ é um morfismo de corpos e $\tau|_F = \sigma$ o que termina a prova. □

Corolário 2.5.3. *Sejam F e L dois corpos com L algebricamente fechado, se E/F for uma extensão finita e $\sigma : F \to L$ um morfismo de corpos. Então existe uma extensão $\tau : E \to L$ de σ.*

Demonstração. Toda extensão finita é algébrica e finitamente gerada, isto é, $E = F(\alpha_1, \ldots, \alpha_n)$, com os α_j algébricos sobre F. Uma simples indução no número de geradores prova o corolário. □

Teorema 2.5.4. *Sejam F e L dois corpos com L algebricamente fechado, se E/F for uma extensão algébrica e $\sigma : F \to L$ um morfismo de corpos. Então existe uma extensão $\tau : E \to L$ de σ.*

Demonstração. A prova pode ser encontrada em [1]. □

2.6 Corpos de Decomposição

Definimos, na seção 2.4, corpo de decomposição de um determinado polinômio, mas, em geral, podemos definir corpos de decomposição para uma família de polinômios como abaixo.

Definição 2.6.1. Seja F um corpo e $\Lambda = \{f_\jmath\}_{\jmath \in J}$ uma família de polinômios de $F[x]$, todos de graus ≥ 1. Um corpo K/F diz-se um **corpo de decomposição** dessa família se:

1. Todo polinômio $f_\jmath \in \Lambda$ possui todas as suas raízes em K
2. $K = F(Z)$, onde $Z \subset K$ é o conjunto de todos os zeros de todos os elementos de Λ.

Tomemos a família $\Lambda = \{f\}$ constituída por um único polinômio $f(x)$. Então, se $\alpha_1, \ldots, \alpha_n$ são as raízes de f em K, temos $K = F(\alpha_1, \ldots, \alpha_n)$. Já sabemos pelo corolário 2.4.1, que tais corpos de decomposição existem.

Teorema 2.6.2. *Seja $\sigma : F \to F'$ um isomorfismo de corpos e $\Lambda \subset F[x]$ uma família de polinômios com graus ≥ 1. Se E/F é um corpo de decomposição para Λ e E' um corpo de decomposição para $\Lambda^\sigma = \{f^\sigma : f \in \Lambda\} \subset F'[x]$, então o isomorfismo σ se estende a um isomorfismo $\tau : E \to E'$.*

Demonstração. Seja $\overline{F}'$ um fecho algébrico de F' contendo E'. Assim, σ pode ser vista como um homomorfismo de F em $\overline{F}'$. Pelo Corolário 2.5.3, existe um morfismo $\tau : E \to \overline{F}'$ estendendo σ. Se $\alpha \in E$ for um zero de algum $f \in \Lambda$, então, como

$$0 = \tau(f(\alpha)) = f^\sigma(\tau(\alpha)),$$

vemos que $\tau(\alpha)$ é um zero de $f^\sigma \in \Lambda^\sigma$, ou seja: $\tau(\alpha) \in E'$ Mas $E = F(Z)$, onde Z é o conjunto dos zeros de Λ, de modo que $\tau(E) \subset E'$. Para provar que τ é um isomorfismo, tomo um fecho algébrico $\overline{F}$ de F e construímos $\theta : E' \to \overline{F}$, estendendo σ^{-1}. Observe que σ^{-1} está bem definida pois σ é bijetora e além disso novamente σ^{-1} pode ser vista como um morfismo de F' em $\overline{F}$ justificando assim a extensão θ.

O mesmo raciocínio, usado para τ, demonstra que $\theta(E') \subset E$. Agora considere as composições $\tau \circ \theta$ e $\theta \circ \tau$.

$$\tau \circ \theta : E \to E \qquad\qquad \theta \circ \tau : E' \to E'$$

são morfismos sobre F e assim, pelo lema 2.5.1, são automorfismos de E e E' respectivamente e portando τ é isomorfismo.

$$\begin{array}{ccc} E & \underset{\theta}{\overset{\tau}{\rightleftarrows}} & E' \\ {\scriptstyle \Lambda}\big| & & \big|{\scriptstyle \Lambda^\sigma} \\ F & \underset{\sigma^{-1}}{\overset{\sigma}{\rightleftarrows}} & F' \end{array}$$

□

Corolário 2.6.3. *Se $f \in F[x]$, então dois quaisquer corpos de decomposição para f são isomorfos.*

Teorema 2.6.4. *Seja K/F uma extensão algébrica e $\overline{F}$ um fecho algébrico de F contendo K. São equivalentes:*

1. *Todo morfismo $\sigma : K \to \overline{F}$ sobre F verifica: $\sigma(K) = K$.*
2. *K é o corpo de decomposição de alguma família Λ de polinômios de $F[x]$.*
3. *Se um polinômio irredutível de $F[x]$ possui uma raiz em K, então ele possui todas as raízes em K.*

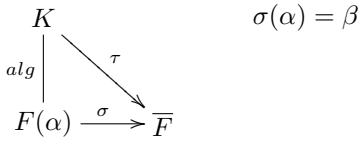
Demonstração.

(2) $\Rightarrow$ (1). Seja, então $K = F(Z)$, onde Z é o conjunto da raízes dos polinômios da família Λ, e $\sigma : K \to \overline{F}$ um morfismo sobre F. Então, se $\alpha \in Z$, $f(\alpha) = 0$ para algum $f \in \Lambda$,

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$$

ou seja, se $\sigma(Z) \subset Z$. Logo $\sigma(K) \subset K$. Assim, podemos enxergar $\sigma : K \to K$ sobre F e como Lema 2.5.1 garante que σ é um isomorfismo, então $\sigma(K) = K$.

(1) $\Rightarrow$ (3). Seja f um polinômio irredutível em $F[x]$ que possui uma raiz $\alpha \in K$. Seja $\beta \in \overline{F}$ uma raiz qualquer de f em $\overline{F}$. Como f é irredutível, já sabemos que existe um isomorfismo $\sigma : F(\alpha) \to F(\beta) \subset \overline{F}$ sobre F com $\sigma(\alpha) = \beta$. Assim temos a seguinte situação:



Nessa situação, podemos estender o morfismo σ a um morfismo $\tau : K \to \overline{F}$ usando o teorema 2.5.4. Então, como τ restrito a F é σ que por sua vez é sobre F, então τ é sobre F e pela hipótese (1), $\tau(K) = K$, donde

$$\tau(\alpha) = \sigma(\alpha) = \beta.$$

O que acarreta $\beta \in K$.

(3) $\Rightarrow$ (2). Seja Λ a família dos polinômios $f_\alpha(x) = Irr(\alpha, F)(x) \in F[x]$ para todo $\alpha \in K$. Assim, é claro que todo polinômio $f \in \Lambda$ tem todas as suas raízes em K. Falta mostrar que $K = F(Z)$. Isso é imediato dado que K/F é uma extensão algébrica.

Então como K/F é algébrica, é imediato por (3) que vale (2). □

Definição 2.6.5. Uma extensão algébrica K/F satisfazendo uma das condições equivalentes do Teorema 2.6.4 é chamada uma **extensão normal**.

Se $F \subset E \subset K$ é uma torre de corpos com K/E e E/F normais, a extensão K/F não é necessariamente normal, como mostra o exemplo: $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, e $K = \mathbb{Q}(\sqrt{\sqrt{2}}) = \mathbb{Q}(\sqrt[4]{2})$.

2.7 Extensões Separáveis

Teorema 2.7.1. *Seja L um corpo algebricamente fechado e $\sigma : F \to L$ um morfismo de corpos. Se α é algébrico sobre F, o número de extensões de σ a morfismos $\tau : F(\alpha) \to L$ é igual ao número de raízes distintas do $irr(\alpha, F)(x)$.*

Demonstração. Seja R o conjunto das raízes distintas do polinômio $irr(\alpha, F)^\sigma(x)$ $= \sigma(irr(\alpha, F)(x))$ em L. Como L é algebricamente fechado, $irr(\alpha, F)^\sigma(x)$ tem todas as suas raízes em L. É claro que $|R|$ é igual ao número de raízes distintas de $irr(\alpha, F)(x)$ em algum fecho algébrico de F. Seja o conjuntos das extensões τ de σ: $S_\sigma(L) = \{\tau : F(\alpha) \to L : \tau|_F = \sigma\}$ e seja $\phi : S_\sigma \to R$ a função dada por

$$\phi(\tau) = \tau(\alpha).$$

Observe que $\tau(irr(\alpha, F)(\alpha)) = 0 = irr(\alpha, F)^\sigma(\tau(\alpha))$ e portanto $\tau(\alpha) \in R$.
ϕ está bem definida pois se:

$$\tau = \theta \Rightarrow \tau(\alpha) = \theta(\alpha) \Rightarrow \phi(\tau) = \phi(\theta)$$

e é claramente injetora já que só precisamos nos preocupar com o que os morfismos fazem com α.

$$\phi(\tau) = \phi(\theta) \Rightarrow \tau(\alpha) = \theta(\alpha) \Rightarrow \tau = \theta$$

Por outro lado, se $\beta \in R$, sabemos que

$$\tau(g(\alpha)) := g^\sigma(\beta)$$

define um elemento de S. Como $\phi(\tau) = \tau(\alpha) = \beta$, ϕ é uma bijeção. □

Seja E/F uma extensão algébrica de corpos fixada e $\sigma : F \to L$ um morfismo de corpos, com L algebricamente fechado. Já vimos que o conjunto $S_\sigma(L) = \{\tau : E \to L : \tau|_F = \sigma\}$ é não vazio. Pode-se mostrar que a cardinalidade de $S_\sigma(L)$ depende somente da extensão algébrica E/F. Será denotada por $[E : F]_S$ e será chamado **grau de separabilidade** de E sobre F.

Teorema 2.7.2. *Seja $K \subset F \subset E$ uma torre finita de corpos. Então*

$$[E : K]_S = [E : F]_S[F : K]_S$$

e, além disso, se L/M for uma extensão finita, então

$$[L : M]_S \leq [L : M].$$

Demonstração. Para provar a primeira parte, basta observar que se $\sigma : K \to L$, então para cada extensão $\tau : F \to L$ de σ, teremos $[E : F]_S$ extensões de τ. Como temos $[F : K]_S$ morfismos τ, então vamos ter $[E : F]_S[F : K]_S$ extensões $\theta : E \to L$.

Se L/M é finita, então $L = M(\alpha_1, \ldots, \alpha_n)$, para certos elementos algébricos $\alpha_1, \ldots, \alpha_n \in L$. Então

$$M \subset M(\alpha_1) \subset M(\alpha_1, \alpha_2) \subset \cdots \subset M(\alpha_1, \ldots, \alpha_n) = L.$$

Como $[M(\alpha_1, \ldots, \alpha_{j+1}) : M(\alpha_1, \ldots, \alpha_j)]_S$ é igual ao número de raízes distintas do polinômio $Irr(\alpha_{j+1}, M(\alpha_1, \ldots, \alpha_j))(x)$, pela multiplicatividade dos graus temos o teorema. □

É interessante observar que, como o grau de separabilidade de uma extensão $F(\alpha)/F$ depende do número de raízes **distintas** do polinômio irredutível de α em F, nos casos em que pudermos garantir que os polinômios irredutíveis não possuem raízes múltiplas, então o grau de separabilidade será igual ao grau do polinômio irredutível e portanto igual ao grau da extensão.

Corolário 2.7.3. *Seja $K \subset F \subset E$ uma torre de extensões finita. Então*

$$[E : K]_S = [E : K] \Leftrightarrow [E : F]_S = [E : F] \ e \ [F : K]_S = [F : K]$$

Definição 2.7.4. Seja E/F uma extensão finita. E/F diz-se uma extensão separável se $[E : F]_S = [E : F]$

Definição 2.7.5. Seja E/F uma extensão qualquer. O elemento $\alpha \in E$, algébrico, diz-se separável sobre F se a extensão $F(\alpha)/F$ for separável.

Definição 2.7.6. Se $f \in F[x]$, f diz-se um polinômio separável se o número de raízes distintas for igual ao grau de f.

Se E/F for uma extensão finita separável e $\alpha \in E$, o corolário acima garante que $F(\alpha)/F$ será uma extensão separável, e, assim, todo elemento de E será se-parável sobre F. Logo, $irr(\alpha, F)(x)$ será um polinômio separável. Por outro lado, se $f(x) \in F[x]$ for um polinômio separável e $\alpha \in \overline{F}$ for raiz de f, então como $irr(\alpha, F)(x)$ divide $f(x)$, α será um elemento separável sobre F. Vamos resumir essas observações num lema:

Lema 2.7.7. *Uma extensão finita E/F é separável se e somente se cada elemento de E for separável sobre F. Além disso, se E/F for uma extensão finita gerada por elementos separáveis sobre F, então ela será separável.*

Definição 2.7.8. Seja $f \in F[x]$ um polinômio e E/F uma extensão de corpos onde f possui uma raiz $\alpha \in E$. Então $f(x) = (x - \alpha)^m g(x)$ em $E[x]$, onde $(x - \alpha)$ não divide $g(x)$. Dizemos que α é uma raiz múltipla de f se $m \geq 2$. Caso contrário, dizemos que α é uma raiz simples. É claro que todas as raízes de f são simples (num corpo de decomposição para f) se e somente se o número de raízes distintas de f for igual ao grau de f.

Precisamos de um critério simples que nos diga quando um polinômio é separável, ou seja, quando um polinômio possui apenas raízes simples. Para isso, vamos trazer a idéia de derivada da Análise para a Álgebra. Podemos começar com o seguinte exemplo:

1. $F = \mathbb{R}$.

   Se $f(x) = (x-\alpha)^2 g(x) \in \mathbb{R}[x]$, então a derivada será $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$ e portanto $(x-\alpha)$ divide $f(x)$ e $f'(x)$. Nesse caso, vemos que $f(x)$ possui uma raiz dupla α e $f'(x)$ possui uma raiz simples. Portanto fica claro que se um polinômio tem uma raiz múltipla α, então a sua derivada também terá α como raiz.

Na análise a derivada é definida tomando-se o limite $\lim_{h\to 0} \frac{f(x+h)-f(x)}{h}$, mas aqui nem sempre para todo corpo F faz sentido tomar h tão perto de zero quanto se queira ($h \to 0$). Portanto façamos o seguinte.

Seja $f(x) \in F[x]$ um polinômio de grau ≥ 1. Tomemos h outra variável independente sobre $F[x]$. O polinômio $f(x+h) \in F[x,h]$ pode ser escrito:

$$f(x+h) = f_0(x) + f_1(x)h + \cdots + f_n(x)h^n,$$

onde $f_j(x) \in F[x]$. Fazendo $h = 0$ percebemos que $f_0(x) = f(x)$. Isso implica que h divide $f(x+h) - f(x)$, donde

$$\frac{f(x+h)-f(x)}{h} = f_1(x) + f_2(x)h + \cdots + f_n(x)h^{n-1}.$$

Como exemplo, seja $f(x) = ax^2$, então:

$$f(x+h) = a(x+h)^2 = x^2 + 2axh + h^2$$

$$f(x+h) - x^2 = 2axh + h^2 \tag{2.2}$$

$$\frac{f(x+h)-f(x)}{h} = 2ax + h$$

Repare que podemos dividir os dois lados de 2.2 por h já que o segundo lado é claramente divisível por h. E assim é bastante conveniente definir a derivada de ax^2 como sendo $2ax$.

Podemos, então, definir a derivada de $f(x)$ como sendo o polinômio $f_1(x)$. Usaremos a notação usual para a derivada: $f'(x)$. É claro que vale a congruência:

$$f(x+h) \equiv f(x) + f'(x)h \qquad mod\ h^2$$

E essa congruência determina univocamente a derivada: se, para algum polinômio $g(x) \in F[x]$ tivermos $f(x+h) \equiv f(x) + g(x)h \bmod h^2$ então $f'(x)h \equiv g(x)h \bmod h^2$ donde $f'(x) \equiv g(x) \bmod h$. Isso acarreta $f'(x) = g(x)$, pois h é transcendente sobre $F[x]$. Uma aplicação direta da congruência acima garante que:

1. $(f+g)' = f' + g', \qquad \forall f, g \in F[x].$
2. $(fg)' = f'g + fg', \qquad \forall f, g \in F[x].$

3. $(af)' = af'$, $\forall a \in F, \forall f \in F[x]$.

4. Se $f(x) = x$, então $f' = 1$.

Lema 2.7.9. *Se $f(x) = x^n$ é um polinômio em $F[x]$, então $f'(x) = nx^{n-1}$, para todo natural $n \geq 1$.*

Demonstração. Vamos provar por indução sobre n. Claramente vale para $n = 1$. Então suponha que vale para $n-1$, assim:

$$(x^n)' = [x(x^{n-1})]' = x^{n-1} + x(n-1)(x^{n-2}) = x^{n-1} + (n-1)x^{n-1} = nx^{n-1}$$

□

Além disso, como $1^2 = 1$, se $f(x) = 1$, então $(ff)' = f' = f'f + ff' = 2f'$, ou seja, $1' = 0$. Portanto, se $f(x) = a_0 + a_1x + \cdots + a_nx^n$, com $a_j \in F$,

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

Agora que temos tal critério, podemos enunciar o seguinte teorema:

Teorema 2.7.10. *Seja $f \in F[x]$ um polinômio de grau ≥ 1. Então todas as raízes de f são simples (num corpo de decomposição para f) se, e somente se, o maior divisor comum de f e f' for 1.*

Demonstração. Seja E/F um corpo de decomposição para f. Suponhamos que todas as raízes de f sejam simples. Então, em E, temos

$$f(x) = \prod_{j=1}^{n}(x - \alpha_j),$$

com $\alpha_i \neq \alpha_j$ se $i \neq j$. Para provar que a derivada de f não possui nenhum dos fatores $(x - \alpha_i)$ basta notar que:

$$\begin{aligned} f'(x) &= \left[(x-\alpha_i)\prod_{j=1, j\neq i}^{n}(x-\alpha_j)\right]' = [(x-\alpha_i)g(x)]' \\ &= (x-\alpha_i)'g(x) + 1g'(x) \end{aligned}$$

vemos que como $g(x)$ não possui fator do tipo $(x - \alpha_i)$ então $g'(x)$ certamente também não terá. Assim vemos que $(x-\alpha_i)$ não divide $f'(x)$ para todo i. Logo, $(f, f') = 1$. Se $f(x)$ possuir uma raiz múltipla $\alpha \in E$, então $f(x) = (x-\alpha)^m g(x)$, com $m \geq 2$. Derivando obtemos:

$$f'(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x).$$

Assim $f'(\alpha) = 0$, donde $(f, f') \neq 1$, $(x-\alpha)$ divide tanto f quanto f'. Isso prova o teorema. □

Corolário 2.7.11. *Seja F um corpo de característica zero e $f \in F[x]$ um polinômio irredutível de grau ≥ 1. Então f é separável.*

Demonstração. O importante aqui é perceber que a derivada de um polinômio irredutível não pode ter um fator comum com esse irredutível, pois já vimos pelo teorema 2.2.4 que o irredutível é um polinômio de grau mínimo que possui uma dada raiz. Se $(f, f') \neq 1$ em $F[x]$ então, como f é irredutível, $(f, f') = f$, o que acarreta f divide f'. Como em característica zero f' não pode ser identicamente nula e o grau de f' é menor que o grau de f, isso é impossível. □

Corolário 2.7.12. *Se F é um corpo de característica zero, então toda extensão finita E/F é separável.*

Demonstração. Seja $\alpha \in E$. Como α é raiz do polinômio $irr(\alpha, F)(x)$, que é separável, pelo corolário acima, o Lema 2.7.7 garante que E/F é separável. □

2.8 Elemento Primitivo

Seja E/F uma extensão de corpos. Um elemento $\alpha \in E$ diz-se um elemento primitivo de E sobre F se $E = F(\alpha)$.

Teorema 2.8.1. *Se E/F for finita e separável, então existe $\alpha \in E$ tal que $E = F(\alpha)$.*

Demonstração. Basta considerar o caso em que $E = F(\alpha, \beta)$, com α, β separáveis sobre F e F um corpo infinito, pois se $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ então podemos tomar os α_i's dois a dois para reduzir o número de geradores. Por outro lado, se F for finito, então E também será e pode-se mostrar que existe um elemento que gera todo E, exceto o zero, mas esse caso não interessa a esse trabalho.

Suponhamos então, que $[E : F] = n$. Por hipótese, existem n morfismo distintos $\{\sigma_1, \ldots, \sigma_n\}$ de E em $\overline{F}$ sobre F. Consideremos o polinômio na variável x:

$$f(x) = \prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha) + x[\sigma_i(\beta) - \sigma_j(\beta)]).$$

Então $f(x) \not\equiv 0$ pois senão $\sigma_i(\alpha) = \sigma_j(\alpha)$ e $\sigma_i(\beta) = \sigma_j(\beta)$ para certos $i \neq j$. Isso acarretaria $\sigma_i = \sigma_j$. Assim, existe $c \in F$ tal que $f(c) \neq 0$ (o corpo F é infinito, e um polinômio não nulo só possui um número finito de raízes), e, portanto, os elementos de $\sigma_j(\alpha + c\beta)$ são todos distintos, pois:

$$\begin{aligned} f(c) &= \prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha) + c[\sigma_i(\beta) - \sigma_j(\beta)]) \neq 0 \\ &= \prod_{i \neq j} (\sigma_i(\alpha + c\beta) - \sigma_j(\alpha + c\beta)) \neq 0 \end{aligned}$$

e assim o número de morfismo de $F(\alpha + c\beta)$ em $\overline{F}$ é pelo menos n. E então:

$$[F(\alpha + c\beta) : F] = [F(\alpha + c\beta) : F]_S \geq n = [F(\alpha, \beta) : F]$$

já que esses elementos distintos são raízes do $Irr(\alpha+c\beta, F)(x)$. Como $F(\alpha+c\beta) \subset F(\alpha, \beta)$, temos a igualdade. □

Capítulo 3

Teorema Fundamental da Teoria de Galois

3.1 Definições

Definição 3.1.1. Uma extensão algébrica K/k é dita uma extensão de Galois se for normal e separável.

Definição 3.1.2. O grupo de todos os automorfismos de K que são sobre k, denotado $Gal(K/k)$, é chamado o **Grupo de Galois** da extensão K/k.

No Teorema fundamental encontra-se o cerne da base teórica para o presente trabalho. A propriedades necessárias para a prova dos algoritmos do capítulo 4 são quase que conseqüências diretas dos resultados expostos aqui. Portanto, o entendimento desse teorema é imprescindível para a compreensão dos algoritmos.

Observe que o grupo dos automorfismos de K que são sobre k, são as extensões τ da identidade $\imath : k \to \overline{k}$ pois, pelo teorema 2.6.4, toda extensão desse tipo é um automorfismo.

$$\begin{array}{ccc} K & & \tau(K) = K \\ {\scriptstyle galois}\big| & \searrow^{\tau \in Gal(K/k)} & \\ k & \xrightarrow{\imath} & \overline{k} \end{array}$$

Tudo o que fizemos até agora serve para construir extensões da identidade passo a passo. Sabemos exatamente quantas extensões temos, pois o corpo de base será sempre $\mathbb{Q}$, de característica zero, e, portanto, separável. Assim:

$$|Gal(K/k)| = [K : k]_S = [K : k]$$

De maneira grosseira, o teorema fundamental estabelece uma relação de correspondência entre o reticulado de subcorpos de um corpo de decomposição

de um polinômio irredutível e o reticulado dos subgrupos do grupo de Galois. A seguir daremos uma ilustração desse fato:

O corpo $K = \mathbb{Q}(\sqrt{2}, i)$ é o corpo de decomposição da família $\Lambda = \{x^2 - 2, x^2 + 1\}$ e, portanto, é normal sobre $k = \mathbb{Q}$ (teorema 2.6.4). Como o corpo $\mathbb{Q}$ possui característica 0, K/k é uma extensão separável de k (corolário 2.7.11). Além disso, como $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, $x^2 + 1$ é irredutível sobre $\mathbb{Q}(\sqrt{2})$ de onde $[K : k] = [K : k]_s = 4$. Temos exatamente duas extensões da identidade $\imath : k \to \overline{k}$, para morfismos $\tau_j : \mathbb{Q}(\sqrt{2}) \to \overline{k}$, a saber: $\tau_1(\sqrt{2}) = \sqrt{2}$ e $\tau_2(\sqrt{2}) = -\sqrt{2}$.

Cada um dos morfismos, τ_i, possui duas extensões σ_i, pois $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ que permutam as raízes de $x^2 + 1 = 0$.

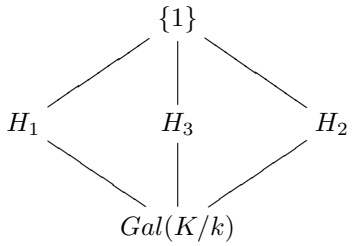
Tabela 3.1: Automorfismos do $Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$

	1	2	3	4
	$\sqrt{2}$	$-\sqrt{2}$	i	$-i$
σ_1	$\sqrt{2}$	$-\sqrt{2}$	i	$-i$
σ_2	$\sqrt{2}$	$-\sqrt{2}$	$-i$	i
σ_3	$-\sqrt{2}$	$\sqrt{2}$	i	$-i$
σ_4	$-\sqrt{2}$	$\sqrt{2}$	$-i$	i

Os automorfismos σ_i permutam as raízes da família Λ e, portanto, podemos identificar as raízes na segunda linha da tabela acima com 1, 2, 3 e 4 respectivamente para criar a inclusão $Gal(K/k) \to \mathfrak{S}_4$ dada por

$$\sigma_1 = 1, \sigma_2 = (34), \sigma_3 = (12), \sigma_4 = (12)(34),$$

e, se pusermos $H_1 =< (12) >$, $H_2 =< (34) >$, $H_3 =< (12)(34) >$, o reticulado dos subgrupos é o seguinte:



Como já foi dito, o grupo de Galois permuta as raízes do corpo de decomposição e vale a pena frisar algumas de suas propriedades.

1. As permutações não mexem nos elementos do corpo de base, $\mathbb{Q}$, e dizemos, nesse caso, que o grupo fixa $\mathbb{Q}$. Essa propriedade vem da própria definição.

2. Por outro lado, com algum esforço pode-se mostrar que todas as funções das raízes $\{\sqrt{2}, -\sqrt{2}, i, -i\}$ que ficam fixas pelo grupo de Galois são elementos de $\mathbb{Q}$.

3. Cada subgrupo do grupo de Galois, no caso (H_1, H_2, H_3), fixam determinados subcorpos de $K = \mathbb{Q}(\sqrt{2}, i)$.

Vamos agora nos concentrar na propriedade 3. Antes precisamos da seguinte definição:

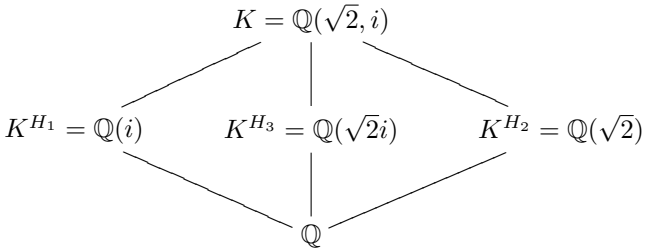
Definição 3.1.3. Seja K um corpo e H um grupo de automorfismos de K. Então K^H será o conjunto de elementos de K fixos por H, ou seja, $K^H = \{x \in K \mid \sigma(x) = x \ \forall \sigma \in H\}$. É fácil ver que K^H é subcorpo de K.

Assim, tentaremos encontrar os subcorpos fixos por cada um dos subgrupos H_1, H_2 e H_3). Como $H_1 =< (12) >$, então no fundo H_1 permuta a primeira raiz $(\sqrt{2})$ com a segunda $(-\sqrt{2})$, deixando o i fixo. Portanto parece razoável que H_1 fixe $\mathbb{Q}(i)$. Para mostrar que $\mathbb{Q}(\sqrt{2}, i)^{H_1} = \mathbb{Q}(i)$ basta observar que não existe nenhum subcorpo de $\mathbb{Q}(\sqrt{2}, i)$ que contenha i além de $\mathbb{Q}(i)$, pois $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(i)] = 2$.

Da mesma forma, $H_2 =< (34) >$ fixa claramente $\sqrt{2}$ e pela mesma razão $\mathbb{Q}(\sqrt{2}, i)^{H_2} = \mathbb{Q}(\sqrt{2})$.

Agora, no caso do grupo $H_3 =< (12)(34) >$, temos que ter um pouco mais de habilidade. Esse grupo permuta a raiz 1 com 2 e a raiz 3 com a raiz 4. Assim é claro que H_3 leva $\sqrt{2}i \to (-\sqrt{2})(-i) = \sqrt{2}i \in \mathbb{Q}(\sqrt{2}, i)$ raiz de $x^2 + 2 = 0$. Novamente não há corpos intermediários entre $\mathbb{Q}(\sqrt{2}, i)$ e $\mathbb{Q}(\sqrt{2}i)$.

Como os elementos da extensão $\mathbb{Q}(\sqrt{2}, i)$ são da forma $a\sqrt{2} + b\sqrt{2}i + ci$, pode-se mostrar que não há mais corpos intermediários entre $\mathbb{Q}(\sqrt{2}, i)$ e $\mathbb{Q}$. Assim temos o seguinte reticulado de corpos:



Podemos agora partir para a formalização do teorema fundamental.

3.2 Teorema Fundamental

Teorema 3.2.1 (Teorema Fundamental)**.** *Seja K/k uma extensão de Galois finita. Então existe uma correspondência bijetora entre o conjunto $\mathcal{S}_C$ dos subcorpos E de K/k e o conjunto $\mathcal{S}_G$ dos subgrupos H de $G = Gal(K/k)$, dada por*

$$E \longmapsto Gal(K/E).$$

A função inversa é dada por $H \longmapsto K^H$. Essa correspondência entre subcorpos e subgrupos possui as seguintes propriedades:

1. $H_1 \supset H_2 \iff K^{H_1} \subset K^{H_2}$
2. $|H| = [K : K^H]$, *e* $[G : H] = [K^H : k]$.
3. $H \lhd G \iff K^H/k$ *é normal. Nesse caso,*

$$Gal(K^H/k) \cong G/H.$$

4. $H_1 \cap H_2$ *corresponde ao compositum* $K^{H_1}K^{H_2}$
5. $E_1 \cap E_2$ *corresponde ao subgrupo* $< Gal(K/E_1), Gal(K/E_2) >$

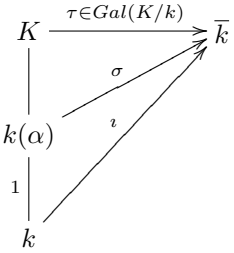
Para auxiliar na demonstração do teorema fundamental, primeiramente provaremos as seguintes proposições:

Proposição 3.2.2. *Seja K/k uma extensão de Galois finita e $G = Gal(K/k)$ o seu grupo de Galois. Então $k = K^G$ é o corpo fixo pelo grupo de Galois. Além disso, se $k \subset F \subset K$, a extensão K/F é de Galois e a função $\mathcal{G} : \mathcal{S}_C \to \mathcal{S}_G$ dada por:*

$$\mathcal{G}(F) := Gal(K/F)$$

é injetora.

Demonstração. Como G é o conjunto dos automorfismos de K que fixam k, então é claro que k está contido no corpo fixo por G, assim $k \subset K^G$. Por outro lado, seja $\alpha \in K^G$ e $\sigma : k(\alpha) \to \overline{k}$ um morfismo sobre k. Podemos tomar uma extensão $\tau : K \to \overline{k}$ de σ. Como K/k é normal e separável, temos que $\tau \in Gal(K/k) = G$ e portanto fixa α e assim σ também fixa α e temos que $[k(\alpha) : k]_S = [k(\alpha) : k] = 1$ e por conseqüência $\alpha \in k$. Um diagrama pode ajudar nessa difícil demonstração.



$$\tau(\alpha) = \alpha \Rightarrow \sigma(\alpha) = \alpha \Rightarrow [k(\alpha) : k]_S = 1$$

Com o mesmo argumento pode-se perceber que, se $k \subset F \subset K$, então $F = K^{Gal(K/F)}$.

Pelo corolário 2.7.3 temos que K/F é separável e pelo teorema 2.6.4 é normal, e portanto, é de Galois.

Pela observação acima, se $Gal(K/F_1) = Gal(K/F_2)$ então:

$$F_1 = K^{Gal(K/F_1)} = K^{Gal(K/F_2)} = F_2$$

o que mostra que $\mathcal{G}$ é injetora. □

Proposição 3.2.3. *Seja K um corpo qualquer e G um grupo finito de automorfismos de K, $|G| = n$. Seja $k = K^G$ o corpo fixo por G. Então K/k é uma extensão de Galois finita de grau n e $Gal(K/k) = G$.*

Demonstração. O grupo G age naturalmente em K e se $\alpha \in K$, então a órbita de α sob ação de G é $o(\alpha) = \{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_r(\alpha)\}$, onde σ_1 é a identidade de G. Assim α é raiz do seguinte polinômio separável.

$$f(x) = \prod_{i=1}^{r}(x - \sigma_i(\alpha))$$

Pode-se ver que se $\tau \in G$, então os conjuntos $\{\tau(\sigma_1(\alpha)), \tau(\sigma_2(\alpha)), \ldots, \tau(\sigma_r(\alpha))\}$ e $o(\alpha)$ são o mesmo, exceto pela ordem e, portanto, $\tau(f(x)) = f(x)$, o que implica que os coeficientes de $f(x)$ estão em k. Além disso, o $irr(\alpha, k)$ divide $f(x)$ que é separável, e, portanto, α é separável sobre k e $[k(\alpha) : k] \leq r$. Pelo lema 2.7.7, temos que K/k é separável. E Pelo teorema 2.6.4, vemos que K/k é também normal e, portanto, é de Galois.

Para mostrar que K/k é finita, basta observar que como vimos acima, todo elemento α de K tem grau no máximo n e, se K/k fosse infinita, algum elemento teria grau maior que n.

Então seja θ o elemento primitivo de K/k. Então $K = k(\theta)$ e $[k(\theta) : k] \leq n$. Por outro lado, $G \subset Gal(K/k)$ e o número de automorfismos de K sobre k é pelo menos n. Portanto $[K : k]_S = [K : k] \geq n$. Assim K/k é uma extensão de Galois de grau n e $G = Gal(K/k)$. Podemos obviamente concluir também que $|G| = [K : K^G]_S = [K : K^G]$ □

Prova do Teorema Fundamental. Consideremos a função

$$\mathcal{C} : \mathcal{S}_G \longrightarrow \mathcal{S}_C$$

dada por $H \mapsto K^H$. A Proposição 3.2.2 mostrou que

$$\mathcal{C}(\mathcal{G}(F)) = F,$$

ou seja, $\mathcal{G}$ é injetora e $\mathcal{C}$ é sobrejetora. Pela Proposição 3.2.3, se $H \in \mathcal{S}_G$, então K/K^H é uma extensão de Galois cujo grupo de Galois é H, ou seja

$$\mathcal{G}(\mathcal{C}(H)) = \mathcal{G}(K^H) = Gal(K/K^H) = H.$$

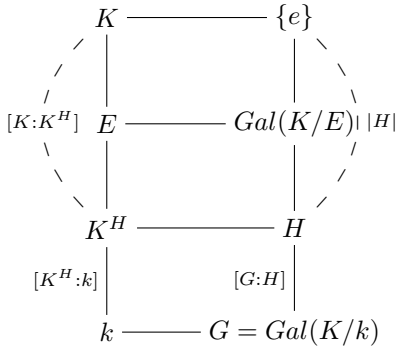
Assim, estabelecemos a bijeção de que fala o teorema fundamental. Vejamos as propriedades básicas.

1. Se $H_1 \supset H_2$ então é claro que $K^{H_1} \subset K^{H_2}$, pois se $\alpha \in K^{H_1}$, α é fixo por H_1 e, portanto é fixo por H_2 donde $\alpha \in K^{H_2}$. Reciprocamente, se $K^{H_1} \subset K^{H_2}$, e $\sigma \in H_2 = Gal(K/K^{H_2})$, então σ é um automorfismo de K que fixa K^{H_2} e, consequentemente fixa K^{H_1} donde $\sigma \in Gal(K/K^{H_1}) = H_1$.

2. A Proposição 3.2.3 implica $|H| = [K : K^H]$. Como $[G : H] = |G|/|H|$, podemos escrever

$$[G : H] = \frac{|G|}{|H|} = \frac{[K : k]}{[K : K^H]} = \frac{[K : K^H][K^H : k]}{[K : K^H]} = [K^H : k].$$

   Vamos resumir os resultados obtidos até agora no seguinte diagrama:



3. $G = Gal(K/k)$ e já vimos que $H = Gal(K/K^H)$. Assim, K^H é normal sobre k se e só se K^H é corpo de decomposição sobre k e isso ocorre se e só se todo morfismo $\sigma : K^H \to \bar{k}$ verifica $\sigma(K^H) = K^H$.

   Como os morfismos de $Gal(K/k)$ são extensões dos morfismos de $Gal(K^H/k)$ então $\forall \sigma \in Gal(K/k)$ temos que se $\alpha \in K^H$, então $\sigma(\alpha) \in K^H$.

   Portanto, K^H/k é normal se e só se $\forall \sigma \in Gal(K/k)$ e $\alpha \in K^H$ temos $\sigma(\alpha) \in K^H$.

   Se $\tau \in Gal(K/K^H)$, τ fixa K^H e, portanto, K^H/k é normal se e só se

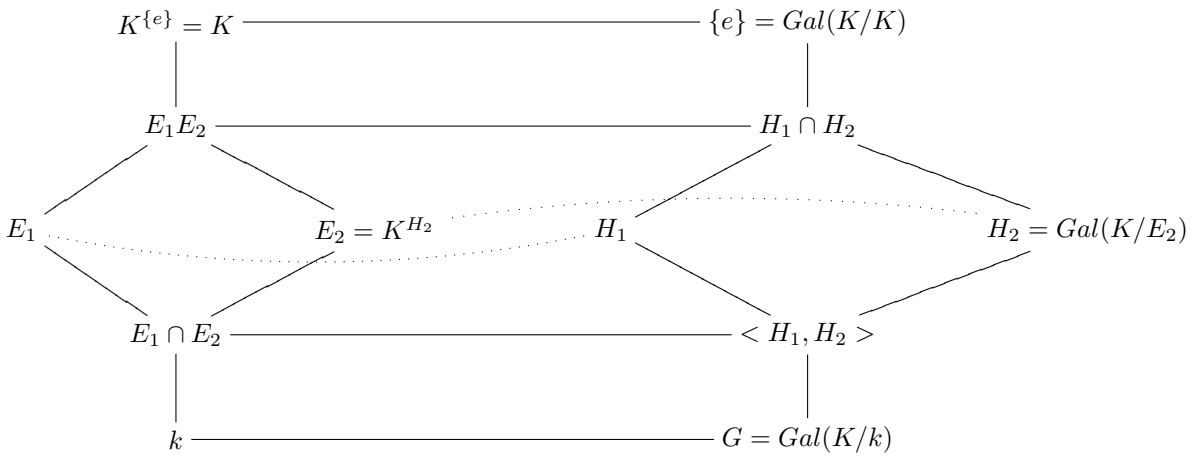
$$\begin{aligned} & \tau(\sigma(\alpha)) = \sigma(\alpha) \\ \Leftrightarrow \quad & \sigma^{-1}\tau\sigma(\alpha) = \alpha \\ \Leftrightarrow \quad & \sigma^{-1}\tau\sigma \in Gal(K/K^H) \\ \Leftrightarrow \quad & Gal(K/K^H) \lhd Gal(K/k) \\ \Leftrightarrow \quad & H \lhd G. \end{aligned}$$

4. Seja $\sigma \in H_1 \cap H_2$. Então σ fixa $F_1 = K^{H_1}$ e fixa $F_2 = K^{H_2}$, ou seja, σ fixa o compositum F_1F_2. A recíproca é clara.

5. Sejam E_1 e E_2 corpos intermediários, $E_1 = K^{H_1}$ e $E_2 = K^{H_2}$. Se $x \in E_1 \cap E_2$ então x é fixo por H_1 e fixo por H_2, donde x é fixo por $< H_1, H_2 >$. Se $y \in K$ fica fixo por $< H_1, H_2 >$, então, em particular y fica fixo por H_1 e por H_2, donde $y \in E_1 \cap E_2$. Isso termina a prova do teorema fundamental da teoria de Galois.

□

O resultado do teorema pode ser entendido pelo diagrama abaixo:



Podemos, agora, estudar um exemplo importante que será utilizado no próximo capítulo.

Corolário 3.2.4. *Se $s_1, s_2, \ldots, s_n$ são variáveis independentes sobre $\mathbb{Q}$ e $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n \in \mathbb{Q}(s_1, \ldots, s_n)[x]$ o polinômio geral de grau n. Então, seu grupo de Galois é o $\mathfrak{S}_n$.*

Demonstração. Sejam $x_1, x_2, \ldots, x_n$ as raízes de f e sabemos por Girard que:

$$\begin{array}{rcl} s_1 & = & x_1 + x_2 + \cdots + x_n \\ s_2 & = & x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ \vdots & & \vdots \\ s_n & = & x_1x_2 \ldots x_n \end{array}$$

Portanto, é claro que $k = \mathbb{Q}(s_1, \ldots, s_n) \subset K = \mathbb{Q}(x_1, \ldots, x_n)$. K é o corpo de decomposição de $f(x)$ e K/k é uma extensão normal e separável. E sabemos que seu grupo de Galois $Gal(K/k)$ pode ser visto como um subgrupo de $\mathfrak{S}_n$.

Pode-se mostrar que $x_1, x_2, \ldots, x_n$ são algebricamente independentes sobre $\mathbb{Q}$. Assim, se $\tau \in \mathfrak{S}_n$, vamos mostrar que τ induz um automorfismo de K que fixa k. Se $f(x_1, x_2, \ldots, x_n) \in K$, então definimos:

$$\tau f(x_1, x_2, \ldots, x_n) \doteq f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)})$$

Por Girard, temos que $\tau(s_i) = s_i$. E então, basta ver que τ está bem definida. Assim, se:

$$f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n)$$

então,

$$f(x_1, x_2, \ldots, x_n) - g(x_1, x_2, \ldots, x_n) = 0$$

Como, as raízes $x_1, x_2, \ldots, x_n$ são algebricamente independentes sobre $\mathbb{Q}$, então isso só é possível se $f = g$.

□

Portanto, $Gal(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(s_1, \ldots, s_n)) = \mathfrak{S}_n$. Podemos, representar esse fato no diagrama abaixo:

$$\begin{array}{ccc} \mathbb{Q}(x_1, x_2, \ldots, x_n) & \text{——} & \{e\} \\ \Big| {\scriptstyle n!} & & \Big| {\scriptstyle n!} \\ \mathbb{Q}(s_1, s_2, \ldots, s_n) & \text{——} & \mathfrak{S}_n \end{array}$$

Capítulo 4

Algoritmos

4.1 Resolventes

Consideremos $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n$ com n raízes a saber $x_1, x_2, \ldots, x_n$ algebricamente independentes, como feito em 3.2.4. Considere então a extensão $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(s_1, \ldots, s_n)$ e considere o subgrupo $A_n \leq \mathfrak{S}_n$ e vamos estudar o subcorpo fixo de $\mathbb{Q}(x_1, \ldots, x_n)$ por A_n.

Queremos encontrar um elemento de $\mathbb{Q}(x_1, \ldots, x_n)$, que fica fixo pela ação do A_n. Lembremos que se $\tau \in \mathfrak{S}_n$, então τ induz um automorfismo dado por:

$$\tau h(x_1, x_2, \ldots, x_n) \doteq h(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)})$$

Assim é natural considerarmos o discriminante de f:

$$\boldsymbol{\Delta} = \boldsymbol{\Delta}(\mathbf{x_1}, \ldots, \mathbf{x_n}) = \prod_{\mathbf{i<j}} (\mathbf{x_j} - \mathbf{x_i}) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix}$$

pois, se aplicarmos uma transposição $\tau = (ij)$ a Δ teremos como resultado a mesmo determinante com as colunas i e j trocadas e, portanto, seu determinante será multiplicado por (-1) e assim teremos que $\tau\Delta = -\Delta$. Assim, sempre que aplicarmos um número par de transposições, Δ não será alterado; caso contrário, se τ for ímpar, então $\tau\Delta = -\Delta$.

Portanto, pela correspondência de Galois, temos:

$$\begin{array}{ccc} \mathbb{Q}(x_1, x_2, \ldots, x_n) & \text{——} & \{e\} \\ \Big| & & \Big| \\ \mathbb{Q}(s)(\Delta) & \text{————} & A_n \\ {\scriptstyle 2}\Big| & & {\scriptstyle 2}\Big| \\ \mathbb{Q}(s_1, s_2, \ldots, s_n) & \text{——} & \mathfrak{S}_n \end{array}$$

Podemos concluir que, como $[\mathfrak{S}_n : A_n] = 2$, então $[\mathbb{Q}(s)(\Delta) : \mathbb{Q}(s)] = 2$ e, assim, o $irr(\Delta, \mathbb{Q}(s))$ tem grau 2, a saber: $(x^2 - \Delta^2) = (x - \Delta)(x + \Delta)$, Pois $\Delta^2 \in \mathbb{Q}(s_1, \ldots, s_n)$.

Agora vamos fazer o mesmo com o corpo de decomposição de $p(x) \in \mathbb{Q}[x]$ polinômio com n raízes complexas distintas $\alpha_1, \alpha_2, \ldots, \alpha_n$. Seja $Gal(p) = Gal(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q})$.

Novamente consideremos $\Delta_p = \Delta(\alpha_1, \ldots, \alpha_n) = \prod_{i<j}(\alpha_j - \alpha_i)$ e agora queremos saber quem é o subgrupo de $Gal(p)$ que fixa Δ_p.

Como A_n fixava Δ, o candidato natural para fixar Δ_p é $Gal(p) \cap A_n$.

Como as raízes são todas distintas, temos que $\Delta_p \neq 0$ e, portanto, se $\sigma \in Gal(p)$ e se $\sigma(\Delta_p) = \Delta_p$ então $\sigma \in A_n$ pois senão, se $\sigma \notin A_n \Rightarrow \sigma(\Delta_p) = (\sigma\Delta)(\alpha_1, \ldots, \alpha_n) = -\Delta(\alpha_1, \ldots, \alpha_n) = -\Delta_p = \Delta_p$ que é um absurdo pois $\Delta_p \neq 0$.

É claro que se $\sigma \in Gal(p)$ for par, $\sigma(\Delta_p) = \Delta_p$.

Portanto temos a correspondência:

$$\begin{array}{ccc} \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) & \text{————} & \{e\} \\ \Big| & & \Big| \\ \mathbb{Q}(\Delta_p) & \text{————} & Gal(p) \cap A_n \\ {\scriptstyle \leq 2}\Big| & & {\scriptstyle \leq 2}\Big| \\ \mathbb{Q} & \text{————} & Gal(p) \end{array}$$

Chamaremos, $R_{\mathfrak{S}_n}(\Delta, p) = (x - \sigma_1\Delta(\alpha_1, \ldots, \alpha_n))(x - \sigma_2\Delta(\alpha_1, \ldots, \alpha_n))$ onde σ_i são representantes das coclasses de A_n em $\mathfrak{S}_n$, o polinômio resolvente com respeito a Δ, $\mathfrak{S}_n$ e p. Nesse caso, podemos tomar $\sigma_1 = e$ e σ_2 qualquer permutação impar.

Temos assim $R_{\mathfrak{S}_n}(\Delta, p) = (x - \Delta_p)(x + \Delta_p) = x^2 - \Delta_p^2$ que tem coeficientes racionais. Podemos notar que se Δ_p estiver em $\mathbb{Q}$, então Δ_p será fixo por todo $Gal(p)$ e, portanto, $Gal(p) \subset A_n$. Podemos então enunciar o seguinte teorema:

Proposição 4.1.1. *Seja A_n o grupo alternado correspondente às permutações pares e $p(x) \in \mathbb{Q}[x]$ um polinômio com n raízes distintas. Então $Gal(p) \subset A_n$ se e somente se o discriminate de $p(x)$, denominado Δ_p for um quadrado em $\mathbb{Q}$.*

Demonstração. A prova é imediata das observações acima. □

O discriminante vai nos servir para verificar se o grupo de Galois tem apenas permutações pares ou não. Agora vamos ver mais um caso, onde o polinômio proposto possui 4 raízes distintas.

Seja $f(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4$ com raízes x_1, x_2, x_3, x_4 algebricamente independentes.

Novamente consideremos a extensão $\mathbb{Q}(x_1, \ldots, x_4)/\mathbb{Q}(s_1, \ldots, s_4)$ e seja $V \leq S_4$ o grupo de Klein dado por $V_4 = \{(12)(34), (1), (13)(24), (14)(23)\}$. Vamos estudar o subcorpo fixo de $\mathbb{Q}(x_1, \ldots, x_4)$ por V_4. É natural portanto considerar o elemento $T = T_1 = x_1x_2 + x_3x_4$.

Pode-se mostrar facilmente que a órbita de T é $o(T_1) = \{T_1, T_2 = x_1x_3 + x_2x_4, T_3 = x_1x_4 + x_2x_3\}$. E também pode-se ver que V_4 é o grupo que fixa o conjunto $\{T_1, T_2, T_3\}$ e assim $\mathbb{Q}(x_1, \ldots, x_4)^V = \mathbb{Q}(T_1, T_2, T_3)$ e novamente pela correspondência de Galois:

$$\begin{array}{ccc}
\mathbb{Q}(x_1, x_2, x_3, x_4) & \text{——} & \{e\} \\
\Big| & & \Big| \\
\mathbb{Q}(s)(T_1, T_2, T_3) & \text{——} & V_4 \\
{\scriptstyle 3}\Big| & & {\scriptstyle 3}\Big| \\
\mathbb{Q}(s_1, s_2, s_3, s_4) & \text{——} & \mathfrak{S}_4
\end{array}$$

Seja então $p(x) \in \mathbb{Q}[x]$ um polinômio com 4 raízes distintas $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ e seja $Gal(p) = Gal(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)/\mathbb{Q})$. Se $t_1 = T_1(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $t_2 = T_2(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ e $t_3 = T_3(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, então o candidato natural para fixar $\mathbb{Q}(t_1, t_2, t_3)$ é $Gal(p) \cap V$.

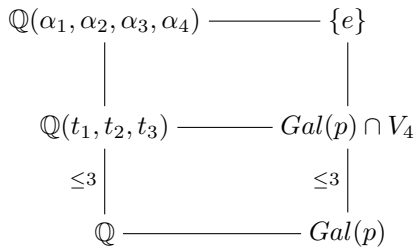
Afirmo que se as raízes de p são distintas, então $t_1 \neq t_2 \neq t_3$, pois se, por exemplo, $t_1 = t_2 \Rightarrow \alpha_1\alpha_2 + \alpha_3\alpha_4 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \Rightarrow (\alpha_2 - \alpha_3)(\alpha_1 - \alpha_4) = 0$ que é um absurdo.

Da mesma forma que fizemos para Δ_p, seja $\sigma \in Gal(p)$ e suponha que σ fixe t_j para $j = 1, 2, 3$. Assim temos que $\sigma t_j = t_j, j = 1, 2, 3$ e, portanto, $\sigma \in V$, pois senão teríamos $\sigma t_j = t_i$ para algum j com $i \neq j$, e $\sigma t_j = (\sigma T_j)(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = T_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = t_i = t_j$, que é um absurdo.

Por outro lado é claro que se $\sigma \in Gal(p) \cap V$, então σ fixará os T_j e, portanto, vai fixar os t_j.

Portanto $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)^{Gal(p)\cap V} = \mathbb{Q}(t_1, t_2, t_3)$.

Temos pela correspondência de Galois:



Utilizando o mesmo raciocinio de 4.1.1, sabemos que se $\{t_1, t_2, t_3\} \in \mathbb{Q}$, então $Gal(p) \subset V_4$.

Podemos perceber que quando tomamos um subgrupo H de $\mathfrak{S}_n$ e encontramos o subcorpo de $\mathbb{Q}(x_1, \ldots, x_n)$ fixo por H podemos ter informações sobre o grupo de Galois de um polinômio qualquer com n raízes distintas. Vamos agora definir o nosso principal objeto, e provar um resultado importante.

Definição 4.1.2. Seja $p(x) \in \mathbb{Z}[x]$ um polinômio com n raízes distintas α_1, α_2 ,...,α_n e $G \leq \mathfrak{S}_n$ um grupo que contém o grupo de Galois de $p(x)$,($Gal(p) \subset G$). Seja também T um polinômio nas variáveis $x_1, x_2, \ldots, x_n$ com coeficientes inteiros. Se H é o estabilizador de T em G, i.e:

$$H = \{\sigma \in G \mid T(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = T(x_1, x_2, \ldots, x_n)\}$$

definimos o polinômio resolvente $R_G(T, p)$ com respeito a G, T e o polinômio original p como sendo:

$$R_G(T,p)(x) = \prod_{\sigma_i \in G/H} (x - T(\alpha_{\sigma_i(1)}, \alpha_{\sigma_i(2)}, \ldots, \alpha_{\sigma_i(n)})),$$

onde os σ_i são representantes das coclasses de H em G.

Lema 4.1.3. *Seja H um subgrupo do $\mathfrak{S}_n$ e $\mathbb{Q}(x_1, \ldots, x_n)^H$ o subcorpo de $\mathbb{Q}(x_1, \ldots, x_n)$ fixo por H. Então, existe sempre T polinômio em $x_1, \ldots, x_n$ um elemento primitivo da extensão $\mathbb{Q}(x_1, \ldots, x_n)^H/\mathbb{Q}(s_1, \ldots, s_n)$.*

Demonstração. Seja T um elemento de $\mathbb{Q}(x_1, \ldots, x_n)^H/\mathbb{Q}(s_1, \ldots, s_n)$ definido por:

$$T = \sum_{\sigma_i \in \mathfrak{S}_n/H} \sigma_i(x_1 x_2^2 \ldots x_n^n)$$

onde os σ_i são representantes das coclasses de H em $\mathfrak{S}_n$.

Se $\tau \in H$, então temos que $\tau(T) = T$, pois:

$$\tau(T) = \tau\sigma_1(x_1 x_2^2 \ldots x_n^n) + \cdots + \tau\sigma_k(x_1 x_2^2 \ldots x_n^n)$$

onde k é o índice de H em $\mathfrak{S}_n$.

E como os conjuntos $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ e $\{\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_k\}$ são o mesmo, então H fixa T.

Por outro lado, se alguma $\tau \in \mathfrak{S}_n$ fixar T, então $\tau(T) = T$ e como os monômios de T são todos distintos, τ vai apenas permutá-los. Assim:

$$\tau(x_1 x_2^2 \ldots x_n^n) = \sigma_i(x_1 x_2^2 \ldots x_n^n)$$

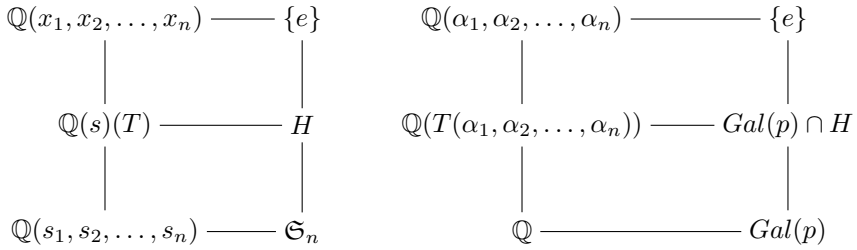
para algum $i \in 1, 2, ..., k$. E, portanto, $\tau^{-1}\sigma_i$ fixa $(x_1 x_2^2 \ldots x_n^n)$, o que implica $\tau^{-1}\sigma_i = e$ e $\tau \in H$.

Portanto, H é o estabilizador de T em $\mathfrak{S}_n$.

□

Teorema 4.1.4. *Seja H um subgrupo do $\mathfrak{S}_n$ e $\mathbb{Q}(x_1, \ldots, x_n)^H$ o subcorpo de $\mathbb{Q}(x_1, \ldots, x_n)$ fixo por H. Seja $T = T_1$ um polinômio em $x_1, \ldots, x_n$ o elemento primitivo da extensão $\mathbb{Q}(x_1, \ldots, x_n)^H/\mathbb{Q}(s_1, \ldots, s_n)$. Se $p(x)$ é um polinômio em $\mathbb{Q}[x]$ com raízes distintas $\alpha_1, \ldots, \alpha_n$ e se o polinômio resolvente $R_{\mathfrak{S}_n}(T, p)(x)$ for separável, então $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)^{Gal(p)\cap H} = \mathbb{Q}(T(\alpha_1, \ldots, \alpha_n))$.*

Queremos provar que, quando $R_{\mathfrak{S}_n}(T, p)$ for separável teremos a seguinte relação entre as correspondências de Galois do corpo de decomposição das indeterminadas $x_1, \ldots, x_n$ e do corpo das raízes de $p(x)$ $\alpha_1, \ldots, \alpha_n$.



Demonstração. Primeiramente vamos denotar a órbita de T por $\mathfrak{S}_n$ por $\{T_1 = T, T_2, \ldots, T_k\}$ onde k é o índice de H em $\mathfrak{S}_n$. Sendo assim, $t_i = T_i(\alpha_1, \ldots, \alpha_n)$. Portanto:

$$R_{\mathfrak{S}_n}(T, p) = \prod_{i=1}^{k}(x - t_i)$$

então é claro que se $\sigma \in Gal(p) \cap H$, então σ fixa T, pois está em H e, portanto, fixa $t = T(\alpha_1, \ldots, \alpha_n)$.

Por outro lado, se $\sigma \in Gal(p)$ fixar t então $(\sigma T)(\alpha_1, \ldots, \alpha_n) = T(\alpha_1, \ldots, \alpha_n)$ e σ deve estar em H pois senão $\sigma(t) = (\sigma T)(\alpha_1, \ldots, \alpha_n) = T_j(\alpha_1, \ldots, \alpha_n) = t_j = t$, que é um absurdo pois $R_{\mathfrak{S}_n}(T, p)$ é separável. Portanto $\sigma \in H$ e $\sigma \in Gal(p) \cap H$ como queríamos demonstrar. □

No primeiro caso o Δ era elemento primitivo de $\mathbb{Q}(x_1, \ldots, x_n)^{A_n}$ e quando $R_{\mathfrak{S}_n}(\Delta, p)$ tinha alguma raiz racional o $Gal(p)$ estava contido no A_n. Vamos ver o que acontece em geral.

Teorema 4.1.5. *Nas condições do teorema anterior, se $Gal(p) \subset \sigma H \sigma^{-1}$ para algum σ, então $R_{\mathfrak{S}_n}(T,p)$ possui uma raiz racional. Por outro lado se $R_{\mathfrak{S}_n}(T,p)$ for separável e possuir uma raiz racional, então $Gal(p) \subset \sigma H \sigma^{-1}$ para algum σ.*

Demonstração. Podemos tomar σ um representante das coclasses de H em $\mathfrak{S}_n$, e em particular, podemos tomar os mesmos representantes que usamos em $R_{\mathfrak{S}_n}(T,p)$, pois se $\sigma H = \tau H$ então $\sigma H \sigma^{-1} = \tau H \tau^{-1}$ e, portanto, o número de conjugados de H é menor ou igual ao número de coclasses de H em $\mathfrak{S}_n$.

($\Rightarrow$) Se $Gal(p) \subset \sigma H \sigma^{-1}$, então se $\tau \in Gal(p)$, temos:

$$\begin{aligned} \tau(\sigma T)(\alpha_1, \ldots, \alpha_n) = &\quad \sigma h \sigma^{-1}(\sigma T)(\alpha_1, \ldots, \alpha_n) = \\ \sigma h(T)(\alpha_1, \ldots, \alpha_n) = &\quad (\sigma T)(\alpha_1, \ldots, \alpha_n) \end{aligned}$$

e portanto, τ fixa $(\sigma T)(\alpha_1, \ldots, \alpha_n) = t_i$ para algum i e assim $t_i \in \mathbb{Q}$.

($\Leftarrow$) Se $R_{\mathfrak{S}_n}(T,p)$ possui uma raiz racional então $(\sigma T)(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$ para algum σ e se $\tau \in Gal(p)$ então τ fixa $(\sigma T)(\alpha_1, \ldots, \alpha_n)$. Assim

$$\tau(\sigma T)(\alpha_1, \ldots, \alpha_n) = \quad (\sigma T)(\alpha_1, \ldots, \alpha_n)$$

e como $R_{\mathfrak{S}_n}(T,p)$ é separável

$$\begin{aligned} \tau(\sigma T) = (\sigma T) &\quad \Rightarrow \\ \sigma^{-1}\tau\sigma(T) = T &\quad \Rightarrow \end{aligned}$$

$\sigma^{-1}\tau\sigma$ fixa $T \Rightarrow \sigma^{-1}\tau\sigma \in H \Rightarrow \tau = \sigma h \sigma^{-1} \Rightarrow \tau \in \sigma H \sigma^{-1}$

Portanto $Gal(p) \subset \sigma H \sigma^{-1}$. □

- Observação:

  Se $Gal(p) \subset \sigma H \sigma^{-1}$, para algum $\sigma \in H/\sigma_n$, então podemos reordenar as raízes por σ. Assim, o novo vetor das raízes ficará assim:

  $$(\alpha_1, \alpha_2, \ldots, \alpha_n) \rightsquigarrow^{\sigma} (\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$$

  Portanto, teremos o novo polinômio resolvente:

  $$\begin{aligned} R_{\mathfrak{S}_n}(T,p) &= (x - T(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})) \ldots (x - (\sigma_k T)(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})) \\ &= (x - (\sigma T)(\alpha_1, \alpha_2, \ldots, \alpha_n)) \ldots (x - (\sigma_k T)(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})) \end{aligned}$$

  E como $(\sigma T)(\alpha_1, \alpha_2, \ldots, \alpha_n))$ era a raiz de $R_{\mathfrak{S}_n}(T,p)$ antes da reordenação, agora teremos $(T)(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})$ como raiz e, portanto, agora $Gal(p) \subset H$. Assim, a menos da ordem das raízes $\alpha_1, \ldots, \alpha_n$, $Gal(p) \subset H$.

Nos algoritmos da próxima seção veremos que se tivermos o conhecimento de que o grupo de Galois está contido em algum grupo $G \leq \mathfrak{S}_n$, então poderemos tomar um polinômio resolvente de grau menor do que o que seria tomado utilizando o teorema anterior. Para isso segue a seguinte proposição:

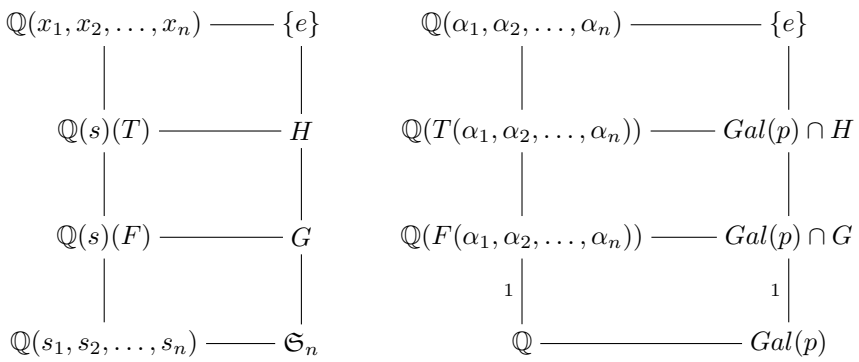
Proposição 4.1.6. *Se $Gal(p) \leq G \leq \mathfrak{S}_n$, então $R_G(T,p)$ é um polinômio com coeficientes em $\mathbb{Q}$ e além disso é um fator de $R_{\mathfrak{S}_n}(T,p)$.*

Demonstração. Por definição $R_G(T,p)$ é um fator de $R_{\mathfrak{S}_n}(T,p)$ pois temos:

$$\begin{aligned} R_G(T,p) &= \prod_{\tau \in G/H} (x - T(\alpha_{\tau(1)}, \alpha_{\tau(2)}, \ldots, \alpha_{\tau(n)})) \\ R_{\mathfrak{S}_n}(T,p) &= \prod_{\sigma \in \mathfrak{S}_n/H} (x - T(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)})) \end{aligned}$$

E portanto basta mostrar que se $\tau \in G/H$, então posso escolher τ como sendo representante de $\mathfrak{S}_n/H$. Para isso basta ver que se $\tau \in G$ e $\tau H = \tau' H$ em $\mathfrak{S}_n/H$ então $\tau H = \tau' H$ em G/H. Em particular o grau de $R_G(T,p)$ divide o grau de $R_{\mathfrak{S}_n}(T,p)$.

Para ver que os coeficientes de $R_G(T,p)$ estão em $\mathbb{Q}$ basta observar a seguinte correspondência:



E como $Gal(p) \leq G$, então $[\mathbb{Q}(F(\alpha_1, \alpha_2, \ldots, \alpha_n)) : \mathbb{Q}] = 1$ e portanto $R_G(T,p)$ tem coeficientes em $\mathbb{Q}(F(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{Q}$. □

4.2 Esquema geral dos algoritmos

Agora que temos toda a teoria, podemos dar a idéia por trás dos algoritmos da seção 4.6.

Primeiramente, é necessário dizer que como o polinômio dado é irredutível, então pode-se mostrar que seu grupo de Galois é um subgrupo transitivo de $\mathfrak{S}_n$, onde n é o grau do polinômio. Esses subgrupos já foram tabelados em [4] e estão representados no apêndice A. Portanto, temos um número finito e relativamente pequeno de candidatos a grupo de Galois para cada grau de polinômio dado.

O principal objeto deste trabalho é o polinômio resolvente. Pode-se mostrar que esse polinômio tem coeficientes inteiros e sua fatoração em $\mathbb{Z}[x]$ vai ajudar a determinar o grupo de Galois do polinômio original.

Para determinar o polinômio resolvente precisamos das raízes do polinômio dado, de um polinômio $T(x_1, x_2, \ldots, x_n)$ e de seu estabilizador H como definido em 4.1.2. A idéia é fazer o grupo H ser um dos candidatos a grupo de Galois e tendo um elemento T estabilizado por ele, determinar o polinômio resolvente. A partir daí, fatora-se o resolvente e concluímos qual o grupo de Galois do polinômio original.

Temos então o esquema abaixo:

Algoritmo 1: Esquema geral dos algoritmos

1 **se** $p(x) \in \mathbb{Q}[x]$ **então**
2 Aplicar a transformação de Tschirnhausen, e trocar o polinômio $p(x)$ original por outro mônico em $\mathbb{Z}[x]$
3 Determinar as raízes de $p(x)$
4 Determinar o polinômio resolvente $R_{\mathfrak{S}_n}(T, p)(x)$
5 **se** *Resolvente não for separável* **então**
6 Aplicar a transformação de Tschirnhausen, mudar o polinômio $p(x)$
7 Volte para o passo 3
8 Verifica como $R_{\mathfrak{S}_n}(T, p)(x)$ se fatora em $\mathbb{Z}[x]$ e conclui

Como teorema 4.1.4 exige que o resolvente seja separável, temos que aplicar uma transformação de Tschirnhausen, descrita em 5, caso ele não seja. Essa transformação simplesmente muda o polinômio original, sem alterar o corpo definido pelas suas raízes.

Além disso, os algoritmos devem receber um polinômio mônico com coeficientes inteiros e, portanto, uma transformação de Tschirnhausen deve ser aplicada para todo polinômio de entrada que tiver seus coeficientes em $\mathbb{Q}[x]$.

Utilizamos os teoremas 4.1.5 e 4.1.6, para concluir ou tomar outro resolvente se for necessário.

Nos algoritmos da seção 4.6, vamos supor que o polinômio de entrada seja mônico com coeficientes inteiros já que em todos os algoritmos o polinômio de entrada deverá ser transformado para ter essa característica. Nas próximas seções vamos demonstrar a validade dos algoritmos para polinômios de grau 3,4 e 5. Para polinômios de grau 6 e 7, as demonstrações são análogas.

4.3 Algoritmo para polinômios do 3º grau

Para polinômios do terceiro grau, basta saber que os subgrupos transitivos do $\mathfrak{S}_3$ são o $\mathfrak{S}_3$ e o grupo alternado A_3. Assim, pelo teorema 4.1.1 provamos o algoritmo seguinte:

Algoritmo 2: Grupo de Galois de um polinômio de grau 3

Saída: Representação usual do grupo de Galois de um polinômio $p(x)$ irredutível de grau 3.

1 $disc \leftarrow$ Discriminante(p)
2 **se** *disc é quadrado perfeito em* $\mathbb{Q}$ **então**
3 **devolve** A_3
4 **senão**
5 **devolve** $\mathfrak{S}_3$

4.4 Prova do Algoritmo 3

Agora, vamos demonstrar a validade do algoritmo para o cálculo do grupo de Galois de um polinômio mônico irredutível $p(x) \in \mathbb{Z}[x]$ do 4º grau descrito na seção 4.6.

Os subgrupos transitivos a menos de conjugação de $\mathfrak{S}_4$ dados no Apêndice A são:

1. $\mathfrak{S}_4$
2. A_4. O subgrupo das permutações pares.
3. V_4. O subgrupo de Klein dado por $\{(1), (12)(34), (13)(24), (14)(23)\}$.
4. D_4. O subgrupo das simetrias do quadrado gerado por $\{(1234), (24)\}$.
5. C_4. O subgrupo cíclico gerado por $\{(1234)\}$.

Algumas inclusões importantes são:

$$C_4 \subset D_4 \quad V_4 \subset A_4 \cap D_4$$

Agora podemos demonstrar a validade do algoritmo 4 dado.

Demonstração.

Lema 4.4.1. *O subgrupo H de $\mathfrak{S}_4$ que estabiliza $T = X_1X_3 + X_2X_4$ é o D_4.*

Demonstração. Para isso, basta testar as permutações de $D_4 = \{(1), (1234), (24), (13)(24), (12)(34), (14)(23), (1432), (13)\}$ e ver que elas fixam T. E, portanto, D_4 está contido no estabilizador de T.

$$D_4 \subset (\mathfrak{S}_4)_T$$

e assim:

$$|(\mathfrak{S}_4)_T| \geq |D_4| = 8$$

Por outro lado, se testarmos os representantes das coclasses de $D_4/\mathfrak{S}_4$, veremos que a órbita de T tem pelo menos 3 elementos.

$$D_4/\mathfrak{S}_4 = \{(1), (12), (14)\} \Rightarrow o(T) \subset \{X_1X_3+X_2X_4, X_2X_3+X_1X_4, X_1X_2+X_3X_4\}$$

$$|o(T)| = \frac{|\mathfrak{S}_4|}{|(\mathfrak{S}_4)_T|}$$

então,

$$|(\mathfrak{S}_4)_T| = \frac{|\mathfrak{S}_4|}{|o(T)|} \leq \frac{24}{3} = 8$$

Portanto, como $|D_4| = |(\mathfrak{S}_4)_T| = 8$ temos que:

$$D_4 = (\mathfrak{S}_4)_T$$

□

Vamos agora construir o polinômio resolvente e ver que informações ele nos traz. Pode-se mostrar que esse polinômio possui coeficientes inteiros e é claramente mônico. Além disso, se o resolvente possuir alguma raiz racional, então essa raiz será inteira já que será um divisor do termo independente.

$$R_{\mathfrak{S}_4}(T,p)(x) = (x-T(\alpha_1,\ldots,\alpha_4))(x-(12)T(\alpha_1,\ldots,\alpha_4))(x-(14)T(\alpha_1,\ldots,\alpha_4))$$

onde $\alpha_1, \ldots, \alpha_4$ são as raízes de p.

Se o polinômio não for separável, então aplicamos uma transformação de Tschirnhausen como descrito no capítulo 5. Portanto, podemos supor que o polinômio resolvente é separável.

Pelo teorema 4.1.5, onde $H = D_4$, $G = \mathfrak{S}_4$ e T dado acima, se $R_{\mathfrak{S}_4}(T,p)(x)$ possuir uma raiz inteira, então o grupo de Galois de p estará contido no D_4. Assim, podemos concluir:

1. Se o resolvente não possuir uma raiz inteira, então $Gal(p) = A_4$ ou $Gal(p) = \mathfrak{S}_4$. Pelo teorema 4.1.1, temos que $Gal(p) = A_4$ se o discriminante for um quadrado em $\mathbb{Q}$ e $Gal(p) = \mathfrak{S}_4$ caso contrário.

2. Se o resolvente possuir uma raiz inteira, então $Gal(p) \subset D_4$, o que significa que $Gal(p) = D_4$, $Gal(p) = C_4$ ou $Gal(p) = V_4$. Como apenas o V_4 está contido no grupo alternado, se o discriminante for um quadrado, então $Gal(p) = V_4$. Se o discriminante não for um quadrado em $\mathbb{Q}$, então $Gal(p) = D_4$ ou $Gal(p) = C_4$. Para decidir, tomamos outro resolvente, onde:

$$H = C_4 \quad G = D_4 \quad T = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$$

onde $G/H = \{(1), (13)\}$.

Utilizando o mesmo argumento acima, é fácil mostrar que H é o estabilizador de T. Portanto, se $R_{D_4}(T, p)(x)$, de grau 2, possuir uma raiz inteira, então $Gal(p) = C_4$ e $Gal(p) = D_4$ caso contrário.

□

4.5 Prova do Algoritmo 4

Vamos agora demonstrar a validade do algoritmo para o cálculo do grupo de Galois de um polinômio irredutível do 5º grau descrito na seção 4.6.

Nesse caso, os subgrupos transitivos a menos de conjugação de $\mathfrak{S}_5$ são:

1. $\mathfrak{S}_5$
2. A_5. O subgrupo das permutações pares.
3. F_{20}. O subgrupo de Frobenius gerado pelas permutações $\{(12345), (2354)\}$.
4. D_5. O subgrupo das simetrias do pentagrama gerado por $\{(12345), (25)(34)\}$.
5. C_5. O subgrupo cíclico gerado por $\{(12345)\}$.

Algumas inclusões importantes são:

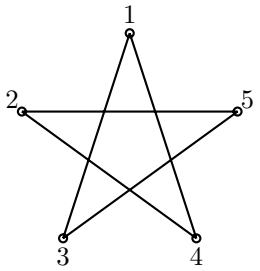
$$C_5 \subset D_5 \subset F_{20} \cap A_5$$

Agora finalmente podemos demonstrar a validade do algoritmo 4 dado:

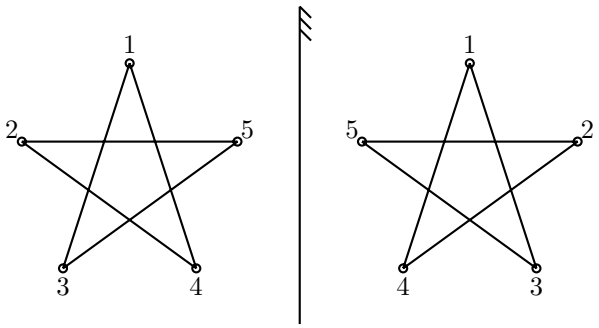
Demonstração.

Lema 4.5.1. *O subgrupo H de $\mathfrak{S}_5$ que estabiliza $T = X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1 - X_1X_3 - X_1X_4 - X_2X_4 - X_2X_5 - X_3X_5$ é o D_5.*

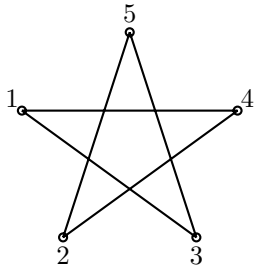
Demonstração. Observe inicialmente o seguinte pentagrama. As suas simetrias são operações que não alteram a sua estrutura, ou seja, os vértices numerados ligados por arestas continuam os mesmos. Queremos mostrar que as suas simetrias são as permutações de D_5.



Assim, se refletirmos utilizando um espelho teremos o seguinte:



E se girarmos teremos:



E, portanto, essas operações não alteram o pentagrama na sua estrutura. Agora observe que essas simetrias são, no caso da rotação, a permutação (12345) e, no caso da reflexão, a permutação (25)(34) que geram justamente o grupo D_5.

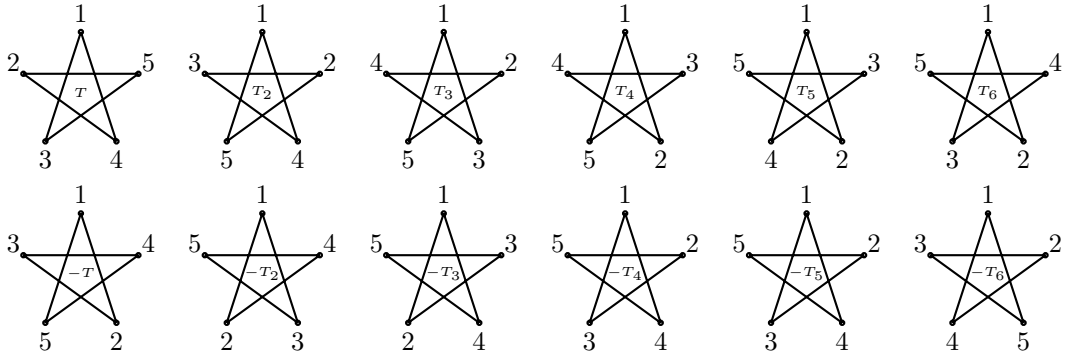
Agora note que os vértices ligados são $(1,3),(1,4),(2,4),(2,5),(3,5)$ que formam os fatores negativos de T. E os vértices que não estão ligados formam os fatores positivos de T. Portanto é claro que D_5 fixa T. Se $(\mathfrak{S}_5)_T$ é o estabilizador de T em $\mathfrak{S}_5$. Então:

$$D_5 \subset (\mathfrak{S}_5)_T$$

e assim:

$$|(\mathfrak{S}_5)_T| \geq |D_5| = 10$$

Falta mostrar que nenhuma outra permutação fixa T e para isso vamos descobrir um limitante inferior para o número de elementos na órbita de T. Podemos então tentar desenhar outros pentagramas:



Então, é fácil ver que todos esses pentagramas são distintos e, portanto, a órbita de T tem pelo menos 12 elementos e como:

$$|o(T)| = \frac{|\mathfrak{S}_5|}{|(\mathfrak{S}_5)_T|}$$

então,

$$|(\mathfrak{S}_5)_T| = \frac{|\mathfrak{S}_5|}{|o(T)|} \leq \frac{120}{12} = 10$$

Portanto como $|D_5| = |(\mathfrak{S}_5)_T| = 10$ e então:

$$D_5 = (\mathfrak{S}_5)_T$$

□

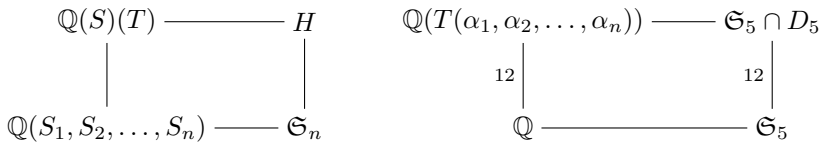
Portando estamos nas condições do teorema 4.1.5 onde $H = D_5$, $G = \mathfrak{S}_5$,T foi dado acima e $R_{\mathfrak{S}_n}(T, p)$ é livre de quadrados e assim separável. Como já foi dito, $R_{\mathfrak{S}_n}(T, p)$ possui coeficientes inteiros. Por conseguinte temos duas possibilidades para o polinômio $R_{\mathfrak{S}_n}(T, p)$.

1. $R_{\mathfrak{S}_n}(T, p)$ não possui raízes inteiras e nesse caso vamos mostrar que há três fatorações possíveis para o polinômio resolvente.

2. $R_{\mathfrak{S}_n}(T, p)$ possui uma raiz inteira e nesse caso o grupo de Galois de $p(x)$ está contido em algum conjugado de D_5. Nesse caso podemos trocar as raízes de maneira que $Gal(p) \subset D_5$.

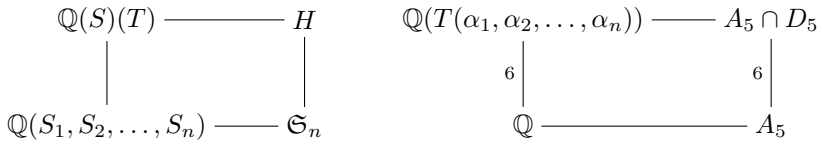
1. Nesse caso temos três possibilidades para o grupo de Galois.

- $Gal(p) = \mathfrak{S}_5$ Como já vimos, o estabilizador de T é o D_5 e portanto o estabilizador de $T(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é $D_5 \cap Gal(p)$. Pelo teorema 4.1.4 temos o seguinte:



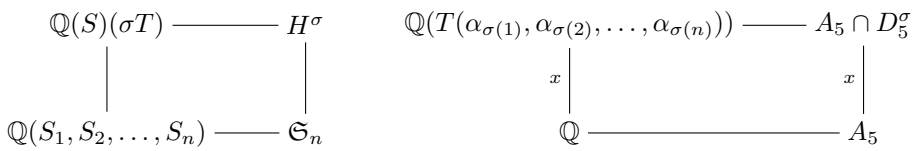
  E assim, como $[\mathbb{Q}(T(\alpha_1, \alpha_2, \ldots, \alpha_n)) : \mathbb{Q}] = 12$, $T(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é raíz de um polinômio irredutível de grau 12 e esse polinômio é justamente $R_{\mathfrak{S}_n}(T, p)$.

- $Gal(p) = A_5$ Nesse caso temos novamente o seguinte diagrama:



  E assim, como $[\mathbb{Q}(T(\alpha_1, \alpha_2, \ldots, \alpha_n)) : \mathbb{Q}] = 6$, $T(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é raíz de um polinômio irredutível de grau 6 que é um fator de $R_{\mathfrak{S}_n}(T, p)$. Para descobrir o grau dos outros fatores precisaremos preceder da seguinte forma:

  Para cada $\sigma \in \mathfrak{S}_5/D_5$ temos que calcular o grau de $Gal(p)/Gal(p) \cap D_5^\sigma$ pois agora o estabilizador de σT é $\sigma D_5 \sigma^{-1} = D_5^\sigma$. Temos para cada σ o seguinte diagrama:



  Agora obtemos cada σ como representante das coclasses de D_5 em $\mathfrak{S}_5$.

$\mathfrak{S}_5/D_5 = \{(1), (12), (13), (14), (15), (25), (123), (132), (125), (124), (134), (2354)\}$

  Temos a seguir a tabela com subgrupos conjugados de D_5.

σ	D_5^σ	$\lvert A_5 \cap D_5^\sigma \rvert$	$\lvert F_{20} \cap D_5^\sigma \rvert$
(1)	(1), (25)(34), (12)(35), (12345), (13)(45) (13524), (14)(23), (14253), (15432), (15)(24)	10	10
(12)	(1), (23)(45), (12)(35), (12543), (13452) (13)(24), (14235), (14)(25), (15)(34), (15324)	10	2
(13)	(1), (24)(35), (12)(34), (12354), (13)(45) (13425), (14532), (14)(25), (15)(23), (15243)	10	2
(14)	(1), (24)(35), (12)(45), (12534), (13245) (13)(25), (14352), (14)(23), (15)(34), (15423)	10	2
(15)	(1), (23)(45), (12)(34), (12453), (13542) (13)(25), (14)(35), (14325), (15234), (15)(24)	10	2
(25)	(1), (25)(34), (12)(45), (12435), (13)(24) (13254), (14)(35), (14523), (15342), (15)(23)	10	2
(123)	(1), (25)(34), (12)(45), (12435), (13)(24) (13254), (14)(35), (14523), (15342), (15)(23)	10	2
(132)	(1), (23)(45), (12)(34), (12453), (13542) (13)(25), (14)(35), (14325), (15234), (15)(24)	10	2
(125)	(1), (24)(35), (12)(45), (12534), (13245) (13)(25), (14352), (14)(23), (15)(34), (15423)	10	2
(124)	(1), (24)(35), (12)(34), (12354), (13)(45) (13425), (14532), (14)(25), (15)(23), (15243)	10	2
(134)	(1), (23)(45), (12)(35), (12543), (13452) (13)(24), (14235), (14)(25), (15)(34), (15324)	10	2
(2354)	(1), (25)(34), (12)(35), (12345), (13)(45) (13524), (14)(23), (14253), (15432), (15)(24)	10	10

Portanto se $Gal(p) = A_5$ então para todo σ teremos que o grau da extensão $\mathbb{Q}(T(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}))/\mathbb{Q}$ é $60/10 = 6$. Concluímos então que o resolvente se fatora nesse caso em dois polinômios de grau 6.

- $Gal(p) = F_{20}$

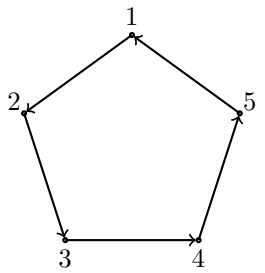
  Nesse caso como visto na tabela acima temos dois graus distintos para a fatoração do resolvente. O grau da extensão $\mathbb{Q}(T(\alpha_1, \alpha_2, \ldots, \alpha_n))/\mathbb{Q}$ é $20/10 = 2$ e a extensão $\mathbb{Q}(T(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}))/\mathbb{Q}$ é $20/2 = 10$ para $\sigma \neq (1), (2354)$. Portanto o resolvente se fatorará em dois polinômios de graus 10 e 2.

2. $R_{\mathfrak{S}_n}(T, p)$ possui uma raiz inteira e nesse caso existe uma ordenação das raízes onde o grupo de Galois de $p(x)$ está contido no grupo D_5. O primeiro passo é reordenar as raízes de tal modo que o grupo de Galois esteja contido no D_5. Agora falta descobrir se o grupo de Galois é de fato o D_5 ou seu subgrupo C_5.

   Assim, agora vamos considerar outro resolvente.

Lema 4.5.2. *O grupo H que estabiliza $T = X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_5^2 + X_5X_1^2$ é o C_5.*

Demonstração. Observe inicialmente o seguinte pentágono e vamos mostrar que as suas simetrias são as permutações de C_5.



Note então que as rotações do pentágono correspondem às permutações geradas por (12345). E essas rotações não alteram o pentágono de maneira que os vértices ligados pelas setas continuam os mesmos. Agora considere os representantes das coclasses de:

$$\begin{aligned}\mathfrak{S}_5/C_5 = \quad & \{(1),(45),(34),(345),(354),(35)\\ & (23),(23)(45),(234),(2345),(2354),(235)\\ & (243),(2453),(24),(245),(24)(35),(2435)\\ & (2543),(253),(254),(25),(2534),(25)(34)\}\end{aligned}$$

Podemos então verificar uma por uma que todas as permutações alteram a configuração do pentágono exceto a (1). É um trabalho simplesmente de testar essas 23 permutações. □

Portando novamente estamos nas condições dos teoremas 4.1.5 e 4.1.6 onde $H = C_5$, $G = D_5$ e T dado acima. Assim as coclasses de C_5 em D_5 tem dois representantes e $R_{D_5}(T,p)$ tem portanto grau 2.

Contudo o polinômio resolvente é livre de quadrados se e só se as raízes forem distintas. Essa condição corresponde no algoritmo ao $d \neq 0$.

Então, finalmente se $R_{D_5}(T,p)$ tiver raízes inteiras então o grupo de Galois será C_5, caso contrário será D_5. Essa condição corresponde no algoritmo ao d^2 ser um quadrado ou não em $\mathbb{Q}$.

□

4.6 Algoritmos

Algoritmo 3: Grupo de Galois de um polinômio de grau 4

Saída: Representação usual do grupo de Galois de um polinômio $p(x)$ irredutível de grau 4.

`[Cálculo do Resolvente]`

1 $\theta_i \leftarrow$ Raízes(p)
2 $T \leftarrow X_1X_3 + X_2X_4$
3 $R \leftarrow R_{\mathfrak{S}_4}(T, p)$
4 **se** !*ResolventeLivreQuadrados*(R) **então**
5 $p \leftarrow$ Tschirnhausen(p)
6 volte para o passo 1

`[Verifica se` R `possui raiz inteira e conclui]`

7 $disc \leftarrow$ Discriminante(p)
8 **se** !*PossuiRaizInteira*(R) **então**
9 **se** *disc é quadrado perfeito* **então**
10 **devolve** A_4
11 **senão**
12 **devolve** $\mathfrak{S}_4$
13 **senão**
14 **se** *disc é quadrado perfeito* **então**
15 **devolve** V_4

`[Reordenação das raízes]`

16 $\sigma \leftarrow$ PermutaçãoDaRaizInteira(R)
17 $\theta_i \leftarrow \theta_{\sigma(i)}$
18 $d \leftarrow ((\theta_1 - \theta_3)(\theta_2 - \theta_4)(\theta_1 + \theta_3 - \theta_2 - \theta_4))^2$
19 **enquanto** $d = 0$ **faça**
20 $p \leftarrow$ Tschirnhausen(p)
21 $\theta_i \leftarrow$ Raízes(p)
22 $R \leftarrow R_{\mathfrak{S}_4}(T, p)$
23 **se** !*ResolventeLivreQuadrados*(R) **então**
24 volte para o passo 20
25 $\sigma \leftarrow$ PermutaçãoDaRaizInteira(R)
26 $\theta_i \leftarrow \theta_{\sigma(i)}$
27 $d \leftarrow ((\theta_1 - \theta_3)(\theta_2 - \theta_4)(\theta_1 + \theta_3 - \theta_2 - \theta_4))^2$
28 **se** $d \neq 0$ **então**
29 **se** *d é quadrado perfeito* **então**
30 **devolve** C_4
31 **senão**
32 **devolve** D_4

Algoritmo 4: Grupo de Galois de um polinômio de grau 5

Saída: Representação usual do grupo de Galois de um polinômio $p(x)$ irredutível de grau 5.

`[Cálculo do Resolvente]`

1 $\theta_i \leftarrow$ Raízes(p)
2 $T \leftarrow X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1 - X_1X_3 - X_1X_4 - X_2X_4 - X_2X_5 - X_3X_5$
3 $R \leftarrow R_{\mathfrak{S}_5}(T, p)$
4 **se** !*ResolventeLivreQuadrados*(R) **então**
5 $p \leftarrow$ Tschirnhausen(p)
6 volte para o passo 1

`[Verifica se` R `possui raiz inteira, fatora o resolvente e conclui]`

7 **se** !*PossuiRaizInteira*(R) **então**
8 $l \leftarrow$ ListaDosGraus(R)
9 **caso** l
10 $(6, 6)$ **devolve** A_5
11 $(2, 10)$ **devolve** F_{20}
12 (12) **devolve** $\mathfrak{S}_5$
13 **senão**

`[Reordenação das raízes]`

14 $\sigma \leftarrow$ PermutaçãoDaRaizInteira(R)
15 $\theta_i \leftarrow \theta_{\sigma(i)}$
16 $d \leftarrow (\theta_1\theta_2(\theta_2 - \theta_1) + \theta_2\theta_3(\theta_3 - \theta_2) + \theta_3\theta_4(\theta_4 - \theta_3) + \theta_4\theta_5(\theta_5 - \theta_4) + \theta_5\theta_1(\theta_1 - \theta_5))^2$
17 **enquanto** $d = 0$ **faça**
18 $p \leftarrow$ Tschirnhausen(p)
19 $\theta_i \leftarrow$ Raízes(p)
20 $R \leftarrow R_{\mathfrak{S}_5}(T, p)$
21 **se** !*ResolventeLivreQuadrados*(R) **então**
22 $p \leftarrow$ Tschirnhausen(p)
23 volte para o passo 18
24 $\sigma \leftarrow$ PermutaçãoDaRaizInteira(R)
25 $\theta_i \leftarrow \theta_{\sigma(i)}$
26 $d \leftarrow (\theta_1\theta_2(\theta_2 - \theta_1) + \theta_2\theta_3(\theta_3 - \theta_2) + \theta_3\theta_4(\theta_4 - \theta_3) + \theta_4\theta_5(\theta_5 - \theta_4) + \theta_5\theta_1(\theta_1 - \theta_5))^2$
27 **se** d *é quadrado perfeito* **então**
28 **devolve** C_5
29 **senão**
30 **devolve** D_5

Algoritmo 5: Grupo de Galois de um polinômio de grau 6

Saída: Representação usual do grupo de Galois de um polinômio $p(x)$ irredutível de grau 6.

`[Cálculo do Resolvente]`

1 $\theta_i \leftarrow$ Raízes(p)

2 $T \leftarrow X_1^2X_5^2(X_2X_4 + X_3X_6)+X_2^2X_4^2(X_1X_5 + X_3X_6)+$
$X_3^2X_6^2(X_1X_5 + X_2X_4)+ X_1^2X_6^2(X_2X_5 + X_3X_4)+$
$X_2^2X_5^2(X_1X_6 + X_3X_4)+X_3^2X_4^2(X_1X_6 + X_2X_5)+$
$X_1^2X_3^2(X_2X_6 + X_4X_5)+X_2^2X_6^2(X_1X_3 + X_4X_5)+$
$X_4^2X_5^2(X_1X_3 + X_2X_6)+X_1^2X_4^2(X_2X_3 + X_5X_6)+$
$X_2^2X_3^2(X_1X_4 + X_5X_6)+X_5^2X_6^2(X_1X_4 + X_2X_3)+$
$X_1^2X_2^2(X_3X_5 + X_4X_6)+X_3^2X_5^2(X_1X_2 + X_4X_6)+$
$X_4^2X_6^2(X_1X_2 + X_3X_5)$

3 $R \leftarrow R_{\mathfrak{S}_6}(T, p)$

4 **se** !*ResolventeLivreQuadrados*(R) **então**

5 $p \leftarrow$ Tschirnhausen(p)

6 volte para o passo 1

`[Fatora o resolvente]`

7 $l \leftarrow$ ListaDosGraus(R)

8 **se** $l \neq (6)$ `[Caso redutível]`

9 **então**

10 **caso** l

11 $(1, 2, 3)$

12 $f_3 \leftarrow FatorResolvente(R, 3)$

13 $disc \leftarrow$ Discriminante(f_3)

14 **se** *disc é quadrado perfeito* **então**

15 **devolve** C_6

16 **senão**

17 **devolve** D_6

18 $(3, 3)$

19 $f_1 \leftarrow FatorResolvente(R, 1)$

20 $f_2 \leftarrow FatorResolvente(R, 2)$

21 $disc_1 \leftarrow$ Discriminante(f_1)

22 $disc_2 \leftarrow$ Discriminante(f_2)

23 **se** $disc_1$ *e* $disc_2$ *não são quadrados perfeitos* **então**

24 **devolve** $D_3 \times D_3$

25 **senão**

26 **devolve** $C_3 \times D_3$

27 $(2, 4)$

28 $f_2 \leftarrow FatorResolvente(R, 2)$

29 $disc \leftarrow$ Discriminante(p)

30 $disc_2 \leftarrow$ Discriminante(f_2)

31 **se** *disc é quadrado perfeito* **então**

32 **devolve** S_4^+

33 **senão**

34 **se** $disc_2$ *é quadrado perfeito* **então**

35 **devolve** $A_4 \times C_2$

36 **senão**

37 **devolve** $S_4 \times C_2$

---

44 **se** $l \neq (6)$ `[Caso redutível]`
45 **então**
46 **caso** l
47 $(1,1,4)$
48 $disc \leftarrow$ Discriminante(p)
49 **se** *disc é quadrado perfeito* **então**
50 **devolve** A_4
51 **senão**
52 **devolve** S_4^-
53 $(1,5)$
54 $disc \leftarrow$ Discriminante(p)
55 **se** *disc é quadrado perfeito* **então**
56 **devolve** A_5
57 **senão**
58 **devolve** S_5
59 $(1,1,1,3)$
60 **devolve** S_3
61 **senão**
  `[Cálculo de um novo resolvente]`
62 $F \leftarrow X_1X_2X_3 + X_4X_5X_6$
63 $R \leftarrow R_{\mathfrak{S}_6}(T,p)$
64 **se** !*ResolventeLivreQuadrados*(R) **então**
65 $p \leftarrow$ Tschirnhausen(p)
66 $\theta_i \leftarrow$ Raízes(p)
67 volte para o passo 63
  `[Verifica se` R `possui raiz inteira e conclui]`
68 $disc \leftarrow$ Discriminante(p)
69 **se** *PossuiRaizInteira*(R) **então**
70 **se** *disc é quadrado perfeito* **então**
71 **devolve** $C_3^2 \times C_4$
72 **senão**
73 **devolve** $C_3^2 \times D_4$
74 **senão**
75 **se** *disc é quadrado perfeito* **então**
76 **devolve** A_6
77 **senão**
78 **devolve** $\mathfrak{S}_6$

Algoritmo 6: Grupo de Galois de um polinômio de grau 7

Saída: Representação usual do grupo de Galois de um polinômio $p(x)$ irredutível de grau 7.

`[Cálculo do Resolvente]`

1 $\theta_i \leftarrow$ Raízes(p)

2
$$R \leftarrow \prod_{1 \leq i < j < k \leq 7} (x - (\theta_i + \theta_j + \theta_k))$$

3 **se** !*ResolventeLivreQuadrados*(R) **então**

4 $\quad p \leftarrow$ Tschirnhausen(p)

5 $\quad$ volte para o passo 1

`[Verifica se` R `possui raiz inteira, fatora o resolvente e conclui]`

6 $l \leftarrow$ ListaDosGraus(R)

7 **se** $l \neq (35)$ `[Caso redutível]`

8 **então**

9 $\quad$ **caso** l

10 $\quad\quad (7, 28)$ **devolve** $PSL_2(\mathbb{F}_7)$

11 $\quad\quad (14, 21)$ **devolve** F_{42}

12 $\quad\quad (7, 7, 21)$ **devolve** F_{21}

13 $\quad\quad (7, 7, 7, 14)$ **devolve** D_7

14 $\quad\quad (7, 7, 7, 7, 7)$ **devolve** C_7

15 **senão**

16 $\quad disc \leftarrow$ Discriminante(p)

17 $\quad$ **se** *disc é quadrado perfeito* **então**

18 $\quad\quad$ **devolve** A_7

19 $\quad$ **senão**

20 $\quad\quad$ **devolve** $\mathfrak{S}_7$

Algoritmo 7: Transformação de Tschirnhausen

Entrada: Recebe um polinômio $p(x) \in k[x]$ irredutível definindo um corpo $k(\theta)$.

Saída: Um polinômio $T(x)$ de mesmo grau definindo o mesmo corpo.

`[Polinômio Aleatório]`

1 $n \leftarrow grau(p)$

2 $A \leftarrow$ Polinômio aleatório em $\mathbb{Z}[x]$ de grau $\leq n - 1$

`[Resultante]`

3 $T \leftarrow Res(p(x), y - A(x), y)$

`[Verifica se` T `possui apenas raízes simples]`

4 **se** *LivreQuadrados*(T) **então**

5 $\quad$ **devolve** T

6 **senão**

7 $\quad$ volte para o passo 2

Capítulo 5

Transformações de Tschirnhausen

Como pôde ser visto no capítulo 4, em todos os algoritmos, trocamos o polinômio original $p(x)$ por outro polinômio de mesmo grau, e esperamos que o corpo definido pelas novas raízes continue o mesmo. Neste capítulo, o objetivo principal será exibir a transformação de Tschirnhausen e mostrar que sob certas condições, o corpo original não se altera.

5.1 Resultantes

Nesta seção, queremos decidir quando dois polinômios $f, g \in k[x]$, com k um corpo qualquer, possuem um fator comum em $k[x]$, isto é, se $\exists h \in k[x]$, $\partial h \geq 1 \mid h|f, h|g$ em $k[x]$. ∂h denota o grau do polinômio $h(x)$.

Lema 5.1.1. *Sejam $f, g \in k[x]$ polinômios tais que, $\partial f = l \geq 1$ e $\partial g = m \geq 1$. Então f e g possuem um fator comum em $k[x]$ se, e só se, $\exists A, B \in k[x]$ com as seguintes propriedades:*

1. *A e B não são nulos.*
2. *$\partial A \leq m - 1$, $\partial B \leq l - 1$*
3. *$Af + Bg = 0$*

Demonstração. ($\Rightarrow$) Se $h \in k[x]$ é fator comum, então $f = hf_1$ e $g = hg_1$, com $\partial f_1 \leq l - 1$ e $\partial g_1 = m - 1$. Temos, portanto:

$$\begin{aligned} \frac{f}{f_1} &= \frac{g}{g_1} \Rightarrow g_1 f = g f_1 \Rightarrow \\ g_1 f + (-f_1) g &= g_1(h f_1) - f_1(h g_1) = g_1 f + (-f_1) g = 0 \end{aligned}$$

Se tomarmos $A = g_1$ e $B = -f_1$ e assim, $(1), (2), (3)$ valem.

($\Leftarrow$) Suponhamos que $\exists A, B \in k[x]$ valendo (1), (2), (3), e, portanto, vale:

$$Af + Bg = 0 \Rightarrow Bg = -Af$$

e que f e g não tenham fator comum em $k[x]$. Então $mdc(f, g) = 1$ e, por Bézout, existem $\widetilde{A}, \widetilde{B} \in k[x]$, tais que:

$$\widetilde{A}f + \widetilde{B}g = 1$$

multiplicando os dois lados por B, temos:

$$\begin{aligned} \widetilde{A}Bf + \widetilde{B}gB &= B \\ \widetilde{A}Bf + \widetilde{B}(-Af) &= B \\ B &= (B\widetilde{A} - \widetilde{B}A)f \end{aligned}$$

como $B \neq 0$, $\partial B \geq \partial f = l$, o que contradiz (2). □

Precisamos agora, traduzir esse lema num critério prático que determine quando dois polinômios têm fator comum. Sejam então:

$$\begin{aligned} f(x) &= a_0x^l + a_1x^{l-1} + \cdots + a_l \qquad a_0 \neq 0 \\ g(x) &= b_0x^m + b_1x^{m-1} + \cdots + b_m \qquad b_0 \neq 0 \\ A(x) &= c_0x^{m-1} + c_1x^{m-2} + \cdots + c_{m-1} \qquad (5.1) \\ B(x) &= d_0x^{l-1} + d_1x^{l-2} + \cdots + d^{l-1} \qquad (5.2) \end{aligned}$$

De 5.1 e 5.2 temos $m + l$ incógnitas

$$c_0, c_1, \ldots, c_{m-1}, d_0, d_1, \ldots, d_{l-1}.$$

Devemos procurar $A(x), B(x) \in k[x]$, $\partial A \leq m - 1$, $\partial B \leq l - 1$ não ambos nulos, verificando:

$$Af + Bg = 0$$

Isso é equivalente a procurar $(c_0, c_1, \ldots, c_{m-1}, d_0, \ldots, d_{l-1}) \neq \overrightarrow{0}$ em k^{m+l} tal que:

$$(a_0x^l + \cdots + a_l)(c_0x^{m-1} + \cdots + c_{m-1}) + (b_0x^m + \cdots + b_m)(d_0x^{l-1} + \cdots + d_{l-1}) = 0$$

Analisando os coeficientes, temos:

$$\begin{aligned} &coef\ x^{l+m-1} && a_0c_0 + b_0d_0 = 0 \\ &coef\ x^{l+m-2} && (a_0c_1 + a_1c_0) + b_0d_1 + b_1d_0 = 0 \\ &coef\ x^{l+m-3} && (a_0c_2 + a_1c_1 + a_2c_0) + b_0d_2 + b_1d_1 + b_2d_0 = 0 \\ &\vdots \\ &coef\ x^0 && a_lc_{m-1} + b_md_{l-1} = 0 \end{aligned}$$

Resolver essas equações é equivalente a resolver o seguinte sistema:

$$\begin{array}{cccccccccc} 1 & 2 & 3 & \dots & m & 1 & 2 & 3 & \dots & l \end{array}$$

$$\left(\begin{array}{ccccc|ccccc} a_0 & & & & & b_0 & & & & \\ a_1 & a_0 & & & & b_1 & b_0 & & & \\ a_2 & a_1 & a_0 & & & b_2 & b_1 & b_0 & & \\ \vdots & & & \ddots & & \vdots & & & \ddots & \\ a_l & & & & a_0 & b_m & & & & b_0 \\ & \ddots & & & & & \ddots & & & \\ & & \ddots & & & & & \ddots & & \\ & & & \ddots & & & & & \ddots & \\ & & & & a_l & & & & & b_m \end{array}\right)\left(\begin{array}{c} c_0 \\ c_1 \\ \vdots \\ \vdots \\ \frac{c_{m-1}}{d_0} \\ \vdots \\ \vdots \\ d_{l-1} \end{array}\right) = \left(\begin{array}{c} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{array}\right)$$

Essa matriz $(m+l)\times(m+l)$ é chamada matriz de Sylvester e será denotada por $Sylv(f,g)$. Definiremos o resultante dos polinômios f e g com relação à variável x como o determinante da matriz.

$$Res(f,\ g,\ x) = det\ Sylv(f,\ g)$$

Lema 5.1.2. *Se $f,g \in k[x]$, são tais que $\partial f = l \geq 1$, $\partial g = m \geq 1$. Então $Res(f,g) \in \mathbb{Z}[a_0,a_1,\dots,a_l,b_0,b_1,\dots,b_m]$ e f,g possuem uma raiz comum em $k[x]$ se, e somente se, $Res(f,g)=0$.*

Demonstração. É claro que se f,g têm uma raiz em comum em $k[x]$, então f,g possuem fator comum. Assim, a prova é clara pela construção da matriz. □

Lema 5.1.3. *Se $f,g \in k[x]$, são tais que $\partial f = l \geq 1$, $\partial g = m \geq 1$. Seja $\overline{k}$ o fecho de k. Então f e g têm uma raiz comum em $\overline{k}$ se, e somente se, $Res(f,g)=0$.*

Demonstração. f e g possuem uma raiz comum α em $\overline{k}$ se, e só se, $irr(\alpha,k) \in k[x]$ divide f e g. Portanto, $irr(\alpha,k)$ é um fator comum a f e g e pelo lema 5.1.1 está provado.

□

5.2 Transformação de Tschirnhausen

Como visto na seção 4.6, a transformação de Tschirnhausen consiste em alterar o polinômio original $p(x)$ de grau n, por outro polinômio irredutível dado por:

$$T(y) = Res(p(x), y - A(x), y)$$

onde $A(x) \in \mathbb{Z}[x]$ é um polinômio de grau menor ou igual a $n-1$ escolhido aleatóriamente. Queremos mostrar que sob certa condição, os corpos de decomposição de $p(x)$ e $T(x)$ são iguais.

Primeiramente devemos observar que:

$$\begin{aligned} p(x) &= x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \\ y - A(x) &= -x^m - b_1x^{m-1} - \cdots - b_{m-1}x + y - b_n \end{aligned} \tag{5.3}$$

E portanto, o determinante da matriz de Sylvester é:

$$Res(p(x), y-A(x), y) = \left(\begin{array}{ccccc|ccccc} 1 & & & & & 1 & & & & \\ a_1 & 1 & & & & b_1 & 1 & & & \\ a_2 & a_1 & \ddots & & & b_2 & b_1 & \ddots & & \\ \vdots & a_2 & & 1 & & \vdots & b_2 & & 1 & \\ a_n & \vdots & & a_1 & & y-b_m & \vdots & & b_1 & \\ & a_n & & a_2 & & & y-b_m & & b_2 & \\ & & \ddots & \vdots & & & & \ddots & \vdots & \\ & & & a_n & & & & & y-b_m & \end{array}\right)$$

com zero nas posições livres.

Pode-se mostrar que o polinômio $T(y)$ resultante é dado por:

$$T(y) = y^n + c_1y^{n-1} + \cdots + c_{n-1}y + c_n$$

onde os coeficientes c_j são funções dos coeficientes a_j e b_j conhecidos e inteiros.

Observe agora, que pelo lema 5.1.3, as raízes y_i de T forçam o sistema abaixo a ter uma raiz comum:

$$\begin{cases} x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \\ y_i = A(x) \end{cases} \tag{5.4}$$

Assim, podemos enunciar o seguinte teorema.

Teorema 5.2.1. *Sejam $x_1, x_2, \ldots, x_n$ raízes de $p(x)$ e seja $T(y) = Res(p(x), y-A(x), y)$ o polinômio que anula $y_i = A(x_i)$, ou seja, x_i é uma raiz comum de 5.4. Se $T(y)$ for separável, então $x_i = r(y_i)$, onde $r(z)$ é um polinômio com coeficientes como sendo funções dos coeficientes de p e A.*

Demonstração. Tomemos uma raiz $y_i = A(x_i)$ de $T(y)$. Afirmo que as equações de 5.4 tem apenas uma raiz comum, pois se tivesse duas, digamos, x_i e x_j, teríamos $y_i = A(x_i) = A(x_j) = y_j$ e y_i teria multiplicidade maior que 1, o que é impossível pois $T(y)$ é separável.

Portanto, $d_i(x) = \text{MDC}(p(x), y_i - A(x))$ é um polinômio na variável x de grau 1. Assim, fazendo $d_i(x_i) = 0$, obtemos $x_i = r(y_i)$. □

Portanto, o corpo de decomposição original $\mathbb{Q}(x_1, x_2, \ldots, x_n)$ é igual ao corpo de decomposição transformado $\mathbb{Q}(y_1, y_2, \ldots, y_n)$, pois $x_i = r(y_i)$ e $y_i = A(x_i)$.

Capítulo 6

Software

Além de estudar os algoritmos do capítulo 4, este trabalho fornece um programa para o cálculo do grupo de Galois. Nesse capítulo, vamos analisar brevemente o software produzido. O programa consiste em um pacote de nome, *GrupoDeGalois*, escrito na linguagem do conhecido software Mathematica versão 6.0.

O programa deve receber um polinômio irredutível, com coeficientes racionais, de grau menor ou igual a 7, e devolve o grupo de Galois correspondente. Os testes realizados nesse capítulo devem avaliar a corretude e eficiência dos algoritmos. Além disso, vamos comparar o tempo de execução com outros programas tradicionais que se propõem a resolver o mesmo problema como por exemplo, o GAP e o PARI.

Os testes foram realizados em uma máquina com processador Pentium 4, 3.0GHz e memória RAM de 512MB.

6.1 Testes Básicos

Nessa seção, utilizaremos como entrada os polinômios de teste fornecidos em [5] para verificar a corretude e eficiência para os casos básicos. Apesar de os polinômios terem, em geral, coeficientes pequenos, forçam o programa a realizarem as transformações de Tschirnhausen descritas no capítulo 5. Portanto, esses polinômios testam de maneira completa os algoritmos propostos.

Para cada polinômio de [5], a tabela a seguir mostra, na ordem, o polinômio testado, o grupo de Galois de resposta, o tempo de execução do programa deste trabalho, e os tempos medidos pelos programas GAP e PARI. É importante salientar que ambos os programas utilizam o mesmo método proposto aqui. Os tempos foram medidos em *milisegundos* e qualquer tempo menor que $0,5ms$ será anotado como *zero* na tabela.

Polinômio	Galois	Programa	GAP	PARI
x	$\mathfrak{S}_1$	$0ms$	$0ms$	$0ms$
x^2+x+1	$\mathfrak{S}_2$	$0ms$	$0ms$	$0ms$
x^3+x^2-2x-1	C_3	$0ms$	$16ms$	$0ms$
x^3+2	$\mathfrak{S}_3$	$0ms$	$0ms$	$0ms$
$x^4+x^3+x^2+x+1$	C_4	$7ms$	$125ms$	$0ms$
x^4+1	V_4	$5ms$	$94ms$	$0ms$
x^4-2	D_4	$10ms$	$47ms$	$0ms$
$x^4+8x+12$	A_4	$7ms$	$16ms$	$0ms$
x^4+x+1	$\mathfrak{S}_4$	$6ms$	$15ms$	$0ms$
$x^5+x^4-4x^3-3x^2+3x+1$	C_5	$18ms$	$203ms$	$0ms$
$x^5+20x+16$	A_5	$15ms$	$16ms$	$0ms$
x^5+2	F_{20}	$35ms$	$3532ms$	$5ms$
$x^5-5x+12$	D_5	$15ms$	$93ms$	$0ms$
x^5-x+1	$\mathfrak{S}_5$	$15ms$	$16ms$	$5ms$
$x^6+x^5+x^4+x^3+x^2+x+1$	C_6	$36ms$	$125ms$	$0ms$
x^6+108	S_3	$35ms$	$203ms$	$5ms$
x^6+2	D_6	$33ms$	$157ms$	$16ms$
x^6-3x^2-1	A_4	$32ms$	$234ms$	$0ms$
x^6+3x^3+3	$C_3\times D_3$	$33ms$	$157ms$	$5ms$
x^6-3x^2+1	$A_4\times C_2$	$28ms$	$172ms$	$10ms$
x^6-4x^2-1	S_4^+	$30ms$	$172ms$	$5ms$
$x^6-3x^5+6x^4-7x^3+2x^2+x-4$	S_4^-	$30ms$	$17031ms$	$16ms$
x^6+2x^3-2	$D_3\times D_3$	$31ms$	$391ms$	$5ms$
$x^6+6x^4+2x^3+9x^2+6x-4$	$C_3^2\times C_4$	$23ms$	$156ms$	$10ms$
x^6+2x^2+2	$S_4\times C_2$	$34ms$	$187ms$	$5ms$
$x^6-2x^5-5x^2-2x-1$	A_5	$18ms$	$282ms$	$0ms$
$x^6+2x^4+2x^3+x^2+2x+2$	$C_3^2\times D_4$	$23ms$	$125ms$	$0ms$
$x^6-x^5-10x^4+30x^3-31x^2+7x+9$	S_5	$19ms$	$1547ms$	$0ms$
$x^6+24x-20$	A_6	$22ms$	$31ms$	$10ms$
x^6+x+1	$\mathfrak{S}_6$	$23ms$	$16ms$	$5ms$
$x^7+x^6-12x^5-7x^4+28x^3+14x^2-9x+1$	C_7	$25ms$	$344ms$	$5ms$
$x^7+7x^3+7x^2+7x-1$	D_7	$41ms$	$265ms$	$16ms$
$x^7-14x^5+56x^3-56x+22$	F_{21}	$25ms$	$657ms$	$0ms$
x^7+2	F_{42}	$37ms$	$547ms$	$5ms$
$x^7-7x^3+14x^2-7x+1$	$PSL_2(F_7)$	$40ms$	$656ms$	$10ms$
$x^7+7x^4+14x+3$	A_7	$32ms$	$15ms$	$11ms$
x^7+x+1	$\mathfrak{S}_7$	$36ms$	$16ms$	$10ms$

6.2 Testes de alcance

Os polinômios da seção anterior possuem, em geral, coeficientes pequenos e, portanto, não medem a utilização de alta precisão pelos programas. Além disso, podemos perceber que os tempos medidos foram relativamente baixos, o que indica que as contas feitas, de fato não requerem grandes recursos de processamento.

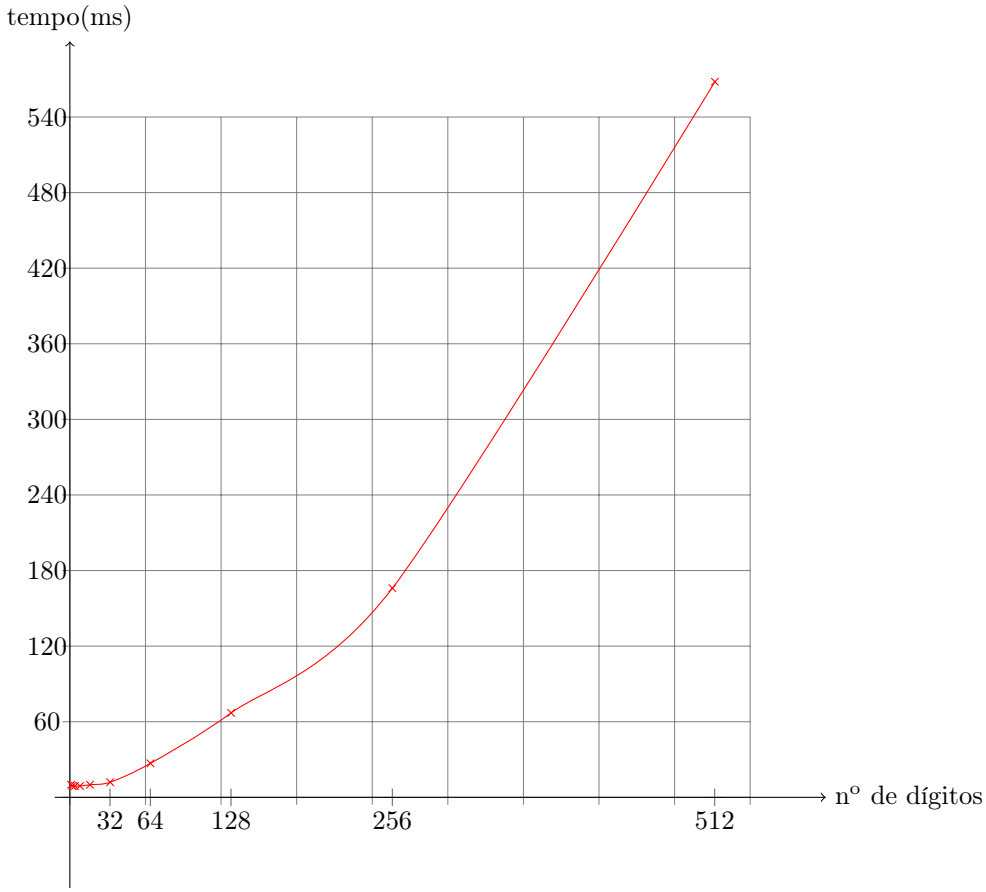
A medida do tamanho dos coeficientes será dada pelo seu termo independente, pois, quanto maior for, maior será o valor do produto das raízes. Essa medida é razoável, pois os resolventes utilizados em geral são somas de produtos das raízes do polinômio original(seção 4.6).

Pretendemos assim, medir como o tempo varia com o aumento dos coeficientes para determinar quanto a precisão utilizada influencia a eficiência do programa. Para isso, a tabela a seguir relaciona o número de dígitos do termo independente do polinômio original, a precisão utilizada pelo programa proposto e o tempo medido. Os polinômios testados em uma mesma tabela possuem o mesmo grupo de Galois associado e, então, as tabelas serão organizadas pelo grupo de seus polinômios.

1. Grupo de Galois: D_4 Polinômio: $x^4 - 2$

Nº dígitos	Precisão utilizada	tempo
1	10	$10ms$
2	20	$9ms$
4	40	$9ms$
8	40	$9ms$
16	80	$10ms$
32	150	$12ms$
64	300	$27ms$
128	600	$67ms$
256	1200	$166ms$
512	2400	$568ms$
1024	4700	$1309ms$
2048	10000	$7384ms$

Com os dados acima, podemos gerar o seguinte gráfico:



Podemos, através do gráfico e da tabela, inferir que a eficiência do programa varia com a precisão utilizada e não, diretamente, com o tamanho do polinômio de entrada. Isso se deve claramente ao algoritmo interno do software utilizado.

2. Grupo de Galois: F_{20} Polinômio: $x^5 + 2$

Nº dígitos	Precisão utilizada	tempo
1	30	$22ms$
2	60	$28ms$
4	100	$27ms$
8	170	$40ms$
16	370	$55ms$
32	660	$89ms$
64	1300	$300ms$
128	2500	$1193ms$
256	2600	$885ms$
512	10000	$24510ms$
1024	20000	$100602ms$

3. Grupo de Galois: S_3 Polinômio: $x^6 + 108$

Nº dígitos	Precisão utilizada	tempo
3	80	$30ms$
4	150	$36ms$
8	240	$47ms$
16	600	$102ms$
32	1000	$200ms$
64	2000	$598ms$
128	4000	$1818ms$
256	8000	$6562ms$
512	16000	$18859ms$
1024	32000	$70825ms$

4. Grupo de Galois: D_7 Polinômio: $x^7 + 7x^3 + 7x^2 + 7x - 1$

Nº dígitos	Precisão utilizada	tempo
1	30	$38ms$
2	30	$38ms$
4	40	$38ms$
8	60	$43ms$
16	100	$48ms$
32	170	$63ms$
64	330	$91ms$
128	640	$191ms$
256	1300	$758ms$
512	2600	$2179ms$
1024	5200	$7093ms$

Nos testes acima, não foi verificado um tamanho para o polinômio de entrada que gerasse uma resposta errada. Acreditamos que 1024 dígitos para o termo independente do polinômio original seja bastante satisfatório. Para a maioria dos casos, com esse tamanho, o tempo de resposta não é mais confortavelmente rápido.

Parte II

Parte Subjetiva

Capítulo 7

Sobre o TCC

7.1 Desafios

O projeto foi dividido em duas partes bem definidas:

1. Parte teórica:

   Essa foi certamente a parte mais difícil. Em 2005, fiz o curso de Álgebra II e foi nesse momento que comecei a me interessar por álgebra abstrata. No semestre seguinte, fiz Álgebra III e com muito esforço consegui ter uma pequena noção da Teoria de Galois. Ainda em 2006 fui monitor de Álgebra II e finalmente em 2007 comecei a estudar o tema do TCC.

   Portanto, foram 2 anos estudando o mesmo assunto e posso dizer que essa matéria é realmente difícil. Não é apenas uma questão de conhecimento e treino, mas principalmente de maturidade.

   Para essa parte do projeto, algumas matérias do curso foram fundamentais:

   - Programação Linear:

     Pois foi a primeira oportunidade em que experimentei a matemática como sendo ferramenta fundamental para a computação. Esse curso talvez seja o mais importante para a minha formação da maneira como eu concebi.
   - Álgebra II:

     Apesar dessa matéria sozinha não servir para muita coisa, ela despertou em mim a vontade de entender matemática mais profundamente. Nessa disciplina, alguns conceitos relativamente intuitivos são abstraídos e isso me fez pensar seriamente no porquê de tal forma de conduzir o pensamento.

- Álgebra III:

  Apesar de não ter entendido muito bem o que eu estava fazendo, percebia que havia muita coisa por trás que precisava ser compreendida. Nessa matéria posso dizer que entendi tudo, mas não compreendi nada. Mas serviu muito bem para que depois a teoria toda fizesse todo o sentido apesar de ter levado um ano para isso.

  Não acho que essa matéria deveria ser obrigatória para computação, mas acho que aquele que deseja e gosta de entender bem as coisas que faz deve cursar essa disciplina. Foi nessa matéria que eu aprendi como se deve escrever matemática e porque se deve escrever dessa forma.

2. Programa:

   Nessa parte, tive uma dificuldade principal que está relacionada com o fato de não conhecer a linguagem do Mathematica em que o programa deveria ser feito. Então, gastei um bom tempo entendendo como o software funcionava para depois começar a escrever o código propriamente dito.

   Essa parte é sempre entediante, mas acho que o currículo do BCC nos dá uma visão bastante abrangente de linguagem de programação e então a dificuldade era mais associada à sintaxe do que à filosofia de programação. Por outro lado, todos nós, cedo ou tarde, vamos passar por professores que não nos ajudam muito e nos fazem descobrir as coisas sozinhos. Esse, certamente não foi o primeiro trabalho em que tive que decifrar códigos de outras pessoas.

   Em suma, as matérias que mais me auxiliaram nessa etapa foram:

   - MAC122:

     Essa matéria dá boa parte da base necessária para se produzir algoritmos. Foi nesse momento do curso que aprendi a diferença entre programar muito mal e programar mal. Acho que é uma das matérias mais importantes do BCC.

   - Conceitos de Linguagem de Programação:

     Essa disciplina mostra outras linguagens de programação pouco intuitivas e apresenta outras formas de resolver problemas. Acho que foi por conta dessa matéria que eu não estranhei a linguagem do Mathematica.

7.2 Frustrações

Eu não tive frustração alguma relacionada ao TCC e acho que isso se deve ao fato de ter esticado meu curso e poder ter me dedicado quase integralmente ao projeto. Se não fosse assim, esse trabalho seria completamente inviável.

7.3 Conclusão

Considero esse projeto a atividade mais importante que realizei durante todo o curso. Foi uma experiência única estudar um determinado tema por 2 anos intensamente e aplicar o conhecimento em algum lugar da mesma forma que eu pude ver sendo feito em Programação Linear. Acho apenas que deveria ser dado mais tempo ao aluno para fazer o trabalho, mas não sei como isso poderia ser feito. Pretendo continuar estudando álgebra e no próximo ano inicio o mestrado em matemática.

Nesse trabalho, eu pude entender razoavemente bem a teoria de Galois e compreender quase que completamente tudo o que cerca o meu trabalho. As poucas dúvidas que tenho estão bem delimitadas e certamente não representam problemas para o projeto.

A parte do algoritmo do 5^o grau foi inteiramente feita por mim desde a confecção do algoritmo até a sua demonstração. Isso mostra o quanto eu compreendi do trabalho.

Além disso, a maior mostra de que realmente aproveitei o trabalho foi ter compreendido mais profundamente Teoria de Galois. Essa matéria que permaneceu incompreensível por mais de 1 ano ficou bastante clara depois de exatamente 2 anos. Esse ganho eu considero de valor inestimável pois, pela primeira vez eu realmente entendi tudo o que estava fazendo e principalmente o que Galois fez.

Apêndice A

Representação dos grupos de Galois

Grupo de Galois	Ordem	Geradores
Grau 1		
$\mathfrak{S}_1$	1	(1)
Grau 2		
$\mathfrak{S}_2$	2	(12)
Grau 3		
$\mathfrak{S}_3$	6	$(12), (13)$
A_3	3	(123)
Grau 4		
$\mathfrak{S}_4$	24	$(12), (13), (14)$
A_4	12	$(123), (134)$
V_4	4	$(12)(34), (14)(23)$
D_4	8	$(1234), (24)$
C_4	4	(1234)
Grau 5		
$\mathfrak{S}_5$	120	$(12), (13), (14), (15)$
A_5	60	$(123), (134), (145)$
C_5	5	(12345)
D_5	10	$(12345), (25)(34)$
F_{20}	20	$(12345), (2354)$

Grupo de Galois	Ordem	Geradores
Grau 6		
$\mathfrak{S}_6$	720	$(12), (13), (14), (15), (16)$
A_6	360	$(123), (134), (145), (156)$
C_6	6	(123456)
D_6	12	$(123456), (16)(25)(34)$
A_4	12	$(25)(36), (135)(246)$
$S_4 \times C_2$	48	$(14), (135)(246), (26)(35)$
$A_4 \times C_2$	24	$(14), (135)(246)$
S_4^+	24	$(25)(36), (135)(246), (26)(35)$
S_4^-	24	$(25)(36), (135)(246), (14)(26)(35)$
$D_3 \times D_3$	36	$(135), (26)(35), (14)(25)(36)$
$C_3 \times D_3$	18	$(135), (14)(25)(36)$
$C_3^2 \times C_4$	36	$(135), (26)(35), (14)(2563)$
$C_3^2 \times D_4$	72	$(135), (35), (14)(25)(36)$
S_5	120	$(12345), (16)(54)(32)$
A_5	60	$(12345), (16)(25)$
S_3	6	$(135)(246), (16)(25)(34)$
Grau 7		
$\mathfrak{S}_7$	5040	$(12), (13), (14), (15), (16), (17)$
A_7	2520	$(123), (134), (145), (156), (167)$
C_7	7	(1234567)
D_7	14	$(1234567), (27)(36)(45)$
F_{42}	42	$(1234567), (243756)$
F_{21}	21	$(1234567), (235)(476)$
$PSL_2(F_7)$	168	$(1234567), (23)(47)$

Referências Bibliográficas

[1] P.A. Martin, INTRODUÇÃO À TEORIA DOS GRUPOS E À TEORIA DE GALOIS, IMEUSP.

[2] I.N. Herstein, TÓPICOS DE ÁLGEBRA, Polígono, São Paulo, 1964.

[3] I. Stewart, GALOIS THEORY, Chapman and Hall, 1989.

[4] G. Butler and J. McKay, The transitive groups of degree up to eleven, Comm. in Algebra 11 A983), 863-911.

[5] H. Cohen, A COURSE IN COMPUTATIONAL ALGEBRAIC NUMBER THEORY, Springer.