Universidade Federal de Minas Gerais

Instituto de Ciências Exatas

Departamento de Matemática

Especialização em Matemática

Polinômios, Corpos de Decomposição e uma Introdução à Teoria de Galois

Autor: Leandro dos Santos Fernandes

Orientador: Prof. John MacQuarrie

Belo Horizonte-MG

Julho / 2016

Universidade Federal de Minas Gerais

Instituto de Ciências Exatas

Departamento de Matemática

Especialização em Matemática

Leandro dos Santos Fernandes

Polinômios, Corpos de Decomposição e Uma Introdução à Teoria de Galois

Belo Horizonte-MG

2016

LEANDRO DOS SANTOS FERNANDES

POLINÔMIOS, CORPOS DE DECOMPOSIÇÃO E UMA INTRODUÇÃO À TEORIA DE GALOIS

Monografia apresentada ao Departamento de Matemática da Universidade Federal de Minas Gerais como parte dos requisitos para obtenção do título de Especialista em Matemática.

Orientador: Prof. Dr. John MacQuarrie

Belo Horizonte-MG

2016

Sumário

Resumo

O presente trabalho tem como objetivo apresentar de maneira breve a Teoria de Galois e um cálculo dos grupos de Galois de polinômios de grau baixo, em corpos de característica nula.

Palavras-chave: Teoria de Galois, Grupos de Galois, Corpos de decomposição.

Abstract

The objective of this text is to give a brief introduction to Galois theory and to computer the Galois groups of low degree polynomials in a field of caracteristic zero.

Keywords: Galois Theory, Galois Groups, Splitting field.

Capítulo 1

Introdução

Um dos mais belos episódios da matemática ocorreu no início do século XIX. A história de um jovem, que embora uma vida banhada em um mar de frustrações, como a rejeição na "*École Polytechnique*"e uma morte precoce em Paris, aos 20 anos, Evariste Galois, é o responsável por abrir portas a solução de problemas que envolvia raízes de polinômio, como a explicação da não resolução de alguns polinômios de quinto grau.

O presente trabalho tem como fim, dar uma introdução ao estudo da teoria iniciada por Galois, e mostrar alguns exemplos de sua aplicação. Para isso foi estudado os livros de STWART, SNAITH, MORANDI, KAPLANSKY, ROTMAN, WEINTRAUB e MARTIN, que nos explicam sobre a teoria de Grupos, a teoria de Corpos e nos apresenta o *Teorema Fundamental da Teoria de Galois*, também chamado de "*Correspondência de Galois*"que faz a conexão entre as duas teorias. Este teorema será o núcleo deste trabalho.

Dessa forma, antes de chegarmos propriamente no *Teorema Fundamental da Teoria de Galois*,vamos rever rapidamente os conceitos e resultados importantes sobre o estudo de Grupos e Corpos.

No primeiro capítulo, revisaremos as principais estruturas algébricas, grupos, anéis e corpos. Também falaremos sobre polinômios e espaços vetoriais, abordando os resultados necessário para dar seguimento ao trabalho. Aqui não será apresentado nenhuma demonstração, se tratando apenas de uma revisão. Os que desejarem conhecer a prova dos resultados, poderão encontrar nos livros usados como referência.

No Capítulo 2, temos nossos principais resultados, e o desenvolvimento propriamente dito de nossa pesquisa, e as demonstrações dos resultados apresentados se encontram ao longo do texto, com exceção de alguns poucos que foram omitidos devido a sua complexidade ou alguma outra conveniência, mas esses são raros, a grande parte esta demonstrada.

A Seção 3.1, nos diz sobre extensões de corpos. Dessa forma mostramos o *Teorema da*

Torre, falamos sobre as *Extensões Algébricas*, concluindo as definições sobre *Extensões Normais* e *Extensões Separáveis* e o *Teorema do Elemento Primitivo*.

Logo após, na Seção 3.4, cujo o título é *Teoria de Galois*, nos indica o início da teoria estudada. Encontraremos nessa seção a definição de *Extensões de Galois* e *Grupos de Galois*, na Seção 3.3, temos o objetivo de mostrar que o grau de uma *Extensão de Galois* é igual a ordem de seu *Grupo de Automorfismo* (*Grupo de Galois*) e na Seção 3.2 veremos que se uma extensão é *Normal* e *Separável* ela também é uma *Extensão de Galois*. É também nesta seção que trataremos do *Teorema da Correspondência de Galois*.

No Capítulo 3, vamos expor outros resultados interessantes para o nosso estudo, que virá colocando no centro o *Teorema Fundamental*, apresentado na seção que o precede. Veremos a definição e resultados sobre *Extensões Ciclotômicas* e *Extensões Solúveis*, dando enfase o fato da não solubilidade algumas extensões de grau cinco ou superior, e com isso a prova da impossibilidade de um algoritmo para solução de equações de grau 5 ou superior, já que o grande fato é que nem toda raiz de polinômio de grau maior ou igual a 5, pode ser escrito por meio de radicais.

Embora a seção 4.2, se conclui com o teorema de não solubilidade para polinômios de quinto grau, é na Seção 4.3, mostraremos o *cálculo dos grupos de Galois* para polinômios de grau mais baixo, veremos alguns métodos fáceis de se conseguir o grupo de Galois de um polinômio a partir do que sabemos de suas raízes. Finalizamos o trabalho com alguns exemplos sobre tais cálculos.

Alguns pontos são importantes para a leitura do texto, como o fato de darmos foco a teoria em cima de extensões algébricas de característica zero, ou seja toda extensão aqui é separável, (como veremos ao longo do texto) o que conclui que a única coisa que difere se uma extensão ser de *Galois* ou não é a normalidade, um fato explicado no segundo capítulo. Nosso objetivo é somente uma breve leitura, sobre a *Teoria de Galois*, ficando o estudo de resultados mais profundos, e releituras e exploração de novos resultados para trabalhos futuros.

Capítulo 2

Estruturas Algébricas

2.1 Grupos

Definição 2.1. *(Grupo)* Seja G *um conjunto e* $\cdot$ *, uma operação definida sobre os elementos deste conjunto, então* $(G, \cdot)$ *é um grupo se são válidas as seguintes propriedades:*

- *Fechamento Se* $a, b \in G$ *então* $a \cdot b \in G$*, para todo par* $a, b \in G$*.*
- *Associatividade: Temos* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$*, Para todo trio* $a, b, c \in G$*.*
- *Elemento neutro: Existe o elemento* $1 \in G$*, tal que* $1 \cdot a = a$*, para todo* $a \in G$*.*
- *Inverso:Para todo* $a \in G$*, existe o elemento* $a^{-1} \in G$ *tal que* $a \cdot a^{-1} = 1$*. Nestas condições dizemos que* a^{-1} *é o inverso de* a*.*

Proposição 2.2. *Em todo grupo* $(G, \cdot)$*, o elemento neutro é único e todo elemento possui um único inverso.*

Definição 2.3. *(Grupo abeliano)* $(G, \cdot)$ *será um grupo abeliano se* $a \cdot b = b \cdot a$*, para todo* $a, b \in G$*.*

Definição 2.4. *(Subgrupo)* $(H, \cdot)$ *é subgrupo de* $(G, \cdot)$ *se,* H *é um subconjunto de* G*, e* H *satisfaz as condições de grupo com a mesma operação que* G*. Neste caso notamos* $H \leqslant G$

Proposição 2.5. *Seja* G *um grupo e* H *um subconjunto não vazio de* G*.* $(H, \cdot)$ *será subgrupo de* $(G, \cdot)$ *se, para todo par* $a, b \in H$*,* $a \cdot b^{-1} \in H$*.*

Exemplo 2.6. Chamamos de *subgrupo trivial*, o subgrupo formado apenas pela identidade de um grupo $(G, \cdot)$. Vemos que todos as propriedades se satisfazem para esse grupo. É fechado pois $1 \cdot 1 = 1$, é associativo pois $1 \cdot (1 \cdot 1) = (1 \cdot 1) \cdot 1$, e vemos o elemento neutro é seu próprio inverso. Notemos também que quando $(G, \cdot)$ é um grupo, $G \leqslant G$, pois $G \subset G$, e com isso satisfaz as propriedades de subgrupo.

Definição 2.7. *(Ordem de um grupo) Definimos ordem de um grupo $(G,\cdot)$ o cardinal, $|G|$ correspondente ao número de elementos deste grupo.*

Se $|G|$ é um número natural, então $(G,\cdot)$ será um grupo finito, mas caso o contrário, será um grupo infinito.

Definição 2.8. *Seja $g \in G$, onde $(G,\cdot)$ é um grupo, dizemos que n é a ordem de $g \in G$ o menor valor natural n tal que $g^n = g \cdot g \cdots g = 1$ neste caso $n = o(g)$, caso este natural exista.*

Definição 2.9. *Seja $(G,\cdot)$ um grupo, dado um elemento $g \in G$, chamamos de classe lateral a direita, o conjunto $Hg := \{hg | h \in H\}$ e classe lateral a esquerda, o conjunto $gH := \{gh | h \in H\}$.*

Definição 2.10. *(subgrupo normal) Seja $(G,\cdot)$ um grupo e $N \leqslant G$. Dizemos que N é normal a G se, para todo $g \in G$ e $a \in N$, $(gag^{-1}) \in N$, ou $g \cdot N = N \cdot g$. Neste caso escrevemos, $N \triangleleft G$.*

Definição 2.11. *(Subconjuntos geradores) Seja $(G,\cdot)$ um grupo e $H_1, H_2 \subset G$, a partir destes conjuntos definimos dois outros conjuntos:*

- $H_1H_2 = \{ab | a \in H_1, b \in H_2\}$
- $\langle H_1, H_2\rangle$ *que é a intersecção de todos os subgrupos de $(G,\cdot)$ que contém H_1 e H_2. Chamamos este conjunto de subgrupo gerado por H_1 e H_2.*

Proposição 2.12. *Sejam $H_1, H_2 \leqslant G$.*
(i) H_1H_2 é subgrupo de G se só se $H_1H_2 = H_2H_1$.
(ii) $H_1H_2 = H_2H_1$ se só se $H_1H_2 = \langle H_1, H_2\rangle$.

Proposição 2.13. *Seja $(G,\cdot)$, um grupo tal que, $H \leqslant G$, as seguintes afirmações são verdadeiras:*
(i) Dado qualquer $g \in G$ o mapa $\lambda : H \to gH$, dado por $\lambda(h) = gh$ é uma bijeção.
(ii) Para quaisquer $g_1, g_2 \in G$, temos a igualdade de classes $g_1H = g_2H$ ou $g_1H \cap g_2H = \emptyset$.

Definição 2.14. *(Índice de um subgrupo) Seja $(G,\cdot)$ e $H \leqslant G$. O índice de H sobre G, é o número de classes laterais que esse subgrupo possui. A notação comum neste caso é $[G : H]$.*

Definição 2.15. *(Grupo quociente)*

Se $N \triangleleft G$ então o conjunto $G/N := \{aN | a \in G\}$, com a operação $aN \cdot bN = abN$, onde $a, b \in G$ é um grupo. Chamamos esse grupo de grupo quociente.

Teorema 2.16. *(Teorema de Lagrange) Seja $(G,\cdot)$ e $H \leqslant G$ então,*

$$|G| = |H|[G : H]$$

Proposição 2.17. *Todo grupo tem pelo menos dois subgrupos normais, o trivial e ele mesmo.*

Proposição 2.18. *Seja G um grupo abeliano. Se H é subgrupo de G então $H \triangleleft G$.*

Teorema 2.19. *Sejam $S, H \leqslant G$, as seguintes afirmações são verdadeiras.*
(i) $S \cup H \leqslant G$ se só se, $H \subset S$ ou $H \supset S$.
(ii) Se $H \triangleleft G$ então $HS \leqslant G$ e $(H \cap S) \triangleleft S$
(iii)Se $H, S \triangleleft G$ então $HS \triangleleft G$ e $(H \cap S) \triangleleft G$.

2.1.1 Teorema da Orbita e do Estabilizador

Definição 2.20. *(Ação) Sejam G e X conjuntos, tais que $(G, \cdot)$ é um grupo, uma ação de G em X é dada pela relação:*

$$G \times X \to X$$
$$(g, x) \to g \cdot x,$$

tais que: (i) $1 \cdot x = x$, para todo $x \in X$
(ii)$(gh)x = g(hx)$ para todo $\in X$ e para todo $g, h \in G$
Dizemos nestas condições que G age em X.

Definição 2.21. *(Orbita e Estabilizador) Sejam G e X conjuntos, e o elemento x, tais que $(G, \cdot)$ e $x \in X$. Se G age em X, a orbita de x é o conjunto*

$$O(x) = \{gx | g \in G\}.$$

O Estabilizador será G_x, subgrupo de G, tal que, $G_x = \{g \in G | g \cdot x = x\}$.

Teorema 2.22. *(Teorema da Orbita e do Estabilizador) Seja G um grupo e X um conjunto que contem x. Se G age em X então $|O(x)| = [G : G_x] = |G|/|G_x|$*

Demonstração. Veja a demonstração deste resultado na página 117 de [4] □

2.1.2 Teoremas do Isomorfismo para Grupos

Definição 2.23. *A aplicação $\phi : G \to K$, é um homomorfismo de grupos se $(G, \cdot)$ e $(K, +)$ são grupos, e para todo $a, b \in G$, $\phi(a)\phi(b) = \phi(ab) \in K$. Se ϕ é bijetivo ele é denominado isomorfismo. Caso $(G, \cdot) = (K, +)$, o isomorfismo recebe o nome de automorfismo.*

Definição 2.24. *Sejam G e K conjuntos e $\phi : G \to K$, definimos o conjunto imagem desta aplicação como sendo $Im(\phi) := \{\phi(g) | g \in G, \forall g \in G\}$.*

Antes de alcançarmos o teorema do isomorfismo é conveniente compreendermos algumas resultados sobre homomorfismo.

Lema 2.25. *Se $\phi : G \to K$ é um homomorfismo, podemos concluir que :*
(i) $\phi(1_G) = 1_K$
(ii) $\phi(a)^{-1} = \phi(a^{-1})$ *, para todo* $a \in G$
(iii)$ker(\phi) := \{a \in G; \phi(a) = 1_K\}$ *(chamado núcleo do homomorfismo) e* $ker(\phi) \triangleleft G$.
(iv)$ker(\phi) = \{1_G\}$ *se, só se* ϕ *for um injetivo.*

Teorema 2.26. *(Primeiro Teorema do Isomorfismo) Se $\phi : G \to K$, é um homomorfismo, podemos concluir que existe um isomorfismo $\rho : G/ker(\phi) \to Im(\phi)$, em que $\rho(a \cdot ker\phi) = \phi(a)$*

Proposição 2.27. *Seja $N \triangleleft G$ um subgrupo normal de G e seja $\phi : G \to H$, um homomorfismo de grupos. Se $N \leqslant ker(\phi)$ então existe um homomorfismo $\rho : G/N \to H$ cuja a fórmula é*

$$\rho(gN) = \phi(g),\ \forall g \in G.$$

Teorema 2.28. *(Segundo Teorema do Isomorfismo) Sejam $H, K \leqslant G$ com $H \triangleleft G$. Então $H \triangleleft HK$, e existe o seguinte isomorfismo :*

$$\rho : \frac{K}{K \cap H} \to \frac{HK}{H}$$

definida pela fórmula

$$\rho(k(K \cap H)) = kH \in \frac{HK}{H}.$$

Teorema 2.29. *(Terceiro Teorema do Isomorfismo) Sejam $H, K \triangleleft G$ com $K \leqslant H \leqslant G$. Então existe o isomorfismo*

$$\rho : \frac{G/H}{K/H} \to \frac{G}{K}$$

cuja a fórmula expressa

$$\rho(gH(K/H)) = gK.$$

Definição 2.30. *(Grupo cíclico) Um grupo $(G, \cdot)$ é dito cíclico se existe $g \in G$ tal que $G = \{1, g, g^2, \cdots, g^{n-1}\}$.*

Proposição 2.31. *Todo grupo de ordem prima p, é cíclico e isomorfo a $\mathbb{Z}/p\mathbb{Z}$.*

Lema 2.32. *Se $(G, \cdot)$ é um grupo cíclico de ordem n então $(G, \cdot)$ é isomorfo a $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Teorema 2.33. *Seja G um grupo cíclico. Podemos afirmar que:*

(i) Todo subgrupo de G é cíclico.

(ii) Para todo $d \in \mathbb{N}$ que divide $|G|$, existe um único subgrupo de G de ordem d.

Teorema 2.34. *Todo grupo abeliano finito é isomorfo a um produto de grupos cíclicos de ordem de potência de primos.*

2.2 Anéis

Definição 2.35. *(Anel) Seja R um conjunto munido de duas operações, adição $(+)$ e multiplicação $(*)$, onde R com a adição $(R,+)$ é um grupo abeliano, onde o elemento identidade é 0, e $(R,*)$ com a multiplicação satisfaz a associatividade e 1 é a identidade multiplicativa. Ainda existe a distributividade , que relaciona as duas operações .*

- *Distributividade: Para todo $r,x,y \in R$ $r*(x+y) = r*x + r*y$ e $(x+y)*r = x*r + y*r$.*

Proposição 2.36. *Seja $(R,+,*)$ um anel, para todo $x \in R$ o produto $0*x = x*0 = 0$.*

Definição 2.37. *(Anel comutativo) $(R,+,*)$ é um anel comutativo, se este for um anel e $(R,*)$ possuir a propriedade da comutatividade, ou seja $x*y = y*x$, $\forall x,y \in R$.*

Definição 2.38. *(Divisores de zero) Um elemento $a \neq 0 \in R$, é divisor de zero quando, existe algum $b \neq 0 \in R$ tal que $ab = 0$.*

Definição 2.39. *(Domínio de Integridade) R é um Domínio de Integridade se for um anel comutativo que não possua divisores de zero.*

Exemplo 2.40. Em $(\mathbb{Z}_6,+,*)$, onde temos divisores de zero já que $2*3 = 0$, Mas em $(\mathbb{Z},+,*)$ não temos nenhum elemento diferente de 0 tal que multiplicado a outro se anule, neste caso $\mathbb{Z}$ é um *Domínio de Integridade.*

Definição 2.41. *(Ideal) Um ideal em um anel $(R,+*)$ é um subconjunto I que contem o elemento 0 tal que:*

(i) Se $a,b \in I$ então $a-b \in I$

(ii) Se $a \in I$ e $r \in R$ então $ra \in I$ e $ar \in I$

Por costume notamos $I \triangleleft R$, quando I é um ideal de R

Definição 2.42. *(Anel Quociente) Se I é um ideal de $(R,+,*)$ então o anel quociente R/I é o conjunto $I+r$, onde :*

$$(I+r)+(I+s)=I+(r+s)$$
$$(I+r)(I+s)=I+(rs)$$

onde $r,s \in R$ e $I+r$ é o conjunto $\{i+r | i \in I\}$.

Definição 2.43. *(Característica de um anel) A característica do Anel $(R,+,*)$, escrevemos $char(R)$, é o menor $n \in \mathbb{N}$ tal que $0 = n*x = x+\cdots+x$ (n vezes), para todo $x \in R$. Caso não exista $n \in \mathbb{N}$ que satisfaça a equação temos $char(R) = 0$ e dizemos que R é um anel de característica nula.*

Exemplo 2.44. $(\mathbb{Z}, +, *), (\mathbb{Q}, +, *)$ são exemplos de anéis de característica nula. Enquanto $(\mathbb{Z}_p, +, *)$, onde $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, é um anel de característica p, já que $p * 1 = 0$, e p não possui divisores naturais diferentes dele mesmo e maiores que 1.

2.3 Corpos

Definição 2.45. *(Corpo) Dizemos que o domínio de integridade $(F, +, *)$ é um corpo, se $(F, +)$ e $(F \ \{0\}, *)$ forem grupos abelianos.*

Exemplo 2.46. $(\mathbb{Q}, +, *)$ $(\mathbb{R}, +, *)$ e $(\mathbb{C}, +, *)$, onde as operações $+$ e $*$ são as operações usuais de soma e produto, são exemplos de corpos de característica nula. Enquanto $(\mathbb{Z}_p, +, *)$, onde $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, é um corpo de característica p, onde p é primo. Já $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ nem sempre é um corpo, se $n = 6$ sabemos que $2 * 3 = 0$, e em domínio de integridade não existe divisores de zero.

Proposição 2.47. *Se $(F, +, *)$ é um corpo então $char(F) = p$, onde p é um número primo, ou $char(F) = 0$.*

2.3.1 Espaço vetorial

Definição 2.48. *(Espaço vetorial) Seja o corpo $(F, +, *)$, dizemos que o conjunto V será um $F-$espaço vetorial se, este com duas leis de composição*

- *adição: $V \times V \to V, (v, w) \to v + w$.*

- *multiplicação por escalar: $F \times V \to V, (\alpha, w) \to \alpha w$.*

E para essas operações satisfazem as seguintes propriedades:

- *Com a adição é um grupo abeliano.*

- *A multiplicação por escalar é associativa, ou seja para todo par $a, b \in F$ e para todo $v \in V$, então $(ab)v = a(bv)$.*

- *O elemento $1 \in F$ é a identidade, tal que $1v = v$, para todo $v \in V$*

- *Temos as propriedades distributivas, ou seja, $(a + b)v = av + bv$ e $a(v + w) = av + aw$, para todo $a, b \in F$ e para todo $v, w \in V$.*

Definição 2.49. *(Base de um F-espaço vetorial) Seja V, um $F-$ espaço vetorial, e $B_F^V := \{v_1, \cdots, v_n\}$ um conjunto linearmente independente. Diremos que B_F^V é uma base para o espaço vetorial V se, os elementos de B_F^V, geram V, ou seja, todo elemento de V pode ser escrito como $v = a_1v_1 + \cdots + a_nv_n$, onde $a_1, \cdots a_n \in F$. Nestas condições diremos também que a dimensão da base de V é n, onde n é o número de vetores que temos na base B_F^V, e escrevemos $dim(V) = n$*

2.4 Polinômios

Definição 2.50. *(Polinômio) Seja R um domínio de integridade. O conjunto $R[x]$, é formado por todas as expressões $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$, com $n \in \mathbb{N}$, onde para cada $a_i \in R$, denominado coeficiente de x^i em $f(x)$. As expressões $f(x) \in R[x]$ são chamadas polinômios.*

Definição 2.51. *(Igualdade de polinômio) Sejam dois polinômios $f, g \in R(x)$ tais que $f(x) = \sum_{i\leq n} a_ix^i$ e $g(x) = \sum_{i\leq n} b_ix^i$, então $f = g$ se somente se $a_i = b_i$ para todo $i \leq n$.*

Definição 2.52. *(Grau de um polinômio) O grau de um polinômio $f(x) \in R[x]$, tal que $f(x) = \sum_{i\leq n} a_ix^i$ e $a_n \neq 0$ é $n \in \mathbb{N}$ e denotamos $deg(f) = n$, ou $deg(f(x))$. Disto, sabemos que, $deg(f) = 0$ se somente se $f(x) = a \in R$.*

Definição 2.53. *(Soma e produto de polinômios) Seja $f_1 = \sum_i^n a_ix^i$, $f_2 = \sum_j^m b_jx^j$ polinômios em R e $deg(f_2) \leq deg(f_1)$ definimos a soma de polinômio como*

$$f_1 + f_2 = \sum_{i=0}^n a_ix^i + \sum_{j=0}^m b_jx^j = \sum_i^k (a_i + b_i)x^i$$

O produto desses elementos é dado por

$$f_1 * f_2 = (\sum_i^n a_ix^i)(\sum_j^m b_jx^j)$$

que resulta em

$$f_1 * f_2 = \alpha_0 + \alpha_1x + \alpha_2x^2 + \cdots$$
$$\alpha_k = \sum_{j+i=k} a_ib_j = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$$

Proposição 2.54. *(Anel de polinômio) O conjunto $R[x]$, dos polinômios com coeficientes no anel $(R, +, *)$ também é um anel.*

Proposição 2.55. *Sejam $f_1, f_2 \in R[x]$, então $deg(f_1 * f_2) \leq deg(f_1) + deg(f_2)$, e sempre teremos a igualdade quando $R[x]$ for um domínio de integridade.*

Proposição 2.56. *Se R é um domínio de integridade, $R[x]$, também será um domínio de integridade com as mesmas operações.*

Proposição 2.57. *Seja $f(x) \in F[x]$ e seja $a \in F$, onde F é um corpo. Se $p(a) = 0$ então, existe $q(x) \in F[x]$, tal que $p(x) = (x - a)q(x)$*

Definição 2.58. *(polinômio irredutível)*

Um polinômio $p(x) \in F[x]$, onde F é um corpo, é dito irredutível se não houver polinômios $q(x)$, $r(x) \in F[x]$, ambos não constantes tais que $p(x) = q(x)r(x)$. Caso p não seja irredutível dizemos que p é redutível.

Definição 2.59. *Seja F um corpo e $p, q, f \in F[x]$. Quando $f(x) = p(x)q(x)$, dizemos que $f(x)$ é divisível por $p(x)$ e $q(x)$ ou que $p(x)$ e $q(x)$ são divisores de $f(x)$.*

Definição 2.60. *(Máximo Divisor Comum) Seja dois polinômios $f, g \in F[x]$ o máximo divisor comum entre f e g, será o polinômio de maior grau, pertencente ao mesmo domínio de polinômio, que divide f e g. Para esse polinômio notamos $mdc(f, g)$.*

Definição 2.61. *Seja n um inteiro, definimos um polinômio como $n-$ésimo polinômio ciclotômico se este for o minimal das raízes de,*

$$f_n(x) = \frac{x^n-1}{x-1} = x^{n-1} + \cdots + x + 1$$

Teorema 2.62. *(Critério de Eisenstein) Seja $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. Se p é um inteiro primo tal que p não divide a_n mas, p divide a_i, para todo $i < n$, e p^2 divide a_0, então $f(x)$ é irredutível em $\mathbb{Q}[x]$.*

Corolário 2.63. *Seja o polinômio $f_p(x) = \frac{x^p-1}{x-1} \in \mathbb{Q}[x]$, se $n \in \mathbb{Z}$, então $f_p(x) \in \mathbb{Q}[x]$ é irredutível, se somente se p for primo.*

Corolário 2.64. *Seja o polinômio $x^n - a \in \mathbb{Q}[x]$, se $a \in \mathbb{Z}$ não é um quadrado perfeito, então este polinômio é irredutível para todo $n \geq 2$.*

Exemplo 2.65. São exemplos de polinômios irredutíveis em $\mathbb{Q}[x]$, $x + 1$, $x^2 + 1$, $x^n + p$, onde p neste caso é um número primo.

Teorema 2.66. *(Algoritmo da divisão de polinômios)Seja F um corpo e $f, g \in F[x]$ onde $g \neq 0$. Então existe únicos $q, r \in F[x]$ tais que $f = gq + r$, na qual $r = 0$ ou $deg(r) < deg(q)$.*

Teorema 2.67. *Seja K um corpo e suponha que $m(x) \in K[x]$ é mônico e irredutível. Seja $\langle m(x) \rangle$ o ideal de $K[x]$ formado por todos os múltiplos de $m(x)$. Então $K[x]/\langle m(x) \rangle$ é um corpo, e existe um monomorfismo natural $\iota : K \to K[x]/\langle m(x) \rangle$ tal que $\iota(k) = \langle m(x) \rangle + k$.*

Capítulo 3

A Teoria de Galois

3.1 Extensão de corpos

Definição 3.1. *(Extensão de corpos) Dizemos que o corpo $(K, +, *)$ é uma extensão do corpo $(F, +, *)$, e escrevemos K/F, se $F \subset K$. Nestas condições também dizemos que $(F, +, *)$ é um subcorpo de $(K, +, *)$.*

Exemplo 3.2. Sabemos que $(\mathbb{R}, +, *)$ e $(\mathbb{Q}, +, *)$ são corpos e $\mathbb{Q} \subset \mathbb{R}$, portanto $\mathbb{R}/\mathbb{Q}$, e $(\mathbb{Q}, +, *)$ é um subcorpo de $\mathbb{R}$.

Proposição 3.3. *Se K/F é um extensão de corpos podemos concluir que K é um $F-$espaço vetorial.*

Demonstração. Seja K/F uma extensão de corpos. Pela Definição 3.1, sabemos que se $a \in F$, então $a \in K$, para todo $a \in F$, pois $F \subset K$.

Dado $a, b \in F$ e $v, w \in K$, as condições para termos um $F-$espaço vetorial, vistas na Definição 2.48 são satisfeitas. Vejamos que, $a \cdot v \in K$ e como K é um corpo, podemos falar que K é um grupo abeliano aditivo, a multiplicação é associativa, $1 \in K$, por definição de corpo, e de igual forma vale a propriedade distributiva. □

Definição 3.4. *(Grau de uma extensão)*

Se K/F é uma extensão de corpos, o grau da extensão é a dimensão de K, visto como $F-$espaço vetorial, e escrevemos $[K : F]$. Se o grau for finito, dizemos que a extensão é finita, caso contrário temos uma extensão infinita.

Definição 3.5. *(Base de uma extensão) Definimos base da extensão de corpos K/F, como o conjunto B_F^K, que é base de K visto como $F-$espaço vetorial.*

Exemplo 3.6. Sejam os corpos $(\mathbb{C}, +, *)(\mathbb{R}, +, *)(\mathbb{Q}, +, *)$, temos que :

1. $[\mathbb{C} : \mathbb{R}] = 2$, logo $\mathbb{C}/\mathbb{R}$ é uma extensão finita.

2. $[\mathbb{R} : \mathbb{Q}] = \infty$, logo $\mathbb{R}/\mathbb{Q}$ é uma extensão infinita.

Por comodidade, e para não sobrecarregar nossas notações, a partir daqui usaremos somente a notação do conjunto para designar a estrutura algébrica, e as operações são as convencionais, quando não explicitadas, sempre vindo portanto especificado o tipo da estrutura que estamos lidando, dessa forma falaremos que K é um corpo ou G é um grupo, omitindo as notações de $(K, +, *)$ ou $(G, \cdot)$ que eram comuns.

3.1.1 Teorema da Torre

Definição 3.7. *(Torre de corpos)*

Dada uma extensão K/F e uma sequência de subcorpos F_i tais que, $F \subseteq F_0 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n \subseteq K$. Nesse caso chamamos K/F de torre de corpos. A torre K/F será finita se $[K : F] = n \in \mathbb{N}$.

Definição 3.8. *(Corpo intermediário) Dizemos que F' é um corpo intermediário da extensão K/F se $F \subset F' \subset K$.*

Teorema 3.9. *(Teorema da Torre) Sejam F',F e K ,tais que K/F uma extensão finita e $F \subset F' \subset K$, então*

$$[K : F] = [K : F'][F' : F]$$

Demonstração. A Proposição 3.3, nos diz que podemos tratar as extensões de corpos como espaços vetoriais. Seja K/F uma extensão finita. Tomemos a base de K/F', $B^K_{F'} := \{x_1, x_2, \cdots, x_n\}$ com n elementos, pela Definição 3.4 temos que $[K : F'] = n$. Por definição de base (Definição 2.49, para todo $v \in F'$ $v = \sum_i \alpha_i x_i = 0$ se só se $\forall \alpha_i \in F$, $\alpha_i = 0$.

Seja também a base de F'/F, $B^{F'}_F = \{y_1, \cdots, y_m\}$, com m elementos, o que nos diz que $[F' : F] = m$ e $w = \sum_j \beta_j y_i = 0$ se só se $\beta_j = 0$, para todo $\beta_j \in F'$.

Nosso passo agora é escrever qualquer elemento de K como combinação linear de elementos de F. Seja então $v \in K$, como visto

$$v = \textstyle\sum_i \alpha_i x_i, \text{ onde } \alpha_i \in F' \text{ e } x_i \in B^K_{F'}.$$

Como $\alpha_i \in F'$, podemos escrever esses elementos como elementos de F'/F. Assim,

$$\alpha_i = \textstyle\sum_j \beta_{j,i} y_j,$$

para algum conjunto $\{\beta_{j,i}\} \in F$, nem todos nulos, onde $y_j \in B_F^{F'}$, de forma que:

$$\begin{aligned}\alpha_1 &= \sum_j \beta_{j,1} y_j \\ \alpha_2 &= \sum_j \beta_{j,2} y_j \\ &\vdots \\ \alpha_n &= \sum_j \beta_{j,n} y_j.\end{aligned}$$

Substituindo esses valores em $v \in F$

$$v = \textstyle\sum_i^n \alpha_i x_i = \sum_i^n (\sum_j \beta_{j,i} y_j) x_i, \text{ onde } \beta_{j,i} \in F.$$

Isso nos garante que o conjunto $\{x_1 y_1, x_2 y_1 \cdots x_n y_1, x_1 y_2 \cdots, x_n y_m\}$ gera os elementos de K, como $F-$espaço vetorial. Agora basta mostrarmos que este conjunto é linearmente independente, com isso será uma base de K/F, de acordo com a Definição 2.49.

Se v é o vetor nulo, então $\sum_i^n (\sum_j \beta_{j,i} y_j) x_i = 0$. Ora, os valores x_i formam um conjunto linearmente independente pois formam um subconjunto de $B_{F'}^K$, ou seja ,

$$\textstyle\sum_i^n (\sum_j^m \alpha_i) x_i = \sum_i^n (\sum_j \beta_{j,i} y_j) x_i = 0 \text{ se só se } \sum_j \beta_{j,i} y_j = 0.$$

da mesma forma , o conjunto dos valores y_j são linearmente independentes, pois base de $B_F^{F'}$, com isso:

$$\textstyle\sum_j \beta_{j,i} y_j = 0 \text{ se somente se para todo } \beta_{j,i} \in F,\ \beta_{j,i} = 0,$$

e vemos que nosso conjunto $\{x_i y_j\}_{i \leq n, j \leq m}$ é base de K/F', contendo $n \cdot m$ elementos. Concluímos que

$$[K : F] = n \cdot m = [K : F'][F' : F]$$

□

Corolário 3.10. *Se F_n/F é uma extensão finita de corpos , tal que $F \subseteq F_2 \subseteq \cdots \subseteq Fn$ então $[F_n : F] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_2 : F]$.*

Demonstração. Como vimos no teorema, dada a torre $F \subseteq F_2 \subseteq \cdots \subseteq F_n$, para qualquer corpo intermediário, F_k,temos que

$$[F_n : F] = [F_n : F_k][F_k : F]$$

desta forma,

$$[F_n : F] = [F_n : F_{n-1}][F_{n-1} : F].$$

Usando o mesmo teorema várias vezes temos que:

$$\vdots$$

$$[F_n : F] = [F_n : F_{n-1}] \cdots [F_2 : F]$$

□

Corolário 3.11. *Seja F_n/F uma extensão finita e seja F_{k+1}/F_k , onde F_{k+1}, F_k, são corpos intermediários de F_n/F. Se $[F_{k+1} : F_k] = m$ e $[F_n : F] = n$ então m divide n.*

Demonstração. Seja a torre de corpos $F \subset F_k \subset F_{k+1} \subset K$. Pelo Teorema 3.9 temos que $n = [F_n : F] = [F_n : F_{k+1}][F_{k+1} : F_k][F_k : F]$, logo $[F_{k+1} : F_k]$ divide n, pois é um fator em uma de suas decomposições. □

Exemplo 3.12. Na torre , $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$$[\mathbb{C} : \mathbb{Q}] = [\mathbb{C} : \mathbb{R}][\mathbb{R} : \mathbb{Q}]$$
$$[\mathbb{C} : \mathbb{Q}] = 2[\mathbb{R} : \mathbb{Q}]$$

Neste exemplo, a extensão $\mathbb{R}/\mathbb{Q}$ é infinita, logo a extensão $\mathbb{C}/\mathbb{Q}$ é infinita. O mesmo não podemos dizer para a torre $\mathbb{C}/\mathbb{R}$, cujo o grau é $[\mathbb{C} : \mathbb{R}] = 2$.

3.1.2 Extensões Algébricas

Definição 3.13. *Na extensão K/F o corpo intermediário, $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ é a interseção de todos os subcorpos de K que contenha F e $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$.*

Definição 3.14. *Seja K/F uma extensão de corpos. Definimos como extensão simples $F(\alpha)/F$, a menor extensão F que contém $\alpha \in K$.*

Definição 3.15. *Dizemos que o elemento $\alpha \in K$ é **algébrico** sobre F, onde K/F é uma extensão de corpos, se existe $f(x) \in F[x]$, tal que $f(\alpha) = 0$. Caso contrário dizemos que α é transcendente sobre F.*

Definição 3.16. *Seja a extensão de corpos K/F , o algébrico $\alpha \in K$ e $m_\alpha(x) \in F[x]$. Se $m_\alpha(x)$ é mônico e $m_\alpha(x)$ tem o menor grau dentre os polinômios $f(x) \in F[x]$, tais $f(\alpha) = 0$, dizemos que $m_\alpha(x)$ é o polinômio minimal de α sobre F.*

Exemplo 3.17. Na extensão $\mathbb{C}/\mathbb{R}$, $\mathbb{C} = \mathbb{R}(i)$, uma vez que para todo $v \in \mathbb{C}$, $v = x + iy$ tal que $x, y \in \mathbb{R}$. Isso justifica o fato de $\mathbb{C}/\mathbb{R}$ ser uma extensão simples, já o polinômio minimal de $i \in \mathbb{C}$ será $x^2 + 1$, nota-se que $i^2 + 1 = 0$ e não existe polinômio de grau 1 em $\mathbb{R}$ tal que i seja sua raiz, pois todos polinômios de grau 1 em $\mathbb{R}[x]$ tem raízes em $\mathbb{R}$, em vista que $x + a \in \mathbb{R}[x]$, se $x + a = 0$ então $x = -a$

Lema 3.18. *O polinômio mínimo $m_\alpha(x) \in F[x]$ de um elemento algébrico $\alpha \in K$, divide todos os outros polinômios $p(x) \in F[x]$ tais que $p(\alpha) = 0$.*

Demonstração. Seja $p(x), m_\alpha(x) \in F[x]$, usando o algorítimo da divisão ,Teorema 2.66, sabemos que existe únicos $q, r \in F[x]$ tais que

$$p(x) = q(x)m_\alpha(x) + r(x)$$

Se $p(\alpha) = 0$ então $p(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = 0$, mas $m_\alpha(\alpha) = 0$, pela Definição 3.16. Com isso $p(\alpha) = 0 + r(\alpha) = 0$, $r(\alpha) = 0$. Se $r(x) \neq 0$, $deg(r) < deg(m_\alpha)$, absurdo pela Definição 3.16. Concluímos com isso que, $p(x) = q(x)m_\alpha(x)$, como desejado, de acordo com a Definição 2.59. □

Exemplo 3.19. Seja $i \in \mathbb{C}$ e $x^2 + 1 \in \mathbb{Q}[x]$. i é um algébrico sobre $\mathbb{Q}$ pois $(i)^2 + 1 = -1 + 1 = 0$. O polinômio $x^2 + 1$ é mínimo de i, assim como nos diz o Lema 3.18, pois ele é mônico e irredutível em $\mathbb{Q}[x]$.

Lema 3.20. *Seja K/F uma extensão de corpos e $\alpha \in K$, então o polinômio minimal $m_\alpha(x)$ é irredutível sobre F.*

Demonstração. Seja $m_\alpha(x) \in F[x]$, o minimal de $\alpha \in K$. Suponha que $m_\alpha(x)$ seja redutível. Logo existem $q, p \in F[x]$, tais que, não possuem uma raiz em comum, tais que $m_\alpha = qp$, pela Definição 2.58. Quando aplicamos $\alpha \in K$, nesta equação temos $0 = m_\alpha(\alpha) = q(\alpha)p(\alpha)$, de acordo com a Definição 3.16. Como $F[x]$ é um domínio de integridade pela Proposição 2.56, temos que $p(\alpha) = 0$ ou $q(\alpha) = 0$.Logo $deg(p) \leq deg(m_\alpha)$ pela Proposição 2.55 e $deg(m_\alpha) \leq deg(p)$ pelo Lema 3.18, para todo $p \in F[x]$ em que $p(a) = 0$, o que nos diz que $m_\alpha = ap(x)$, da mesma forma $m_\alpha = bq(x)$, absurdo pois $p(x)$e $q(x)$, não possuem raízes em comum. Portanto $m_a \in F[x]$ é irredutível. □

Corolário 3.21. *Todo elemento do corpo K que é algébrico sobre o corpo F, possui um único polinômio mínimo em $F[x]$.*

Demonstração. Tomemos o algébrico $\alpha \in K$ e suponha que exista dois polinômios mínimos distintos, $m_1(x)$ e $m_2(x)$ para este elemento. Pelo Lema 3.18, temos que $m_1(x) = m_2(x)q(x)$ para algum $q(x) \in F[x]$ e $m_2(x) = m_1(x)p(x)$ para algum $p(x) \in F[x]$. As Proposições 2.56 e 2.55 nos dizem que $deg(m_1) = deg(m_2) + deg(q)$ e que $deg(m_2) = deg(m_1) + deg(p)$, logo $deg(m_2) = deg(m_2) + deg(q) + deg(p)$, com isso $deg(q) = deg(p) = 0$. Como $p(x)$ e $q(x)$ tem grau nulo, ambos são constantes, ou seja $m_1(x) = m_2(x) \cdot k$, para algum $k \in F$, como m_1 e m_2 são mônicos, pela Definição 3.16, $k = 1$ e $m_1(x) = m_2(x)$. □

Definição 3.22. *(Extensões Algébricas)*

Definimos K/F como uma extensão algébrica se todo elemento de K for algébrico sobre F.

Proposição 3.23. *Seja K/F uma extensão. Se $\alpha \in K$ é um algébrico sobre F, então $F(\alpha) = F(-\alpha)$.*

Demonstração. Seja $\alpha \in K$, um elemento algébrico então elemento $-\alpha \in K$, também é algébrico , pois é raiz do polinômio $g(x) = f(-x) \in F[x]$ tal que $f(\alpha) = 0$. Temos portanto que $-\alpha = -1 \cdot \alpha \in F(\alpha)$, pois $F(\alpha)$ é um corpo. Por definição de extensão simples (Definição 3.14), $F(-\alpha) \subset F(\alpha)$. De forma análoga $\alpha = -1 \cdot (-\alpha) \in F(\alpha)$ e com isso $F(-\alpha) \supset F(\alpha)$. Portanto $F(-\alpha) = F(\alpha)$ □

Teorema 3.24. *Seja α, um algébrico sobre F e $F(\alpha)$ uma extensão simples. Se $m_\alpha(x)$ é o polinômio mínimo de α, então $[F(\alpha) : F] = deg(m_\alpha(x))$.*

Demonstração. Seja $\alpha \in F(\alpha)$ cujo o minimal é m_α. Dividiremos essa demonstração em duas partes. Primeiramente temos que mostrar que o conjunto $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, com $n = deg(m_\alpha(x))$, é um conjunto linearmente independente sobre F. Concluiremos que esse conjunto é uma base de $F(\alpha)/F$.

Para a primeira parte, tomemos um polinômio qualquer, não nulo $p(x) \in F[x]$, em que $deg(p) < n$ certamente $p(\alpha) \neq 0$, pela definição de polinômio minimo (Definição 3.16).

Vamos provar agora que o conjunto $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é uma base de $F(\alpha)$ sobre F. Para isso vamos mostrar que o conjunto $F[\alpha] := \{f(\alpha) |\ f(x) \in F[x],\ deg(f(x)) < n\}$, constitui um corpo, pois $p(\alpha) = \sum_{i=0}^{n-1} b_i \alpha^i$ tal que $b_i \in F$.

Pelo Teorema 2.67, sabemos que $F \to F[x]/\langle m(x)$, nos garante $F[x]/\langle m(x)\rangle$ ser um corpo e por consequência $F[\alpha]$ ser também um corpo, pois $F[\alpha] \cong F[x]/\langle m(x)\rangle$, segundo a definição dada no teorema citado.

Pela definição 3.14 $F(\alpha)$ é o menor corpo que contém F e α, e $F[\alpha] \subset F(\alpha)$, logo $F[\alpha] = F(\alpha)$. Ou seja o conjunto $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $F(\alpha)$. Com isso,

$$[F(\alpha) : F] = |\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}|$$
$$[F(\alpha) : F] = n = deg(m_a(x))$$

□

Exemplo 3.25. Sabemos do Exemplo 3.19 que $x^2 + 1 \in \mathbb{Q}[x]$ é o polinômio minimal de i. Seu corpo de decomposição é $\mathbb{Q}(i)$. $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, Usando as ideias contidas na demonstração sabemos que a base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$ é $\{1, i\}$. Logo neste caso $[\mathbb{Q}(i) : \mathbb{Q}] = deg(m_i(x))$.

Exemplo 3.26. Seja $F(\sqrt{a_0})$ uma extensão de corpos, tal que $a_0 \in F$, se $\sqrt{a_0}$ não pertence a F, logo $[F(\sqrt{a_0}) : F] = 2$, em vista de que, o polinômio mínimo deste caso é $x^2 - a_0 \in F[x]$.

Se em uma extensão $F(\sqrt{a_1} \cdots, \sqrt{a_n})/F$, ocorre que $\sqrt{a_i} \notin F(\sqrt{a_1} \cdots, \sqrt{a_{i-1}})$, para cada $\sqrt{a_i}$, então $[F(\sqrt{a_1} \cdots, \sqrt{a_n}) : F] = 2^n$ Tal afirmativa é justificada pela demonstração do Teorema 3.1.1 e pela demonstração do Teorema 3.24.

3.1.3 Corpos de decomposição

A partir daqui todas as nossas extensões são finitas e os corpos são todos de característica nula.

Definição 3.27. *(Corpo de decomposição de um polinômio)*

O corpo E é chamado como corpo de decomposição do polinômio $f(x) \in F[x]$, se $E = F(\alpha_1, \cdots, \alpha_n)$, onde $\alpha_1, \cdots, \alpha_n$ são as raízes de f.

Neste caso,

$$f = \prod_{i=1}^{n} k(x - \alpha_i)$$

onde $k \in F$, é uma constante.

Lema 3.28. *Seja $F(\alpha_1, \cdots, \alpha_n) = E$. Se $\alpha_1, \cdots, \alpha_n \in E$ são algébricos sobre F então*

$$F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$$

para algum r, tal que $1 \leq r \leq n - 1$.

Demonstração. Seja $\alpha_1, \cdots, \alpha_n$, as raízes de um polinômio $f \in F[x]$. Pela Definição 3.13, o corpo $F(\alpha_1, \cdots, \alpha_n)$ é o menor corpo que contém F e os elementos $\alpha_1, \cdots, \alpha_n$, ou seja, ele é subcorpo de qualquer outro corpo que contenha F e $\alpha_1, \cdots, \alpha_n$. Pela mesma definição o corpo $F(\alpha_1 \cdots, \alpha_r)(\alpha_{r+1} \cdots, \alpha_n)$ é formado pelo corpo $F(\alpha_1 \cdots, \alpha_r)$, que contém F e os elementos $\alpha_1 \cdots, \alpha_r$, e contém também $\alpha_{r+1} \cdots, \alpha_n$. Logo

$$F(\alpha_1, \cdots, \alpha_n) \subset F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$$

A outra inclusão se dá pelo fato de que $F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$ é o menor corpo que contém $F(\alpha_1, \cdots, \alpha_r)$ e os elementos $\alpha_{r+1}, \cdots, \alpha_n$, já $F(\alpha_1, \cdots, \alpha_r)$, é o menor corpo que contém F e $\alpha_1, \cdots, \alpha_r$, logo qualquer corpo que contenha F e os elementos $\alpha_1, \cdots, \alpha_r, \alpha_{r+1}, \cdots, \alpha_n$, contém também $F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$. $F(\alpha_1, \cdots, \alpha_n)$ contém F, $\alpha_1, \cdots, \alpha_r, \alpha_{r+1}, \cdots, \alpha_n$, portanto

$$F(\alpha_1, \cdots, \alpha_n) \supset F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$$

Sendo válida as duas inclusões concluímos que

$$F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$$

□

Exemplo 3.29. Seja $f = (x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$,cuja as raízes são $-\sqrt{3}, \sqrt{3}, -\sqrt{5}, \sqrt{5} \in \mathbb{R}$. Pela Definição 3.27, seu corpo de decomposição é $E = \mathbb{Q}(-\sqrt{3}, \sqrt{3}, -\sqrt{5}, \sqrt{5})$. Pelo Lema 3.28 $\mathbb{Q}(-\sqrt{3}, \sqrt{3}, -\sqrt{5}, \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})(-\sqrt{3}, -\sqrt{5})$, então $\mathbb{Q}(-\sqrt{3}, \sqrt{3}, -\sqrt{5}, \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, pois $-\sqrt{3}, -\sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$, segundo a Proposição 3.23. Portanto $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Teorema 3.30. *Seja $f(x) \in F[x]$ um polinômio de grau $n > 0$ e E o seu corpo de decomposição, então $[E : F] \leq n!$*

Demonstração. Vamos concluir que $[E : F] \leq n!$, para todo $n \in \mathbb{N}$. Caso $n = 1$, teremos $f(x) = a_1x + a_0$, com $a_1 \neq 0$ e $a_1, a_0 \in F$ e sua raiz é $\alpha = -\frac{a_0}{a_1} \in F$. A Definição 3.27, o corpo de decomposição em questão é $F(-\frac{a_0}{a_1})$, como $-\frac{a_0}{a_1} \in F$ temos que $F = F(-\frac{a_0}{a_1})$, logo o grau da extensão é $[F : F] = 1$. Por hipótese de indução assumimos que a afirmação é válida para $n < k \in \mathbb{N}$. Quando $f \in F$ tem raízes $\alpha_1, \alpha_2, \cdots, \alpha_n$, para $n = k - 1$, pela Definição 3.27 o corpo de decomposição de $f \in F$ é $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ e $f = \prod_{i=1}^{n}(x - \alpha_i)$. Quebrando o produto por um polinômio $g \in F(\alpha_1)[x]$ tal que $f = (x - \alpha_1)g$, onde $g = \prod_{i=2}^{n}(x - \alpha_i)$, temos que o corpo de Decomposição do polinômio $g \in F(\alpha_1)[x]$ é

$$F(\alpha_1)(\alpha_2, \cdots, \alpha_n) = F(\alpha_1, \alpha_2, \cdots, \alpha_n) = E,$$

conforme o Lema 3.28 .

Usemos estas afirmações sobre g como hipótese de indução para provarmos o nosso teorema. Sendo válida a nossa afirmação até $n - 1$ temos que

$$[E : F(\alpha_1)] \leq (n - 1)!$$

Pelo "Teorema da Torre"(Teorema 3.9), nós temos

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F] \leq (n - 1)![F(\alpha_1) : F].$$

Sabemos do Teorema 3.24 , que $[F(\alpha_1) : F] = deg(m_{\alpha_1})$, tal que m_{α_1} é o polinômio minimal de α_1 em F e $deg(m_{\alpha_1}) \leq n$, pois α_1 é raiz de f que tem grau n e pela definição de minimal. Portanto

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F] \leq (n - 1)! \cdot n$$
$$[E : F] \leq n!$$

□

Exemplo 3.31. Usando o polinômio $f = (x^2+1)(x^2-5) \in \mathbb{Q}[x]$ que tem como corpo de decomposição $\mathbb{Q}(i, \sqrt{5})$, usando o Teorema da Torre, e o Lema 3.28 vemos que $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(i)(\sqrt{5}) : \mathbb{Q}(i)]deg(m_i)$. Sabemos do Exemplo 3.25, que a base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$ é $\{1, i\}$, com isso os elementos deste corpo são da forma $a_1 + a_2 i$ onde $a_1, a_2 \in \mathbb{Q}$. Se $\sqrt{5} \in \mathbb{Q}(i)$, logo $\sqrt{5} = a_1 + a_2 i$. Se fosse verdadeira essa igualdade, $5 = a_1^2 + 2a_1a_2i - a_2^2$. Como 5 é um número racional, $5 = a_1^2 - a_2^2$ e $2a_1a_2i = 0$, ou seja $a_1 = 0$ ou $a_2 = 0$. Se $a_1 = 0$, então $5 = -a_2^2$, absurdo pois não temos quadrados negativos em $\mathbb{Q}$, se $a_2 = 0$ então $5 = a_1^2$, absurdo pois $a_1 \in \mathbb{Q}$ e a raiz quadrada de 5 não se encontra em $\mathbb{Q}$. Portanto $[\mathbb{Q}(i)(\sqrt{5}) : \mathbb{Q}(i)] = deg(m_{\sqrt{5}})$. O polinômio mínimo de $\sqrt{5}$ é $x^2 - 5$, vejamos que este é irredutível pelo Critério de Eisenstein e tem $\sqrt{5}$ como raiz. Logo, pelo Lema 3.28 $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = deg(m_{\sqrt{5}})deg(m_i) = 4 \leq 4!$, assim como dito no Teorema 3.30.

Lema 3.32. *Se F é um corpo, então as seguintes sentenças são equivalentes:*

- *1) Não existe extensão algébrica de F que não seja F*
- *2) Não existe extensão finita de F que não seja F*
- *3) Se K é uma extensão de F, então $F = \{\alpha \in K |\ \alpha$ é algébrico sobre $F\}$.*
- *4) Todo $f \in F[x]$ se decompõe completamente sobre F.*
- *5) Todo $f \in F[x]$ tem uma raiz em F*
- *6) Todo polinômio irredutível sobre F tem grau 1.*

Demonstração. Faremos a seguinte sequência para demonstração : $1 \to 2 \to 3 \to 4 \to 5 \to 6 \to 1$.

$(1 \to 2)$: Toda extensão finita em um corpo é algébrica, pois se existisse $x \in K$ que fosse transcendente, sobre F, pela Definição 3.15 $[F(x) : F] = \infty$, assim pelo Teorema 3.9 $[K : F] = \infty$. Logo a condição de (1) ainda é garantida.

$(2 \to 3)$: seja $\alpha \in K$ um algébrico sobre F, e seja $F(\alpha)$ o menor corpo extensão de F que contém α. Vimos no Teorema 3.24, que $[F(\alpha) : F] = deg(m_\alpha)$. Assim $F = F(\alpha)$, pois não existe extensões finitas de F, que diferem de F.

$(3 \to 4)$: Seja $f \in F[x]$ tal que K seja seu corpo de decomposição sobre F. Com isso K é algébrico sobre F, por hipótese, $F = \{\alpha \in K : \alpha$ é algébrico sobre $F\}$, ou seja $f(x)$ se decompõe

em F.

$(4 \to 5)$: Se $f(x)$ decompõe-se sobre F então certamente ele tem todas suas raízes em F, por definição de corpo de decomposição (Definição 3.27).

$(5 \to 6)$: Seja f um polinômio irredutível sobre F. Pela afirmação (5) ele tem pelo menos uma raiz em F. Isso nos leva a dizer que $f(x) = (x-\alpha)g(x)$ onde α é a raíz de f em F. Como f é irredutível, $g \in F[x]$ deve ser constante, pela Definição 2.58. Usando a Proposição 2.55, vemos que

$$deg(f) = deg((x-\alpha)) + deg(g) = 1$$

.

$(6 \to 1)$: Seja K/F uma extensão algébrica. Tomemos $k \in K$, então o polinômio mínimo deste elemento, que é irredutível, tem grau 1, pelo item (6), portanto pelo Teorema 3.24, $K = F$. □

Definição 3.33. *(Fecho Algébrico) Seja $\bar{F}/F$ uma extensão de corpos, dizemos que $\bar{F}$ é fecho algébrico de $\bar{F}$ se satisfazer alguma das condições acima. Para qualquer corpo K que satisfaça tais condições dizemos que K é algebricamente fechado.*

3.1.4 Extensões Normais

Definição 3.34. *(Extensão Normal) Uma extensão algébrica N/F é normal se todo polinômio irredutível em $F[x]$ que tenha uma raiz em N se decompõe completamente sobre N.*

Lema 3.35. *Seja $\alpha \in N$ e N/F uma extensão algébrica. A extensão N/F será uma extensão normal, se e somente se o polinômio minimal $m_\alpha(x) \in F[x]$ se decompõe completamente sobre N.*

Demonstração. Seja N/F uma extensão de corpos, $\alpha \in N$ e seu polinômio minimal $m_\alpha(x) \in F[x]$. Se N é normal, a Definição 3.34 nos diz que $m_\alpha \in F[x]$ se decompõe completamente sobre N, devido ao Lema 3.20.

Se para todo $\alpha \in N$, polinômio minimal $m_\alpha(x) \in N[x]$ se decompõe completamente sobre N, então com isso podemos alegar que não existe elementos transcendentes em N, como visto na Definição 3.33, logo N/F é algébrica, ou seja, para todo $\alpha \in N$, podemos tomar $f \in F$ tal que $f(\alpha) = 0$, pela Definição 3.22. Seja $f \in F[x]$ irredutível e $f(\alpha) = 0$, para algum $\alpha \in N$, vamos provar que $f(x)$ é um polinômio minimal de α. Se $f(x)$ não fosse mínimo, pelo Lema 3.18, $f = m_\alpha \cdot g$, tal que $g(x) \in F[x]$ não constante. Pela definição de irredutível (Definição 2.58),

isso é um absurdo. Logo $f \in F[x]$ deve ser minimal. Já sabemos que todo minimal é irredutível (Lema 3.20) portanto N/F é normal, pela Definição 3.34. □

Definição 3.36. *(Multiplicidade de uma raiz) Sendo $f \in K[x]$, um polinômio escrito em seu corpo de decomposição tal que sua decomposição é polinômio como*

$$f = a_0(x - \alpha_1)^{k_1} \cdots (x - \alpha_m)^{k_m}$$

Dizemos que k_i é a multiplicidade da raiz α_i, caso a multiplicidade da raiz for igual a 1, dizemos que essa raiz é simples.

Definição 3.37. *(Separabilidade)*

Polinômio separável:

O polinômio $f \in F[x]$ é dito separável se este não é constante e todas as suas raízes são simples. Em outras palavras f é separável se todas as suas raízes são distintas.

Elemento separável:

Em uma extensão algébrica K/F , dizemos que $\alpha \in K$ é separável, se seu polinômio minimal é separável.

Extensão separável:

A extensão K/F será separável se todo elemento algébrico de K for separável, se todo polinômio irredutível terá todas as suas raízes distintas.

Definição 3.38. *(Elemento primitivo) Dado K/F uma extensão de corpos, $\alpha \in K$ é um elemento primitivo se $F(\alpha) = K$.*

Teorema 3.39. *(Teorema do elemento primitivo) Seja F um corpo de característica zero. Toda extensão separável de F é uma extensão simples.*

Demonstração. O leitor poderá consultar a demonstração deste teorema em [7], página 119. □

Exemplo 3.40. Provemos que $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, para quais quer $a, b \in \mathbb{Q}$. A primeira inclusão é simples, $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \supset \mathbb{Q}(\sqrt{a} + \sqrt{b})$, pois como $\sqrt{a}, \sqrt{b} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$ então $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$, por definição de corpo, Como $\mathbb{Q}(\sqrt{a}+\sqrt{b})$ é o menor corpo que contem $\sqrt{a}+\sqrt{b}$ então $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \supset \mathbb{Q}(\sqrt{a}+\sqrt{b})$. Para a segunda inclusão, $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subset \mathbb{Q}(\sqrt{a}+\sqrt{b})$, basta tomarmos $(\sqrt{a} + \sqrt{b})^2$, que pertence a $\mathbb{Q}(\sqrt{a} + \sqrt{b})$, por definição de corpo. Calculando as potências deste elemento primitivo, temos

$$\begin{aligned}(\sqrt{a} + \sqrt{b})^2 =& a + 2\sqrt{a}\sqrt{b} + b \\ (\sqrt{a} + \sqrt{b})^3 =& a\sqrt{a} + 3a\sqrt{b} + 3b\sqrt{a} + b\sqrt{b} = (a + 3b)\sqrt{a} + (b + 3a)\sqrt{b}.\end{aligned}$$

Com isso, $(a+3b)\sqrt{a}+(b+3a)\sqrt{b}-(a+3b)(\sqrt{a}+\sqrt{b})=2(a-b)\sqrt{b}$. Como, $2(a-b)\in\mathbb{Q}$, $\sqrt{b}\in\mathbb{Q}(\sqrt{a}+\sqrt{b})$ e $\sqrt{a}\in\mathbb{Q}(\sqrt{a}+\sqrt{b})$, pois $\sqrt{a}=+(\sqrt{a}+\sqrt{b})-\sqrt{b}$.

Portanto, $\mathbb{Q}(\sqrt{a},\sqrt{b})=\mathbb{Q}(\sqrt{a}+\sqrt{b})$.

3.2 Teoria de Galois

3.2.1 Automorfismo de Corpos

Definição 3.41. *(Automorfismo) Para qualquer corpo K, chamamos de automorfismo toda bijeção $\phi : K \to K$, onde a soma e o produto deste corpo são preservados, no sentido de que para todo $a, b \in K$,*

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Proposição 3.42. *(Grupo de automorfismo) O conjunto de automorfismo de um corpo K é um grupo com a operação de composição de automorfismos*

Demonstração. Se temos dois automorfismo de K, ϕ, σ a composição é um automorfismo e o inverso também goza das propriedades dessas funções. Isso ocorre pois ,

$$\sigma(\phi(a)) = \sigma(b) \text{ , para } \phi(a) = b \text{ , tal que } a \text{ e } b \in K.$$

e pelo fato de que todo automorfismo é um isomorfismo, portanto possui inverso. Existe $id : K \to K$ onde $id(a) = a, \forall a \in K$ chamamos de automorfismo identidade. Deste modo,

$$\sigma(id(a)) = \sigma(a) = id(\sigma(a)).$$

Se tomamos um outro automorfismo ι de K ,

$$\iota(\sigma\phi(a)) = (\iota\sigma)\phi(a).$$

Com esse fato podemos chegar a conclusão de que o conjunto G de todos os automorfismo sobre K é um grupo com a operação da composição. □

Definição 3.43. *(Grupo de Galois) Seja K/F uma extensão algébrica. O conjunto de todos os automorfismos de K que fixam os elementos de F é chamado de grupo de Galois desta extensão, notamos $Gal(K/F)$. Em outros termos*

$$Gal(K/F) := \{\phi : K \to K, \text{ automorfismo} | \phi(\alpha) = \alpha, \text{para todo} \alpha \in F\}$$

Proposição 3.44. *Seja K/F uma extensão de corpos. O conjunto*

$$Gal(K/F) := \{\phi : K \to K, \text{ automorfismo} | \phi(\alpha) = \alpha, \text{para todo} \alpha \in F\}$$

é um grupo com a operação de composição.

Demonstração. Sabemos da Proposição 3.42, que os automorfismo de K é um grupo com a operação de composição de automorfismo. Se tomamos $\phi, \psi \in Gal(K/F)$, $\phi\psi(x) = \phi(x) = x$ $\forall x \in K$, sabemos também que $\phi^{-1} \in Gal(K/F)$, pois $x = \phi^{-1}\phi(x) = \phi^{-1}(x) = x$ e por fim, todo elemento de $Gal(K/F)$ pertence ao grupo de automorfismo de K, por definição anterior. □

Lema 3.45. *Seja K/F uma extensão algébrica e E um corpo intermediário, então $Gal(K/E)$ é subgrupo de $Gal(K/F)$.*

Demonstração. Seja $\phi \in Gal(K/E)$ então $\phi(x) = x$, $\forall x \in E$. Se $z \in F$, então $z \in E$, pois $F \subset E$, logo para o mesmo automorfismo $\phi \in Gal(K/E)$, $\phi(z) = z$, ou seja, $\phi \in Gal(K/F)$. Vamos usar agora a Proposição 2.5 para mostrar que $Gal(K/E) \leq Gal(K/F)$. Tomemos $\phi_a, \phi_b \in Gal(K/E)$, $\phi_b^{-1} \in Gal(K/E)$, pois $id(x) = \phi_b \cdot \phi_b^{-1}(x) = x$, para todo $x \in E$, pela Definição 3.43, logo $\phi_b^{-1} \in Gal(K/E)$. $\phi_a\phi_b^{-1}(x) = \phi_a(x) = x$, para todo $x \in E$, portanto pela Proposição 3.44 citada nesta demonstração, $Gal(K/E) \leq Gal(K/F)$. □

Definição 3.46. *(Corpo Fixo) Seja K um corpo e G um grupo de automorfismos deste corpo. K^G é o corpo fixo de G, ou seja, o conjunto dos elementos de K que são fixos pelos automorfismos de G.*

$$K^G := \{x \in K | \phi(x) = x, \forall \phi \in G\}$$

Lema 3.47. *Se K um corpo e G um grupo de seus automorfismos, K^G é um subcorpo de K.*

Demonstração. Seja K^G o corpo fixo de K como definido na Definição 3.46, ou seja $K^G \subset K$ e para todo $\phi \in G$, automorfismo de K, e $x \in K^G$ $\phi(x) = x$. Sejam $x, y \in K^G$, $\phi(0) = 0 \in K$.
$\phi(0) = \phi(x - x) = \phi(x) + \phi(-x) = x + \phi(-x) = 0$, isso nos afirma que todo elemento em K^G possui inverso aditivo dentro do conjunto, logo $-x \in K^G$.
$\phi(x - y) = \phi(x) + \phi(-y) = x - y$, segundo as últimas linhas desta mesma demonstração, logo é subgrupo aditivo de K, de acordo com a Propriedade 2.5.
Avaliemos agora ser um grupo multiplicativo. Como $\phi(1) = 1$, para qualquer automorfismo de K então $1 \in K^G$. Para todo elemento $x \in K^G/\{0\}$, existe $x^{-1} \in K$ tal que $x \cdot x^{-1} = 1, \phi(x^{-1}x) = (\phi(x^{-1})) * x = 1$, como o inverso é único, $\phi(x^{-1}) = x^{-1}$. Se $x, y \in K^G/\{0\}$ então $\phi(x \cdot y^{-1}) = \phi(x) \cdot \phi(y^{-1}) = xy^{-1}$, logo $K^G/\{0\}$ é um subgrupo multiplicativo de $K/\{0\}$, como visto na Propriedade 2.5. A comutatividade em ambas as operações derivam das propriedade do corpo K, assim como a distribuitividade. Portanto, pela Definição 2.45, K^G é subcorpo de K. □

Definição 3.48. *(Extensão de Galois) A extensão finita algébrica K/F será uma extensão de Galois se $K^{Gal(K/F)} = F$.*

Definição 3.49. *(Conjugado) Os elementos $x, y \in K$ são conjugados se existir o automorfismo $\phi : K \to K$ tal que $\phi(x) = y$ ou $\phi(y) = x$.*

Lema 3.50. *Seja $\phi \in Gal(K/F)$ e $\alpha \in K$, Se $\alpha \in K$ é raiz de um polinômio $f \in F[x]$ então a sua imagem $\phi(\alpha)$ também será raiz do mesmo polinômio.*

Demonstração. Seja $\alpha \in K$ e sua imagem $\phi(\alpha) \in K$, tais que $f(\alpha) = 0$. Com isso, $f(\alpha) = \alpha^n + a_{n-1} \cdot \alpha^{n-1} + \cdots + a_0 = 0$. Sabe-se, pela Definição 3.2.1 que $\phi(0) = 0$, logo $\phi(f(\alpha)) = 0$.

$$\phi(f(\alpha)) = \phi(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) = 0$$

Usando as propriedades de automorfismo dadas na Definição 3.2.1 e sabendo através da Definição 3.43, que ele deixa fixo os elementos de F,

$$\begin{aligned}
\phi(f(\alpha)) =& \phi(\alpha^n) + \phi(a_{n-1} \cdot \alpha^{n-1}) + \cdots + \phi(a_0) \\
\phi(f(\alpha)) =& \phi(\alpha^n) + \phi(a_{n-1} \cdot \alpha^{n-1}) + \cdots + \phi(a_0) \\
\phi(f(\alpha)) =& \phi(\alpha)^n + a_{n-1}\phi(\alpha)^{n-1} + \cdots + a_0 = f(\phi(\alpha)) = 0
\end{aligned}$$

A sentença acima nos diz que $\phi(\alpha)$, também é raiz de $f(x) \in F[x]$.

□

Corolário 3.51. *Seja $\alpha \in K$ e $Gal(K/F)$, grupo de Galois da extensão K/F. O polinômio mínimo de α e de seu conjugado são iguais.*

Demonstração. Se $m_\alpha(x)$, o polinômio mínimo de $\alpha \in F$, então $m_\alpha(\alpha) = m_\alpha(\phi(\alpha)) = 0$, de acordo com o Lema 3.50. Todo polinômio minimal é irredutível pelo Lema 3.20, logo pela definição de polinômio mínimo, $m_\alpha(x) = m_{\phi(\alpha)}(x)$, uma vez que o polinômio mínimo de $\phi(\alpha)$ divide todo polinômio em que este é raiz, pelo Lema 3.18. □

Definição 3.52. *Seja K/F uma extensão algébrica com $x \in K$. Então $\Theta_x := \{\sigma(x) | \sigma \in Gal(K/F)\}$ é o conjunto dos conjugados de $x \in K$.*

Lema 3.53. *Seja $x \in K$, $\Theta_x := \{\sigma(x) | \sigma \in Gal(K/F)\} \subset K$ e $H_x := \{\sigma \in Gal(K/F) | \sigma(x) = x\}$. O conjunto H_x é subgrupo de $Gal(K/F)$ e o número de conjugados de $x \in K$ é igual ao índice $[Gal(K/F) : H_x]$*

Demonstração. Nota-se que por hipótese , H_x é subconjunto de $Gal(K/F)$. Dado dois elementos de H_x, σ_1 e σ_2 o produto destes elementos (ou seja a composição), é um elemento de H_x , pois , $\sigma_2(\sigma_1(x)) = \sigma_2(x) = x$, já que $\sigma(x) = x$, para todo $\sigma \in H_x$. O automorfismo $id_K \in H_x$ pois $id_K(x) = x$. Todo elemento possui inverso em H , pois dado $\sigma \in H$, então $\sigma^{-1}(x) = x$ logo $\sigma^{-1} \in H_x$. Com isso concluímos que $H_x \leqslant Gal(K/F)$, pela definição de subgrupo (Definição

2.4) . Sabe-se pela Definição 3.52 que, $\Theta_x := \{\sigma(x)|\sigma \in Gal(K/F)\} \subset K$, o que equivale a órbita de $x \in K$, e o grupo H_x é o estabilizador deste elemento, de acordo com a definição de órbita e estabilizador (Definição 2.21). Agora basta aplicarmos o "Teorema da Órbita e Estabilizador"(Teorema 2.22), mostrando nos que,

$$[Gal(K/F) : H_x] = |\Theta_x|.$$

□

Proposição 3.54. *Se K/F é uma extensão algébrica, então as seguintes afirmações são equivalentes:*

(1) K/F é normal

(2) Seja $\bar{K}$ o fecho algébrico de K e $\phi : K \to \bar{K}$ um homomorfismo que fixa os elementos de F, então $\phi(K) = K$.

(3) Se $F \subseteq L \subseteq K \subseteq N$ são corpos e $\sigma : L \to N$ é um homomorfismo que fixa os elementos de F , então $\sigma(L) \subseteq K$, e existe um $\phi \in Gal(K/F)$ onde ϕ restrito a L é igual a esse automorfismo de $Gal(K/F)$.

(4)Para qualquer polinômio $f(x) \in F[x]$, se f tem uma raiz em K , então f se decompõe sobre K.

Demonstração. Veja a demonstração dessa proposição na página 36 de [2]. □

3.3 Teorema de Dirichlet

Definição 3.55. *(Caracter) Dizemos que δ é um "caracter"do grupo G para o corpo K, se $\delta : G \to K/\{0\}$, for um homomorfismo.*

Definição 3.56. *Seja G um grupo de automorfismos do corpo K. Um conjunto de caracter de G, $\{\delta_1, \cdots, \delta_n\}$, é linearmente dependente se existir elementos $\{a_1, \cdots, a_n\} \subset K$, nem todos nulos, tal que $(a_1\delta_1 + \cdots + a_n\delta_n)(\xi) = 0$, para todo $\xi \in G$.*

Teorema 3.57. *(Teorema de Dirichlet) Seja G, grupo de automorfismos de K. O conjunto $\Delta^G := \{\delta_1, \cdots, \delta_n\}$, de caracters mutuamente distintos de G é linearmente dependente.*

Demonstração. Demonstraremos por indução sobre n. Primeiramente vemos que é válido para $n = 1$, pela Definição 3.56, $a_1\delta_1 = 0$ implica $a_1 = 0$. Por hipótese de indução, suponha ser válido para um conjunto com menos de n *caracters*. Tomemos $\Delta^G := \{\delta_1, \cdots, \delta_n\}$ e suponha que $a_1\delta_1 + \cdots + a_n\delta_n = 0$, onde $a_i \in K/\{0\}$. Se $\delta_1 \neq \delta_n$ então existe $x \in G$ tal que $\delta_1(x) \neq \delta_n(x)$.

Suponha que para todo $\xi \in G$,

$$a_1\delta_1(\xi) + \cdots + a_n\delta_n(\xi) = 0.$$

Multiplicando $\delta_n(x)$ a essa última expressão, temos

$$\text{(i) } a_1\delta_1(\xi)\delta_n(x) + \cdots + a_n\delta_n(\xi)\delta_n(x) = 0.$$

por outro lado, pela Definição 2.23, para todo $\xi \in G$

$$a_1\delta_1(\xi x) + \cdots + a_n\delta_n(\xi x) = 0$$
$$(ii) a_1\delta_1(\xi)\delta_1(x) + \cdots + a_n\delta_n(\xi)\delta_n(x) = 0.$$

Subtraindo (i)-(ii) teremos,

$$a_1(\delta_1(x) - \delta_n(x))\delta_1(\xi) + \cdots + a_{n-1}(\delta_{n-1}(x) - \delta_n(x))\delta_{n-1}(\xi) = 0$$

Neste caso, todos os termos, $a_1(\delta_1(x) - \delta_n(x)) = 0$, são nulos. Mas, como $a_1 \neq 0$ temos que, $\delta_1(x) - \delta_n(x) = 0$, ou seja $\delta_1(x) = \delta_n(x)$. □

Teorema 3.58. *Seja $G := \{\delta_1, \cdots, \delta_n\}$ um grupo de automorfismos distintos do corpo K. Se $K^G = F$, ou seja F é o corpo fixo deste grupo, então $[K : F] = n$.*

Demonstração. Primeiramente mostramos que $n \leq [K : F]$. Suponhamos que $n = |G| > r$, tal que $\{b_1, \cdots, b_r\}$ é uma base para K/F. Consideremos o sistema de equações em K:

$$\begin{bmatrix} \delta_1(b_1) & \dots & \delta_n(b_1) \\ \vdots & \ddots & \vdots \\ \delta_1(b_r) & \dots & \delta_n(b_r) \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0.$$

Ou seja,

$$\sum_{i=1}^{n} \alpha_i \delta_i(b_k) = 0, \text{para todo } k = 1, \cdots, r.$$

Seja $x \in K$ pela Definição 3.1, $x = \sum_{k=1}^{r} y_k b_k$ com $y_k \in F$, tal que $F = K^G$, por hipótese do teorema. Com isso $\delta_i(y_k) = y_k$, onde $\delta_i \in G$ e todo $y_k \in F$. Usando esse fato temos

$$\begin{gathered} \sum_{i=1}^{n} \alpha_i \delta_i(x) = \\ \sum_{i=1}^{n} \alpha_i \delta_i(\sum_{k=1}^{r} y_k(b_k)) = \\ \sum_{i,k} \alpha_i y_k \delta_i(b_k) = \\ \sum_{k=1}^{r} y_k(\sum_{i=1}^{n} \alpha_i \delta_i(b_k)) = \sum_{k=1}^{r} y_k(0), \end{gathered}$$

ou seja

$$\sum_{i=1}^{n} \alpha_i \delta_i(b_k) = 0,$$

O que contradiz o Teorema 3.57, pois desta forma os automorfismos seriam linearmente dependentes. Isso nos garante que $[K : F] \geq n$.

Por outro lado, se G é um grupo, existe algum $\delta_i \in G$ que seja a identidade, por simplicidade usaremos que $\delta_1 = id_K$. Tomemos nossa base de K, $B_F^K = \{b_1, \cdots, b_r\}$, nos garantindo

$$\begin{bmatrix} \delta_1(b_1) & \dots & \delta_1(b_{n+1}) \\ \vdots & \ddots & \vdots \\ \delta_n(b_1) & \dots & \delta_n(b_{n+1}) \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_{n+1} \end{bmatrix} = 0.$$

Este novo sistema tem mais incógnitas do que equações, o que nos diz que tem pelo menos uma solução não trivial.

Seja o conjunto solução $\{\beta_1, \cdots, \beta_s, 0, \cdots, 0\}$ e suponha $s = 1$, então $\beta_1 \delta_1(b_1) = 0$ o que nos faz concluir que $\beta_1 = 0$, pois $\delta(b_1) = b_1 \neq 0$. Multiplicando as equações por β_s^{-1} temos

$\beta_s^{-1}(\beta_1\delta_1(b_1) + \cdots + \beta_s\delta_1(b_s)) = \beta_s^{-1}\beta_1 b_1 + \cdots + b_s = 0$, o que nos leva a dizer que $\{b_1, \cdots, b_n\}$, são linearmente dependentes.

Assumimos que β_1 não pertence a F então:

$$\beta_s^{-1}(\beta_1\delta_i(b_1) + \cdots + \beta_s\delta_i(b_s)) =$$
$$\beta_s^{-1}\beta_1\delta_i(b_1) + \cdots + \delta_i(b_s)) = 0$$

Para não sobrecarregar notações usaremos $\gamma_i = \beta_s^{-1}\beta_i$ para cada i, tendo como nova expressão

$$(i)\gamma_1\delta_i(b_1) + \cdots + \delta_i(b_s) = 0$$

Se γ_1 não esta em F, corpo fixo de G, então existe algum destes automorfismos, δ, em que $\delta(\gamma_1) \neq \gamma_1$. Como G se trata de um grupo, podemos falar que existe $\delta_k \in G$, tais que $\delta_i = \delta\delta_k$. Aplicando δ em nossa última expressão teremos

$$\delta(\gamma_1\delta_i(b_1) + \cdots + \gamma_{s-1}\delta_i(b_{s-1}) + \delta_i(b_s)) = 0$$
$$(ii)\delta(\gamma_1)\delta_i(b_1) + \cdots + \delta(\gamma_{s-1})\delta_i(b_{s-1}) + \delta_i(b_s)) = 0$$

Subtraindo (i)-(ii)

$$(\gamma_1 - \delta(\gamma_1))\delta_i(b_1) + \cdots + \delta(\gamma_{s-1})\delta_i(b_{s-1}) = 0$$

Se $\gamma_1 - \delta(\gamma_1) \neq 0$ e essa equação tem menos de de s coeficientes diferentes de zero, o que é um absurdo pois o conjunto $\{\delta_i(b_1), \cdots, \delta_i(b_{s-1})\}$ é linearmente independente pelo Teorema 3.57. Logo $[K : F] \leq n$.

Pela primeira parte $[K : F] \geq n$ e temos agora que $[K : F] \leq n$, portanto $[K : F] = n = |G|$. □

Corolário 3.59. *K/F é de Galois se e só se $[K : F] = |Gal(K/F)|$.*

Demonstração. Segundo a Definição 3.43 e a Definição 3.55, podemos olhar para $Gal(K/F)$ sendo um grupo de *"caracters"* de $G = K/\{0\}$ para K, pois G é um grupo abeliano multiplicativo, segundo a Definição 2.45 e a Definição 2.3.

Se K/F é de Galois, pela Definição 3.48 sabe-se que $K^{Gal(K/F)} = F$ e usando o Teorema 3.58 temos que $[K : F] = |Gal(K/F)|$. Por outro lado se $[K : F] = |Gal(K/F)|$ e $M =$

$K^{Gal(K/F)}$, então $Gal(K/F) = Gal(K/M)$ ainda pelo Teorema 3.58. Com isso, pelo Teorema 3.9 $|Gal(K/F)| = [K : M] \leq [K : F]$. Sendo por hipótese $[K : F] = |Gal(K/F)|$, então $[K : F] = [K : M]$, portanto $M = F = K^{Gal(K/F)}$, ou seja, K/F é de Galois, de acordo com a definição de uma extensão de Galois.

□

Corolário 3.60. *Seja $F(\alpha)/F$ uma extensão de Galois $\alpha \notin F$. Se $m_\alpha(x) \in F[x]$ é o polinômio mínimo deste algébrico, então $|Gal(F(\alpha)/F)| = deg(m_\alpha)$.*

Demonstração. O resultado segue-se do Teorema 3.24 e do Corolário 3.59. □

Exemplo 3.61. Veja o Exemplo 3.25 e o Exemplo 3.26.

3.4 Teorema Fundamental da Teoria de Galois

Teorema 3.62. *Seja K/F uma extensão algébrica finita, as seguintes afirmações são equivalentes:*

(1)K/F é uma extensão de Galois.

(2)K/F é normal e separável.

(3)K é corpo de decomposição de um conjunto de polinômios separáveis em $F[x]$.

Demonstração. $(1 \to 2)$: K/F é de Galois por hipótese, tomemos $\alpha \in K$. Seja $\{\alpha_i\}$ o conjunto de conjugados de α em K, com $\alpha_1 = \alpha$, pelo Corolário 3.51, $m_\alpha = m_{\alpha_i}$.

Tomado o polinômio $f = \prod_{i=1}^{n}(x - \alpha_i)$ polinômio que tem como raiz todos os α_i, e $\sigma \in Gal(K/F)$ então $\sigma(f) = f$, assim como visto no Lema 3.50. Com isso podemos dizer que $f \in F[x]$, pois seus coeficientes são fixos por qualquer automorfismo. Por definição m_α divide $f(x)$, pelo Lema 3.20 temos que suas raízes não são repetidas, ou seja , m_α é separável sobre F, de acordo com a Definição 3.37.

A Definição 3.34 nos diz que K/F é normal, pois é corpo de decomposição dos minimais m_{α_i}, assim se usamos a mesma ideia para qualquer algébrico desta extensão. Logo K/F é normal e separável.

$(2 \to 3)$: Sendo K/F normal, por hipótese, então pela Definição 3.37, K é corpo de decomposição do conjunto de polinômios $\{m_\alpha | \alpha \in K\}$. Os polinômios mínimos são separáveis, pois tem todas as suas raízes distintas 3.20. Se tomarmos o conjunto de polinômios $\{m_{\alpha_i} | \alpha_i \in K\}$, vemos que o mesmo procede, para cada um deles. Logo K é corpo de decomposição de um conjunto de polinômios separáveis sobre F.

$(3 \to 1)$: Seja K o corpo de decomposição de um polinômio separável em $F[x]$ e $n = [K : F]$ usaremos indução.

Se $[K : F] = 1$ então $K = F$ neste caso K/F é de Galois. Usaremos o seguinte fato como hipótese de indução. Dado certo $n \in \mathbb{N}$, suponhamos que para toda extensão em que $n > [K : F]$, K/F é de Galois. Seja $n > 1$ e $\alpha \in K$, uma das raízes do polinômio $f \in F[x]$, tal que α não pertence a F, e K é o corpo de decomposição deste polinômio. Por hipótese de indução $K/F(\alpha)$ é Galois, pois $f \in F(\alpha)[x]$ é separável, K é seu corpo de decomposição e o grau desta extensão é menor que n, pelo Teorema 3.9.

Por hipótese do item (3) deste teorema, α é separável. Sejam $\alpha = \alpha_1, \cdots, \alpha_r$ as raízes distintas do polinômio minimal de α, em F, $m_\alpha(x) \in F[x]$. Se $M = F(\alpha)$, o grau da extensão $[M : F] = deg(m_\alpha) = r$, pelo Corolário 3.24. Pelo Teorema 3.50, podemos assumir, $\phi_i \in Gal(K/F)$ em que, $\phi_i(\alpha) = \alpha_i$.

Os conjuntos $\phi_i Gal(K/M)$ são distintos, se $\phi_i^{-1}\phi_j \in Gal(K/M)$, então $\phi_i^{-1}\phi_j(\alpha) = \alpha$, por definição de $Gal(K/M)$.

Pelo Teorema de Lagrange (Teorema 2.16), $|Gal(K/F)| = |Gal(K/F) : Gal(K/M)| \cdot |Gal(K/M)| \geq r \cdot |Gal(K/M)|$. Como K/M é de Galois, $[K : F] = [K : M][M : F] = |Gal(K/M)| \cdot r$, pelo Teorema da Torre (Teorema 3.9). Sendo assim, $|Gal(K/F)| \geq [K : F]$. O outro lado da desigualdade se dá pelo Teorema 3.58, logo $|Gal(K/F)| = [K : F]$, onde pelo Corolário 3.59, nos diz que K/F é de Galois. □

Exemplo 3.63. Seja a extensão de corpos $\mathbb{Q}(i)/\mathbb{Q}$. Como $[\mathbb{Q}(i) : \mathbb{Q}] = deg(x^2 + 1)$, tal que, $x^2 + 1 \in \mathbb{Q}[x]$ é o polinômio minimo de $i \in \mathbb{Q}(i)$. Sabemos dos Corolários 3.59, que devido a igualdade acima, tal extensão é de Galois. Por definição de corpo de decomposição (Definição 3.27) podemos afirmar que $\mathbb{Q}(i)$ é o corpo de decomposição de $x^2 + 1 \in \mathbb{Q}[x]$ que é separável.

Corolário 3.64. *Seja K/F uma extensão de Galois. Se M é um corpo intermediário desta extensão então K/M é de Galois.*

Demonstração. Se K/F é de Galois, pelo Teorema 3.62 K é corpo de decomposição de $p(x) \in F[x]$. Como existe $p(x) \in F[x]$, podemos considerar o mesmo polinômio sobre M, corpo intermediário, logo K é corpo de decomposição de um conjunto de polinômios sobre M, pelo Teorema 3.62, K/M é de Galois.

□

Lema 3.65. *Seja K/F uma extensão de Galois e os conjuntos Ω e Λ definidos por*

$$\Omega := \{M | F \subset M \subset K\}$$
$$\Lambda := \{Gal(K/M) | F \subset M \subset K\}$$

e a aplicação entre esses conjuntos,

$$\xi : \Omega \to \Lambda$$
$$M \mapsto Gal(K/M),$$

então esta aplicação é bijetiva.

Demonstração. Seja $F \subset M \subset K$, uma torre onde M é corpo intermediário na extensão de Galois K/F. Pelo Corolário 3.64, K/M também é de Galois, onde pela Definição 3.48 $M = K^{Gal(K/M)}$.

Seja a aplicação

$$\xi : \Omega \to \Lambda$$
$$M \mapsto Gal(K/M).$$

onde Ω e Λ são definidos na hipótese deste lema.

Pela Definição 3.48, temos que $M = K^{Gal(K/M)} = K^{\xi(M)}$.

Tomemos dois corpos intermediários distintos, $F \subset M_1 \subseteq M_2 \subset K$, e suas respectivas imagens $\xi(M_1)$ e $\xi(M_2)$.

Se $\xi(M_1) = \xi(M_2)$ então $K^{\xi(M_1)} = K^{\xi(M_2)}$, por construção da aplicação $M_1 = K^{\xi(M_1)} = K^{\xi(M_2)} = M_2$, um absurdo pois $M_1 \neq M_2$, logo ξ é injetiva.

Para provar que tal função é bijetiva, basta mostrarmos que ela também é sobrejetiva. Tomemos um elemento qualquer $Gal(K/M') \in \Lambda$, e vamos mostrar que ele é imagem de M'. Sendo M' um corpo intermediário da extensão de Galois K/F, o Corolário 3.64 nos diz que K/M' também é de Galois, logo pela Definição 3.48, $K^{Gal(K/M')} = M'$. Portanto $\xi^{-1}Gal(K/M') = M'$, ou seja, todo elemento de Λ é imagem de algum elemento de Ω. Logo ξ é bijetiva. □

Teorema 3.66. *(Teorema Fundamental da Teoria de Galois) Seja K/F é uma extensão de Galois. Podemos concluir que:*

(i) existe uma bijeção entre o conjunto dos corpos intermediários da extensão K/F e os subgrupos de $Gal(K/F)$.

(ii) para todo $H \leqslant Gal(K/F)$, $|H| = [K : K^H]$ e $[Gal(K/F) : H] = [K^H : F]$

(iii)dada a torre $F \subseteq M' \subseteq M" \subseteq K$ temos por consequência $Gal(K/F) \geqslant Gal(K/M') \geqslant Gal(K/M")$.

Demonstração. (i) O Lema 3.65, nos diz válida tal afirmação para um certo subconjunto do conjunto dos subgrupos de $Gal(K/F)$, vamos mostrar todo subgrupo de $Gal(K/F)$ é imagem de um corpo intermediário de K/F, para a aplicação ξ dada no Lema 3.65.

Seja $H \leqslant Gal(K/F)$. O Lema 3.47, nos diz que existe $M \subset K$ tal que $K^H = M$. Tomemos $\sigma \in H$, por definição de H, $\sigma \in Gal(K/F)$, logo para todo $x \in F$, $\sigma(x) = x$, isso nos mostra que $M \supset F$.

O parádiagrama acima nos diz que $M = K^H$ é corpo intermediário de K/F, logo pelo Corolário 3.64, K/M é de Galois, ou seja, $M = K^{Gal(K/M)} = K^H$, portanto $H = Gal(K/M)$. Concluimos portanto que a aplicação que leva os corpos intermediários de K/M ao seus respectivos grupos de Galois é bijetiva, pois para toda K/M é de Galois (Corolário 3.64) e todo subgrupo de $Gal(K/F)$ tem uma extensão de Galois correspondente.

(ii)O item anterior, já demonstrado nos diz que se $H \leqslant Gal(K/F)$, então K/K^H é de Galois, com isso, pela Definição 3.48 e pelo Corolário 3.59 temos que $|H| = [K : K^H]$. O Teorema

2.16 diz nos que $[Gal(K/F) : H] = |Gal(K/F)|/|H|$, então

$$\begin{aligned}[Gal(K/F) : H] &= \frac{|Gal(K/F)|}{|H|} \\ &= \frac{[K : F]}{[K : K^H]} \\ &= \frac{[K : K^H][K^H : F]}{[K : K^H]}. \\ &= [K^H : F]\end{aligned}$$

(iii) Se temos a cadeia $F \subseteq M' \subseteq M'' \subseteq K$ onde K/F é de Galois, então pelo Corolário 3.64, K/M' e K/M" também são de Galois. Pelo Lema 3.45 temos que $Gal(K/F) \geqslant Gal(K/M') \geqslant Gal(K/M")$. O mesmo se da para as demais desigualdades.

□

Teorema 3.67. *Se K/F uma extensão de Galois e M um de seus corpos intermediários, tal que M/F seja normal, então $Gal(K/M) \triangleleft Gal(K/F)$.*

Demonstração. Provaremos que $Gal(K/M) \triangleleft Gal(K/F)$. Sabemos pelo Lema 3.45 que $Gal(K/M) \leqslant Gal(K/F)$, pois M é corpo intermediário. Seja $\sigma \in Gal(K/M)$ e $\phi \in Gal(K/F)$, basta mostrarmos que $\phi^{-1}\sigma\phi(x) \in M$, para todo $x \in M$.

Se $x \in M$, então podemos escrever x como elemento de um $F-$espaço vetorial, já que M/F é uma extensão. Com isso $x = \sum a_i\alpha_i$, onde cada α_i é um elemento da base de M/F, e $a_i \in F$. Logo, por definição de $\phi \in Gal(K/F)$, $\phi(x) = \sum a_i\phi(\alpha_i) \in M$, pois M/F é normal, cada $\phi(\alpha_i) \in M$, pelo Lema 3.50. Sendo $\sigma\phi(x) = \phi(x)$, pois $\phi(x) \in M$ o que nos diz que $\phi^{-1}\sigma\phi(x) = \phi^{-1}\phi(x) = x \in M$. O que conclui nossa demonstração. □

Corolário 3.68. *Seja K/F é uma extensão de Galois e M um corpo intermediário. Se a extensão M/F é de Galois, então*

$$Gal(M/F) \cong \frac{Gal(K/F)}{Gal(K/M)}.$$

Demonstração. Sendo satisfeitas as condições do Teorema anterior, podemos dizer que $Gal(K/M) \triangleleft Gal(K/F)$.

Vamos usar a seguinte relação, $\phi : Gal(K/F) \mapsto Gal(M/F)$, tal que se dado um $\sigma \in Gal(K/F) \cap Gal(M/F)$, então $\phi(\sigma) = \sigma$, caso contrário, $\phi(\sigma) = 0$. Esta relação é um homomorfismo, pois, dados $\sigma_1, \sigma_2 \in Gal(K/F)$, a imagem de seu produto ou é ela mesma ou é nula. Os elementos de $Gal(K/M)$, estão no núcleo, pois se $\sigma \in Gal(K/M)$, um automorfismo

diferente da identidade, então σ não pertence a $Gal(M/F)$, e com isso sua imagem é nula. Estas condições são suficientes para aplicarmos o Teorema do Isomorfismo 2.26, ou seja,

$$\frac{Gal(K/F)}{Gal(K/M)} \cong Gal(M/F).$$

□

Exemplo 3.69. Seja $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}$. Sabemos através da Demonstração 3.1.1, que a Base $B_{\mathbb{Q}}^{K} := \{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$, e através da Definição 3.48, por deixar fixo os elementos do corpo fixo, vemos que os automorfismos de $Gal(K/\mathbb{Q})$ agem diretamente sobre os elementos da base, já que segundo a Definição 3.1, todos elementos de K, podem ser escrito como uma combinação linear destes elementos. Sabemos também através do Lema 3.50 que a imagem de cada um dos elementos da base é raiz de seu polinômio mínimo. Desta forma os possíveis automorfismos do corpo são:

$$\begin{aligned} id :& 1 \to 1 \\ & \sqrt{3} \to \sqrt{3} \\ & \sqrt{5} \to \sqrt{5} \\ & \sqrt{15} \to \sqrt{15} \end{aligned}$$

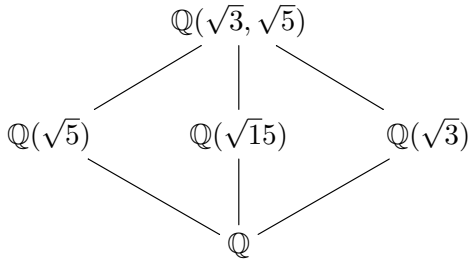
$$\begin{aligned} \phi :& 1 \to 1 \\ & \sqrt{3} \to \sqrt{3} \\ & \sqrt{5} \to -\sqrt{5} \\ & \sqrt{15} \to -\sqrt{15} \end{aligned}$$

$$\begin{aligned}\sigma :& 1 \to 1\\ & \sqrt{3} \to -\sqrt{3}\\ & \sqrt{5} \to \sqrt{5}\\ & \sqrt{15} \to -\sqrt{15}\end{aligned}$$

$$\begin{aligned}\omega : \phi :& 1 \to 1\\ & \sqrt{3} \to -\sqrt{3}\\ & \sqrt{5} \to -\sqrt{5}\\ & \sqrt{15} \to \sqrt{15}\end{aligned}$$

Notamos que, $\phi\sigma = \omega$. Com isso sabemos que estes são os únicos automorfismos de K pois $Gal(K/\mathbb{Q})$ é um grupo, de acordo com a Proposição 3.42. A ordem desse grupo portanto é 4, assim como o grau da extensão também é 4, como também poderia ser justificado pelo Corolário 3.59.

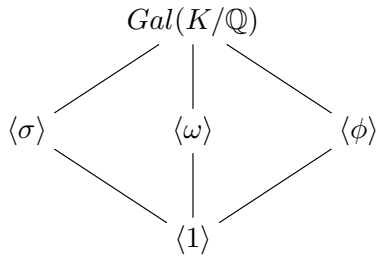
Exemplo 3.70. Analisemos a extensão do Exemplo 3.69, cujo o diagrama da extensão pode ser visto abaixo.



Ainda olhando para esta extensão vemos que $\mathbb{Q}(\sqrt{3}))$ é um corpo intermediário. A extensão $K/\ \mathbb{Q}\ (\sqrt{3}))$ tem como grupo de automorfismo $Gal(K/\ \mathbb{Q}\ (\sqrt{3}))$ tal que seus automorfismos são:

$$\begin{aligned}id :& 1 \to 1\\ & \sqrt{5} \to \sqrt{5}\\ \phi :& 1 \to 1\\ & \sqrt{5} \to -\sqrt{5}\end{aligned}$$

já que, são os automorfismos de K que deixam fixo os elementos de $\mathbb{Q}(\sqrt{3})$, pela definição de grupo de Galois. Um caso análogo seria a análise de $Gal(K/\mathbb{Q}(\sqrt{5}))$, onde ambos os grupos são isomorfos a $\mathbb{Z}_2$. Como a ordem do Grupo de Galois é igual a ordem do polinômio minimal do elemento primitivo da extensão, então esta extensão é Galoisiana, como visto no Corolário 3.59. Assim como é nos mostrado nos diagramas deste exemplo, vemos que pode se haver uma bijeção entre extensão, com seus corpos intermediários e subextensões com os seus respectivos grupos de Galois:



Exemplo 3.71. Vamos agora tomar uma extensão simples, genérica, e fazer o cálculo e uma breve análise em torno do Teorema Fundamental da Teoria de Galois.

(i) Seja K/F uma extensão de Galois, de grau n. O Corolário 3.59, nos diz que $[K : F] = |Gal(K/F)| = n$.

(ii) Se $\alpha \in K$ é um algébrico sobre F, temos a torre $K \supset F(\alpha) \supset F$. O Corolário 3.60 mostra nos que, $deg(m_\alpha) = p = [F(\alpha) : F] = |Gal(F(\alpha)/F)|$ e pelo Teorema Fundamental da Teoria de Galois $[F(a) : F] = [Gal(K/F) : Gal(K/F(\alpha))] = p$.

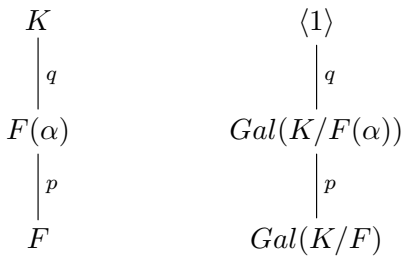
(iii)Aplicando o Teorema de Lagrange (Teorema 2.16) sobre essa expressão,

$$\begin{gathered}[Gal(K/F) : Gal(K/F(\alpha))] = p \\ \frac{|Gal(K/F)|}{|Gal(K/F(\alpha))|} = p \\ |Gal(K/F(\alpha))| = \frac{n}{p} = q.\end{gathered}$$

Da mesma forma, agora aplicando o Teorema da Torre (Teorema 3.9) e a Demonstração do Teorema 3.66, temos que,

$$[K : F(\alpha)] = \frac{[K : F]}{[F(\alpha) : F]} = \frac{|Gal(K/F)|}{|Gal(F(\alpha)/F)|} = \frac{n}{p} = q$$

(iv) Portanto, podemos usar como base o seguinte diagrama,



Capítulo 4

Solubilidade e Cálculo do Grupo de Galois de Polinômios

4.1 Extensões ciclotômicas

Definição 4.1. *(Raiz n-ézima) Chamamos $\omega \in K$ de $n-$ésima raiz $n-$ésima da unidade se $\omega^n = 1$, mas $\omega^m \neq 1$, para todo m tal que, $1 \leq m \leq n$. Se K é o corpo de decomposição do polinômio $x^n - 1 \in \mathbb{Q}[x]$, então as raízes deste polinômio são os elementos $\omega_i = e^{\frac{2\pi i}{n}}$*

Definição 4.2. *Seja F um corpo que contêm uma raiz primitiva $n-$ésima da unidade. Um corpo de Kummer é o corpo de decomposição de um polinômio da forma*

$$\prod_{i=1}^{r}(x^n - a_i)$$

para $a_i \in F$. Em relação a extensão podemos chamar K/F de uma extensão $n - Kummer$.

Lema 4.3. *Seja F um corpo que contenha a raiz $n-$ésima primitiva da unidade, e K/F uma extensão. Então K/F é uma extensão $n - Kummer$, se só se $K = F(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_r})$.*

Demonstração. Seja dada as condições de hipótese do nosso lema. Se K/F é uma extensão $n - Kummer$, então K é corpo de decomposição de $\prod_{i=1}^{r}(x^n - a_i)$, com isso $K = F(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_r})$, pois as raízes de cada polinômio $x^n - a_i$ são $\sqrt[n]{a_i}\omega_1, \cdots, \sqrt[n]{a_i}\omega_n$, onde ω_j, com $j \leq n$ são as raízes da unidade. Como as raízes da unidade já pertencem ao corpo F, por hipótese do lema, basta ser acrescido para cada termo $(x^n - a_i)$ sua raiz $\sqrt[n]{a_i}$. A outra direção se segue da Definição 4.2. □

Lema 4.4. *Seja F, corpo que contém as n raízes distintas da unidade, $\{\omega_1, \cdots, \omega_n\}$, e, para*

$(a_i \in F)$, seja

$$f = \prod_{i=1}^{r} (x^n - a_i) \in F[x].$$

Se K é o corpo de decomposição deste polinômio, então

(i) K/F é de Galois

(ii) $Gal(K/F)$ é abeliano

Demonstração. A demonstração deste Lema se encontra na página 130 do livro [1]. □

Definição 4.5. *(Extensões cíclicas) Uma Extensão de Galois é cíclica se seu grupo de Galois é um grupo cíclico*

Definição 4.6. *(Extensões ciclotômica) Se ω é raíz $n-$ézima da unidade de F, então a extensão $F(\omega)/F$ é chamada de extensão ciclotômica.*

4.2 Solubilidade

Definição 4.7. *(Grupo Solúvel) Dizemos que o grupo G é solúvel se existir uma cadeia de subgrupos G_j, $0 \leq j \leq n$, tais que $\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ e todo quociente G_{j+1}/G_j seja abeliano.*

Lema 4.8. *Seja G um grupo. Se G é solúvel e $H \leqslant G$, então H é solúvel.*

Demonstração. A prova deste Lema se encontra na página 204 do Livro [8].

□

Definição 4.9. *(Permutação) Seja um conjunto $X := \{x_1, \cdots, x_n\}$, onde $|X| = n$. Uma permutação dos elementos de X é um bijeção $\phi_i : X \to X$.*

Proposição 4.10. *(Grupo de permutações) O conjunto $S(X)$ de todas as possíveis permutações dos elementos de um conjunto X forma um grupo com a operação de composição. A este grupo chamamos de Grupo de permutações de X.*

Demonstração. Seja $S(X)$ o conjunto dado na hipótese. A função identidade de X, $id(x) = x$ pertence a esse conjunto, pois ela é uma bijeção, por definição de identidade. Se tomamos outra bijeção, $\phi \in S(X)$, onde $\phi(x_i) = x_j$, tais que $x_i, x_j \in X$.

(i)Compondo essas funções sabemos que, a identidade é o elemento neutro nesse conjunto em relação a composição de permutações, pois,

$$id(\phi(x_i)) = id(x_j) = x_j = \phi(x_i) = \phi(id(x_i)).$$

(ii)Pela Definição 4.9, toda permutação possui inversa, pois é uma bijeção.

(iii)E por fim, o produto de duas permutações é uma permutação, pois é uma bijeção, e a composição de bijeções é também uma função bijetora.

Com esses resultados vemos que $S(X)$ com a operação de composição satisfaz as condições de grupo, dadas na Definição 2.1 .

□

Definição 4.11. *(Grupo Simétrico) Chamamos de grupo simétrico o grupo de permutações $S(X)$, quando $X := \{1, 2, \cdots, n\}$. Neste caso $S(X) = S_n$, onde n é o número de elementos do conjunto X.*

Definição 4.12. *(Subgrupo Transitivo) Seja T um grupo de permutação de n elementos então T será transitivo se, para todo $i, j \leq n$ existe $\tau \in T$, tal que $\tau(i) = j$. Também podemos dizer que, para todo $i, j \leq n$ existem $\tau, \phi \in T$, onde $\tau(1) = j$ e $\phi(1) = i$, em que $\tau(\phi^{-1}(i)) = j$.*

Definição 4.13. *(Subgrupo Alternado) Uma transposição de X é um elemento $\tau \in S(X)$, tal que permuta dois e somente dois elementos. O subgrupo $A_n \leqslant S_n$ formado por todos os elementos que podem ser fatorados em um número par de transposições é chamado de subgrupo Alternado.*

Lema 4.14. *A_n não é solúvel para todo $n \geq 5$*

Demonstração. A demonstração deste fato pode ser encontrada em [4], página 148. □

Teorema 4.15. *S_n é solúvel se e somente se, $n < 5$.*

Demonstração. Usando a Definição 4.7 e o Lema 4.8, vemos que S_5 não é solúvel, pois se S_5 fosse solúvel, todos os seus subgrupos seriam solúveis, mas $A_5 \leqslant S_5$, não é solúvel segundo o Lema 4.14 o que é um absurdo.

Agora basta provar que S_4 é solúvel. Tomando a cadeia solúvel $S_4 \triangleright A_4 \triangleright K_4 \triangleright \langle id \rangle$, onde $K_4 = \{id, \phi, \gamma, \tau\}$, para as seguintes permutações pares:

$\phi : 1 \to 2$	$\gamma : 1 \to 3$	$\tau : 1 \to 4$
$2 \to 1$	$3 \to 1$	$4 \to 1$
$3 \to 4$	$2 \to 4$	$2 \to 3$
$4 \to 3$	$4 \to 2$	$3 \to 2$

e id é a identidade.

Pela Definição 2.3, vemos que K_4 é abeliano. Os quocientes S_4/A_4, A_4/K_4 são abelianos, pois são isomorfos a grupos cíclicos de ordem prima. □

Proposição 4.16. *O polinômio $f \in F[x]$ tem raízes repetidas em um corpo K, extensão de F, se só se, f e $\dfrac{df}{dx}$, tiver uma raíz em comum, se e só se $deg(mdc(f, \dfrac{df}{dx})) > 0$.*

Demonstração. Seja $f \in F[x]$ e $\alpha \in K$, uma raíz de f. Sendo K/F uma extensão, podemos escrever, $f = (x - \alpha)^k g(x) \in K[x]$, com $g(\alpha) \neq 0$.

$$\frac{df}{dx} = k(x - \alpha)^{k-1} g(x) + (x - \alpha)^k \frac{dx}{dx}.$$

Se f e $\dfrac{df}{dx}$ tem α, como raíz em comum, então o polinômio minimal de α, $m_\alpha \in F[x]$ divide ambos os polinômios, pelo Lema 3.18, e pela Definição 2.60, o minimal divide o $mdc(f, \dfrac{df}{dx})$.

Se o $deg(mdc(f, \dfrac{df}{dx})) > 0$ então existe o algébrico α que é raiz de $mdc(f, \dfrac{df}{dx})$. Como $mdc(f, \dfrac{df}{dx})$ divide f e $\dfrac{df}{dx}$, então α também é raiz de ambos os polinômios, pela Definição 2.59. □

Definição 4.17. *Seja o polinômio* $f(x) \in F[x]$*, tal que* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$*, então a derivada de* $f(x)$ *será o polinômio* $\dfrac{df}{dx} = n \cdot a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \in F[x]$.

Proposição 4.18. *Se* $f \in F[x]$ *é irredutível então* $f \in F[x]$ *é separável.*

Demonstração. Seja o algébrico α, raíz do polinômio irredutível $f(x) \in F[x]$, e o seu minimal $m_\alpha \in F[x]$. Pela Definição 2.58, $f = am_\alpha$, onde $a \in F$. Sabemos portanto que o polinômio $\dfrac{df}{dx} = a\dfrac{dm_\alpha}{dx}$ é não nulo, pois trabalhamos com corpos de cateterística zero. Se α for raiz desta derivada, teremos um absurdo pois $deg(m_\alpha) > deg(\dfrac{m_\alpha}{dx})$ e pela Definição 3.16. Logo $f \in F[x]$ é separável, pois todas as suas raízes são distintas.

□

4.2.1 Extensão radical

Definição 4.19. *(Extensão Radical)*
Dizemos que K/F é uma extensão radical se existir algébricos $\{\alpha_n, \alpha_{n-1}, \cdots, \alpha_1\}$ em K e $k_1, k_2, \cdots k_n$, naturais não nulos, tais que $\alpha_1^{k_1} \in F$, $\alpha_i^{k_i} \in F(\alpha_1, \alpha_2, \cdots, \alpha_{i-1})$ onde $1 < i \leq n$. Por conveniência podemos adotar um único inteiro k que satisfaça a relação, basta tomarmos $k = mmc(k_1, \cdots, k_n)$ neste caso chamamos a extensão de $k - Radical$ e $K = F(\alpha_n, \alpha_{n-1}, \cdots, \alpha_1)$.

Definição 4.20. *(Extensão Solúvel) Um extensão L/F é solúvel, ou solúvel por radicais, se existir uma extensão K/L, tal que K/F seja radical.*

Definição 4.21. *(Polinômio solúvel por radicais)*
O polinômio $f \in F[x]$ será solúvel por radicais se existir uma extensão radical L/F que contenha todas as raízes de f.

Lema 4.22. *Sejam as extensões K/E e E/F, radicais, então K/F é radical.*

Demonstração. Segundo a hipótese de nosso lema, E/F é radical, por definição, isso quer dizer que, sendo $E = F_m$, F_m/F é radical, e de acordo com a Definição 4.19, $F_i = F_{i-1}(\alpha_i)$ e $\alpha_i^{k_i} \in F_{i-1}$, para todo $i \leq m$.

Uma vez que $K/E = K/F_m$ (Definição 4.19), sendo $K = F_n$, onde $n \geq m$, $F_i = F_{i-1}(\alpha_i)$ e $\alpha_i^{k_i} \in F_{i-1}$, para $m \leq i \leq n$. Pela mesma definição é válido para todo $i \leq m$, $\alpha_i \in F_i = F(\alpha_1, \cdots, \alpha_m)(\alpha_{m+1}, \cdots, \alpha_{i-1})$. Usando o Lema 3.28, $\alpha_i \in F_i = F(\alpha_1, \cdots, \alpha_m, \alpha_{m+1}, \cdots, \alpha_{i-1})$, para todo i no intervalo de 1 a n. Logo K/F é radical. □

Definição 4.23. *(Grupo de Galois de um polinômio)*
Seja $f \in F[x]$, cujo o corpo de decomposição seja E. O grupo de Galois do polinômio $f(x)$ é $Gal(f) = Gal(E/F)$.

Proposição 4.24. *Se $f \in F[x]$ um polinômio separável, então $Gal(f)$ é isomorfo a um subgrupo do grupo de permutação das raízes de $f \in F[x]$. Se f for irredutível então $Gal(f)$ é isomorfo a um subgrupo transitivo.*

Demonstração. Seja $\alpha_1, \cdots, \alpha_d$ as raízes de $f \in F[x]$ em seu corpo de decomposição. Para todo automorfismo $\sigma \in Gal(f)$, $\sigma(\alpha_i)$ é uma raiz de $\sigma(f) = f$ (Lema 3.50). Além disto, se K é o corpo de decomposição de f, então $K = F(\alpha_1, \cdots, \alpha_d)$ (Definição 3.27), se $\sigma(\alpha_i) = \alpha_i$, para toda raiz α_i do polinômio f, $\sigma(x) = id(x)$, pois podemos escrever a base desta extensão em função destas raízes (demonstração do Teorema 3.9), e se o automorfismo deixa fixo todos os elementos da base logo ele preserva o elemento do corpo, pois os elementos de um corpo pode ser

escrito em função dos elementos da base (Definição 2.49). Caso f seja irredutível, pelo Teorema 3.39, podemos dizer que se trata de uma extensão simples, pois é corpo de decomposição de um polinômio separável (Teorema 3.62), ou seja, existe $\beta \in K$ tal que, $K = F(\beta)$. Neste caso, se um automorfismo fixa β então ele é a identidade, pois, os elementos da base desta extensão são potências de β, e como $\sigma(\beta) = \beta$, então $\sigma(\beta^i) = \sigma(\beta)^i = \beta^i$, portanto $\sigma = id_{Gal(f)}$. Se dado dois automorfismos $\sigma, \phi \in Gal(f)$, $\sigma(\beta) = \phi(\beta)$ então $\sigma = \phi$, pois $\phi^{-1}\sigma(\beta) = \beta$, logo $\phi^{-1}\sigma = id_{Gal(f)}$, uma vez que $Gal(f)$ é um grupo (Lema 3.45) e se dois elementos em um grupo tem o mesmo inverso, eles são iguais.

Neste caso, podemos usar o Corolário 3.60, cuja sua demonstração nos prova que se uma permutação fixa β então ela será a identidade, e pela mesma demonstração vemos que o grupo neste caso é isomorfo a um subgrupo transitivo (Definição 4.12) pois, $\phi \neq \sigma$ implica $\phi(\alpha) \neq \sigma(\alpha)$, onde $\phi, \sigma \in Gal(F(\beta)/F)$ e $\alpha \in F(\beta)/F$.

□

Definição 4.25. *(Fecho Galoisiano) Seja a extensão M/F, o fecho galoisiano desta extensão é o menor corpo K que contem M tal que K/F seja de Galois.*

Definição 4.26. *("Compositum") Sejam os subcorpos F_1 e F_2 de um corpo K, o Compositum F_1F_2, é o menor subcorpo de K que contem F_1 e F_2.*

Proposição 4.27. *Suponha que K/F seja de Galois e M seja um corpo intermediário, então o "Compositum"de todos os conjugados de M, ou seja, $\sigma_1(M)\cdots\sigma_r(M)$, onde para todo $i \leq r$, $\sigma_i \in Gal(K/F)$, é o fecho galoisiano da extensão M/F.*

Demonstração. Como M é separável, pelo Teorema 3.39, existe $\alpha \in M$, tal que $M/F = F(\alpha)/F$. Por hipótese, K/F é de Galois, logo o polinômio minimal de $\alpha \in M$, se decompõe completamente sobre K, pelo Teorema 3.62. Seja L o menor corpo que contem F e as raízes de m_α, então $L = F(\alpha_1, \cdots, \alpha_r)$. Ainda pelo Teorema 3.62, L/F é Galois e M é seu corpo intermediário, por construção, e podemos afirmar, que $\sigma_1(M), \cdots, \sigma_r(M)$ são corpos intermediários de L/F, pelo Lema 3.50, sabemos que cada σ_i permuta as raízes de m_α, logo $\sigma_1(M)\cdots\sigma_r(M) \subset L$, pela Definição 4.26.

Para toda raiz α_i de m_α, existe $\sigma_i \in Gal(m_\alpha)$, tal que $\sigma_i(\alpha) = \alpha_i$. Logo, $L = F(\sigma_1(\alpha), \cdots, \sigma_r(\alpha))$, como L é o menor corpo que contem todos as raízes de m_α, por construção de L, então $L \subset \sigma_1(M)\cdots\sigma_r(M)$. Por essas duas inclusões temos que $L = \sigma_1(M)\cdots\sigma_r(M)$, ou seja, $\sigma_1(M)\cdots\sigma_r(M)$ é o fecho galoisiano de M/F, pois $L = \sigma_1(M)\cdots\sigma_r(M)$.

□

Lema 4.28. *Seja a extensão K/F, e sejam M_1 e M_2, dois corpos intermediários desta extensão.*

(i) Se M_1/F é radical então M_1M_2/M_2 também é radical.

(ii) Se M_1/F e M_2/F são radicais então M_1M_2/F também é radical.

Demonstração. Se M_1/F é radical, por Definição 4.19,

$$M_1 = F(\alpha_1, \cdots, \alpha_r) \supset F(\alpha_1, \cdots, \alpha_{r-1}) \supset \cdots \supset F$$

onde cada $\alpha_i^{k_1} \in F(\alpha_1, \cdots, \alpha_{i-1})$, para $k_i \in \mathbb{N}$. Logo $M_1M2 = M_2(\alpha_1, \cdots, \alpha_r)$, pois $M_2 \supset F$ e $M_2F = M_2$. Basta tomar o *Compositum* de M_2 a cada um dos corpos da cadeia, com isso $M_1M_2 = M_2F(\alpha_1, \cdots, \alpha_r) \supset M_2F(\alpha_1, \cdots, \alpha_{r-1}) \supset \cdots \supset M_2F$. Com isso $\alpha_i^{k_1} \in M_2(\alpha_1, \cdots, \alpha_{i-1})$, pois $F(\alpha_1, \cdots, \alpha_{i-1}) \subset M_2(\alpha_1, \cdots, \alpha_{i-1})$, e $M_2F = M_2$, pois $M_2 \supset F$. Portanto, pela Definição 4.19, M_2M_1/M_2 é radical.

(ii) Se M_1/F e M_2/F, são radicais então M_1M_2/M_2 é radical pelo item (i) deste Lema e usando o Lema 4.22, por ser radical M_1M_2/M_2 e M_2/F, então M_1M_2/F também será. □

Lema 4.29. *Se L/F é radical então existe a torre $K \supset L \supset F$, tal que K/F seja normal e radical.*

Demonstração. Seja L/F radical e K o seu fecho galoisiano. Para cada $\sigma_i \in Gal(K/F)$, a extensão σ_iL/F é radical (Definição 4.19 e Lema 3.50), pois se $\alpha_i^n \in F(\alpha_{i-1})$ então $\sigma(\alpha_i)^n \in F(\sigma(\alpha_{i-1})) = \sigma L$. Pela Proposição 4.27, sabemos que K é igual ao *compositum* de todos os conjugados do corpo L, com isso e pelo Lema 4.28 temos que K/F é radical. Segundo o Teorema 3.62, toda extensão galoisiana é normal, o que conclui nossa demonstração. □

Definição 4.30. *(Polinômio solúvel) Seja $f \in F[x]$ um polinômio não constante cujo corpo de decomposição é L.*

(i) Uma raiz de f, $\alpha \in L$ será expressável por radicais F, se α esta em alguma extensão radical de F.

(ii) O polinômio f será solúvel por radicais (ou solúvel), se L/F for solúvel.

Proposição 4.31. *Seja $f \in F[x]$, irredutível. f será solúvel por radicais, se só se f tiver uma raiz expressável por radicais em F.*

Demonstração. Se f é solúvel, então pela Definição 4.30, L/F é solúvel, onde L é o corpo de decomposição de f. Pela definição de extensão solúvel (Definição 4.20) e pela definição de corpo de decomposição (Definição 3.27), as raízes de f estão em L.

Para a volta tomemos $\alpha \in L$, raiz de f, expressável por radicais. Pela Definição 4.30, existe a torre $M \supset F(\alpha) \supset F$, tal que M/F seja radical. Pelo Lema 4.29, existe $K \supset M \supset F(\alpha) \supset F$, tal que K/F seja normal e radical. Por definição de extensão normal (Definição 3.34),

por ser $f \in F[x]$ irredutível, todas as suas raízes estão contidas em K, logo, pela Definição 4.30, f é solúvel por radicais. □

Definição 4.32. *(Fecho normal) Se $K = F(\alpha_1, \cdots, \alpha_r)$, o fecho normal da extensão K/F é o corpo N tal que, N é corpo de decomposição dos polinômios minimais, $m_{\alpha_1}, \cdots, m_{\alpha_r} \in F[x]$.*

Lema 4.33. *Se K/F é uma extensão $n-$radical e N seu fecho normal então N/F será uma extensão $n-$radical.*

Demonstração. Seja $K = F(\alpha_1, \cdots, \alpha_r)$ com $\alpha_i^n \in F(\alpha_1, \cdots, \alpha_r)$. Se $r = 1$, então $K/F = F(\alpha_1)/F$ com $\alpha^n \in F$, neste caso $N = F(\beta_1, \cdots, \beta_m)$, onde β_i são raízes de $m_\alpha(x) \in F[x]$, pela Definição 4.32. Contudo, este minimal divide $x^n - a$, tal que $a = \alpha^n$, o que nos leva a dizer que $a = \beta_i^n$, pois o minimal divide todo polinômio em que α é raiz, como descrito no Lema 3.18. Com isso, N/F é $n-$radical. Agora suponhamos que $r > 1$, e para valores menor que r, N/F seja $n-$radical. Seja N'/F uma extensão $n-$radical, com N' o corpo de decomposição dos minimais $m_{\alpha_1}, \cdots, m_{\alpha_{r-1}} \in F[x]$. Seja N corpo de decomposição do polinômio $m_{\alpha_i} \in F[x]$, para todo $i \leq r$, com isso $N = N'(\gamma_1, \cdots, \gamma_m)$, onde $\gamma_1 \cdots, \gamma_m$ são as raízes de m_{α_r}. Como $\alpha_r^n = b \in F(\alpha_1, \cdots, \alpha_{r-1}) \subseteq N'$ □

Proposição 4.34. *Seja K/F uma extensão de Galois, e $E_1 = F^{G_1}$ e $E_2 = F^{G_2}$ são corpos intermediários desta extensão. Logo segue-se que:*

(i) $E_1E_2 = F^{G_1 \cap G_2}$

(ii)$E_1 \cap E_2 = F^{G_1G_2}$

Demonstração. (i) Se $\sigma \in G_1 \cap G_2$, então $\sigma \in G_1$ e com isso σ fixa os elementos de E_1 de mesma forma σ fixa os elementos de E_2, com isso σ fixa os elementos de E_1E_2 (pela Definição 4.26). Por outro lado se σ fixa os elementos de E_1E_2, ele fixa os elementos de qualquer um de seus subcorpos, logo $\sigma \in G_1$, grupo que fixa os elementos de E_1 e $\sigma \in G_2$, grupo que fixa os elementos de E_2 ou seja $\sigma \in G_1 \cap G_2$. Portanto $F^{G_1 \cap G_2} = E_1E_2$.

(ii) Se para todo $\sigma \in G_1$, $\sigma(\alpha) = \alpha$, então $\alpha \in E_1$ e se para todo $\sigma \in G_2$, $\sigma(\alpha) = \alpha$ então $\alpha \in E_2$ com isso $\alpha \in E_1 \cap E_2$. Ou seja $F^{G_1G_2} \supset E_1 \cap E_2$. Por outro lado, se $\alpha \in E_1 \cap E_2$, então $\sigma(\alpha) = \alpha$ para todo $\sigma \in G_1$ e para todo $\sigma \in G_2$, com isso $\alpha = \sigma(\alpha)$ para todo $\sigma \in G_1G_2$. Ou seja $F^{G_1G_2} = E_1 \cap E_2$. □

Lema 4.35. *Seja $f \in F[x]$ um polinômio separável, K seu corpo de decomposição e L/F uma extensão arbitrária.*

(i) LK é corpo de decomposição de $f \in L[x]$

(ii) $Gal(LK/L) \cong Gal(K/L \cap K)$

Demonstração. O primeiro item (i) segue pela Definição 3.27 e pela Definição 4.26, já que LK é o menor corpo que contém todas as raízes de $f \in F[x]$, que é extensão de L.

Para (ii) sabemos que KL/L é Galois, pois é corpo de decomposição de um polinômio separável, assim como a extensão $K/K\cap L$, já que $f \in (K\cap L)[x]$ tem como corpo de decomposição K, pelo item anterior deste lema. Como $Gal(K/L\cap K) \cong Gal(LK/L\cap K)$, pelo Corolário 3.68.

Seja M o fecho normal de $KL/K\cap L$ (Definição 4.32), por consequência será de Galois, pois aqui tratamos de extensões separáveis (Teorema 3.62). A torre $M \supset KL \supset L$ nos diz que M/KL, M/L e KL/L são de Galois, pelo Corolário 3.64 e pelo item anterior, já que KL é corpo de decomposição de polinômios separáveis (Teorema 3.62). Para a Torre $M \supset K \supset (K\cap L)$ vemos que as extensões $M/(K\cap L)$, M/K e $K/(K\cap L)$ são de Galois. Usando o Corolário 3.68, vemos que

$$Gal(KL/L) \cong \frac{Gal(M/L)}{Gal(M/KL)}$$

e

$$Gal(K/K\cap L) \cong \frac{Gal(M/(K\cap L)}{Gal(M/K)}$$

.

Vemos que $Gal(M/L)\cap Gal(M/K) \cong Gal(M/KL)$ pois $\phi \in Gal(M/KL)$, fixa os elementos de $L \subset KL$, logo $\phi \in Gal(M/L)$, de forma análoga, $\phi \in Gal(M/K)$, portanto $\phi \in Gal(M/L)\cap Gal(M/K)$. Por outro lado, se $\sigma \in Gal(M/L)\cap Gal(M/K)$, então σ fixa os elementos de L e K, por consequência fixa os elementos do menor corpo que contêm K e L, portanto $\sigma \in Gal(M/KL)$. Também temos que $Gal(M/L)Gal(M/K) \cong Gal(M/K\cap L)$, através da Proposição 4.34.

O Teorema 2.28, nos diz que

$$\frac{Gal(M/L)}{Gal(M/L)\cap Gal(M/K)} \cong \frac{Gal(M/L)Gal(M/K)}{Gal(M/K)},$$

logo

$$\frac{Gal(M/L)}{Gal(M/KL)} \cong \frac{Gal(M/K\cap L)}{Gal(M/K)}.$$

Aplicando novamente o Corolário 3.68 em ambos os lados temos que, $Gal(KL/L) \cong Gal(K/K\cap L)$.

□

Teorema 4.36. *O polinômio $f \in F[x]$ é solúvel por radicais se somente se $Gal(f)$ é um grupo solúvel.*

Demonstração. Se $f \in F[x]$ é solúvel por radicais, de acordo com a Definição 4.30, suas raízes estão contidas em uma extensão radical. Pelo Lema 3.35 , podemos afirmar que o corpo de decomposição de $f \in F[x]$ esta contido em uma extensão normal e radical K/F. O Teorema 3.62

nos diz que K/F é de Galois, pois é normal e separável. Pelo Teorema 3.67, podemos assumir que $Gal(K/M) \triangleleft Gal(K/F)$, e pelo Colorário 3.68, $Gal(M/F) \cong Gal(K/F)/Gal(K/M)$, onde M é o corpo de decomposição de $f \in F[x]$. Dividiremos em dois casos, o primeiro em que M contém a raiz $n-$ésima da unidade ω , e o segundo caso é em que M não contém, tal raiz.

Tomemos a cadeia de corpos intermediários, da extensão K/F,

$$F = K_0 \subset K_1 \subset \cdots \subset K_n = K,$$

onde $K_1 = F(\omega)$, tal que ω é a raiz $n-$ézima da unidade, como dado na Definição 4.1 e a na demonstração do Lema 4.29. Seja $K_{i+1} = K_i(\alpha_i)$, onde $\alpha_i \in K$. Neste caso cada extensão K_{i+1}/K_i é de Galois, pois K/K_i é de Galois pelo Corolário 3.64 e $Gal(K_{i+1}/K_i) \triangleleft Gal(K_{i+1}/F)$. Pelo Lema 4.4, cada $Gal(K_{i+1}/K_i) \cong Gal(K_i/F)/Gal(K_{i+1}/F)$ é abeliano, logo $Gal(K/F)$ é solúvel, pela Definição 4.7.

Uma segunda possibilidade é supor que a extensão radical dada não tenha a raíz $n-$ézima da unidade. Neste caso, pela Definição 4.21, suas raízes estão contidas em uma extensão $n-$radical M/F. Seja $\omega \in M(\omega)$ uma raíz $n-$ézima da unidade, pela Definição 4.19 $M(\omega)/M$ é $n-$radical, assim como $F(\omega)/F$ também é, logo pelo Lema 4.28, $M(\omega)/F$ é $n-$radical, já que $M(\omega) = MF(\omega)$. Apartir daqui basta considerar a extensão $M(\omega)/F$ e usar o mesmo argumento do último parádiagrama.

Por outro lado, se $Gal(K/F)$ é solúvel, onde K é o corpo de decomposição de $f \in F[x]$, por definição de solubilidade de grupos (Definição 4.7), existe a seguinte cadeia normal de subgrupo,

$$Gal(K/F) = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 = \langle 1 \rangle$$

tais que os quocientes G_{i+1}/G_i são abelianos, para todo $i < n$. Seja $K_i = K^{G_i}$, pela Definição 3.48, K/K_i é Galois para todo $i \leq n$ e com isso, pelo Corolário 3.64, K_{i+1}/K_i também é uma extensão de Galois.

Pelo Corolário 3.68 $Gal(K_{i+1}/K_i) \cong Gal(K_i/F)/Gal(K_{i+1}/F) = G_i/G_{i+1}$.

Seja $|Gal(K/F)| = r$, e ω seja a raiz primitiva $r-$ésima da unidade. Se tomamos os corpos $L_i = K_i(\omega)$, podemos considerar a seguinte torre de corpos

$$F \subseteq L_0 \subseteq \cdots \subseteq L_n.$$

Notemos que $K \subset L_r$, e $L_{i+1} = L_i K_{i+1}$. Com isso e pelo Lema 4.35, como K_{i+1}/K_i é Galois L_{i+1}/L_i é Galois e $Gal(L_{i+1}/L_i)$ é abeliano, pois é isomorfo a G_{i+1}/G_i.

L_{i+1}/L_i é uma $n - Kummer$ pelo Lema 4.3 e pela Definição 4.19, L_{i+1}/L_i é $n-$ radical.

Seja $L_0 = F(\omega)$ em nossa cadeia, $F(\omega)/F$ é radical, pela Definição 4.19, L_1/F é radical pelo Lema 4.28, com esse argumento podemos afirmar que L_r/F é radical. Como o corpo de

decomposição de $f \in F[x]$, é um corpo intermediário na extensão L_r/F, o polinômio $f \in F[x]$ é solúvel (Definição 4.21), o que encerra nossa demonstração. $\square$

4.3 Calculando Grupos: Quadráticas, Cúbicas e Quárticas

4.3.1 Discriminante

Definição 4.37. *(Discriminante de um polinômio) Seja $f \in F[x]$ um polinômio cuja as raízes são $\alpha_1, ...\alpha_n \in K$. A discriminante de f é $\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2$.*

Definição 4.38. *(Discriminante de um elemento) Seja $\alpha \in F$, cujo o polinômio minimo é $m_\alpha \in F[x]$. A discriminante de α é igual a discriminante de seu polinômio mínimo.*

Lema 4.39. *Seja $f \in F[x]$, um polinômio irredutível com n raízes, cujo discriminante é Δ, e seja $\sigma \in Gal(f) \cong G \leqslant S_n$. O automorfismo σ é uma permutação par, se só se, $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$*

Demonstração. Tomemos $f \in F[x]$ onde, $deg(f) = n$, seja $M = F(x_1, ..., x_n)$, onde $\{x_1, ...x_n\}$ é o conjunto das raízes de f. Seja $h(x) = \prod_{i<j}(x_i - x_j)$. Suponha que $\sigma \in S_n$ é uma transposição ou seja, $\sigma(x_i) = x_j$,e $\sigma(x_j) = x_i$ onde $i < j$. Analisemos o comportamento desse automorfismo, separando os fatores de $h(x)$ em quatro grupos:

$$\begin{aligned} x_i - x_j & \\ x_k - x_i, x_k - x_j & \qquad k < j \\ x_i - x_l, x_j - x_l & \qquad j < l \\ x_i - x_m, x_m - x_j & \qquad i < m < j \end{aligned}$$

.

Para $k < i$, temos o automorfismo $\sigma(x_k - x_i) = x_k - x_j$ e $\sigma(x_k - x_i) = x_k - x_j$. Para $j < l$ teremos,$\sigma(x_i - x_l) = x_j - x_l$. Já para $i < m < j$, o que temos é

$$\begin{aligned} \sigma(x_i - x_m) &= x_j - x_m = -(x_m - x_j) \\ \sigma(x_m - x_j) &= \alpha_m - \alpha_i = -(x_i - x_m) \end{aligned}$$

.

Somando as expressões, utilizando as propriedades de automorfismo, concluiremos que $\sigma(x_i - x_j) = x_j - x_i = -(x_i - x_j)$. Com esses resultados , podemos dizer que o automorfismo de todos termos de h nos leva $\sigma(h) = h$ se e somente se σ é produto de um numero par de permutações. Se aplicarmos em h as raízes de f teremos $h = \prod_{i<j}(\alpha_i - \alpha_j) = \prod_{i<j}(-(\alpha_j - \alpha_i)) = \Delta$, o que conclui o nosso lema, pois $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$, se só se σ for par. □

Corolário 4.40. *Seja $f \in F[x]$, um polinômio irredutível com n raízes, cujo discriminante é Δ, e seja $\sigma \in Gal(f) \cong G \leqslant S_n$.*

$Gal(f) \cong G \leqslant A_n$ se só se $\sqrt{\Delta} \in F$.

Demonstração. Sejam $f \in F[x]$ e $\sigma \in Gal(f)$. Se $\sqrt{\Delta} \in F$, então $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$ (Definição 3.48), pois $\sigma \in Gal(f)$, portanto σ é uma permutação par segundo o Lema 4.39. Se $Gal(f) \cong G \leqslant A_n$ então σ é par, por definição de A_n, e pelo Lema 4.39, $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$, ou seja $\sqrt{\Delta} \in K^{Gal(f)}$, onde K é o corpo de decomposição de $f \in F[x]$. A extensão K/F é de Galois, pois K é o corpo de decomposição de um polinômio separável (Teorema 3.62), logo $K^{Gal(f)} = F$, por definição de extensão de Galois (Definição 3.48). Portanto $\sqrt{\Delta} \in F$. □

4.3.2 Polinômios de grau 2

Proposição 4.41. *Se $f \in F[x]$ irredutível de grau 2, então $Gal(f) \cong G \leqslant S_2$.*

Lema 4.42. *A discriminante de um polinômio de grau 2, $f = x^2 + bx + c \in F[x]$ é $\Delta_f = b^2 - 4c$*

Demonstração. Através da fórmula resolvente de um polinômio de segundo grau, sabemos que suas raízes são $\alpha_1 = \dfrac{-b + \sqrt{b^2 - 4c}}{2}$ e $\alpha_2 = \dfrac{-b - \sqrt{b^2 - 4c}}{2}$. Por definição de discriminante de um polinômio (Definição 4.37) temos que $\Delta_f = (\alpha_1 - \alpha_2)^2$. Fazendo as substituições temos que $\Delta_f = (\sqrt{b^2 - 4c})^2 = b^2 - 4c$. □

Exemplo 4.43. Seja o polinômio irredutível $f(x) = x^2 + bx + c \in F[x]$. Pela fórmula quadrática, as soluções desse polinômio são $\dfrac{b + \sqrt{\Delta(f)}}{2}$ e $\dfrac{b - \sqrt{\Delta(f)}}{2}$. O corpo de decomposição de $f \in F[x]$ é $F(\dfrac{b + \sqrt{\Delta(f)}}{2}, \dfrac{b - \sqrt{\Delta(f)}}{2}) = F(\dfrac{b + \sqrt{\Delta(f)}}{2})(\dfrac{b - \sqrt{\Delta(f)}}{2})$.

$F(\dfrac{b + \sqrt{\Delta(f)}}{2}) \supset F(\sqrt{\Delta(f)})$ e $F(\dfrac{b + \sqrt{\Delta(f)}}{2}) \subset F(\sqrt{\Delta(f)})$, pois $b \in F$, portanto $F(\dfrac{b + \sqrt{\Delta(f)}}{2}) = F(\sqrt{\Delta(f)})$. De forma análoga $F(\dfrac{b - \sqrt{\Delta(f)}}{2}) = F(-\sqrt{\Delta(f)})$. Como $-1 \in F$, podemos dizer que $F(-\sqrt{\Delta(f)}) = F(\sqrt{\Delta(f)})$. Portanto o corpo de decomposição de um polinômio de grau 2 escrito em $F[x]$ será $F(\sqrt{\Delta(f)})$.

Pelo Teorema do Elemento primitivo sabemos que o corpo de decomposição de $f \in F[x]$ é $F(\alpha)$ onde α é uma das raízes de f. Como f é irredutível, então f é o polinômio mínimo de α, pelo Lema 3.20. Como f tem grau 2, $[F(\alpha) : F] \leq 2!$ pelo Teorema 3.24. Portanto $Gal(f) \cong G \leqslant S_2$, pois $[F(\alpha) : F] = |Gal(f)|$, segundo o Corolário 3.59. Nesta situação temos o seguinte diagrama

$$\begin{array}{ccc} F(\sqrt{\Delta(f)}) & & \langle 1 \rangle \\ {\scriptstyle 2}\big| & & \big|{\scriptstyle 2} \\ F & & Gal(f) \end{array}$$

4.3.3 Polinômios de grau 3

Lema 4.44. *(Fórmula de Cardano) As raízes de uma cúbica $f = x^3 + px + q$ são*

$$\alpha_1 = \sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 + \frac{4p^3}{27}})} + \sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 - \frac{4p^3}{27}})}$$

$$\alpha_2 = \omega\sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 + \frac{4p^3}{27}})} + \omega^2\sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 - \frac{4p^3}{27}})}$$

$$\alpha_3 = \omega^2\sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 + \frac{4p^3}{27}})} + \omega\sqrt[3]{\frac{1}{2}(-q + \sqrt{q^2 - \frac{4p^3}{27}})}$$

onde $\omega = \dfrac{-1 + i\sqrt{3}}{2}$.

Demonstração. A prova deste lema se encontra na página 3 do livro [7]. □

Lema 4.45. *Seja $f = x^3 + bx^2 + cx + d \in F[x]$, um polinômio irredutível. Podemos reescrever o polinômio $f(x) \in F[x]$ como $f(y) = y^3 + py + q \in F[y]$.*

Demonstração. Faremos a seguinte mudança de variável $x = y - \dfrac{b}{3}$. Vejamos:

$$\begin{aligned} f(x) =& x^3 + bx^2 + cx + d \\ f(y - \frac{b}{3}) =& (y - \frac{b}{3})^3 + b(y - \frac{b}{3})^2 + c(y - \frac{b}{3}) + d = 0 \end{aligned}$$

Pelo teorema da expansão binomial temos que

$$\begin{aligned} (y - \frac{b}{3})^2 =& y^2 - 2y\frac{b}{3} + (\frac{b}{3})^2 = y^2 - \frac{2b}{3}y + \frac{b^2}{9} \\ (y - \frac{b}{3})^3 =& y^3 - 3y^2\frac{b}{3} + 3y(\frac{b}{3})^2 - (\frac{b}{3})^3 = y^3 - by^2 + \frac{b^2}{3}y - \frac{b^3}{27} \end{aligned}$$

assim

$$\begin{aligned} f(x) &= x^3 + bx^2 + cx + d \\ f(y) &= (y^3 - by^2 + \frac{b^2}{3}y - \frac{b^3}{27}) + b(y^2 - \frac{2b}{3}y + \frac{b^2}{9}) + c(y - \frac{b}{3}) + d \\ f(y) &= y^3 + (-b + b)y^2 + (\frac{b^2}{3} - \frac{2b^2}{3} + c)y - \frac{b^3}{27} + \frac{3b^3}{27} + \frac{bc}{3} + d \\ f(y) &= y^3 + py + q \end{aligned}$$

dessa forma,

$$\begin{aligned} p =& -\frac{b^2}{3} + c \\ q =& \frac{2b^2}{27} - \frac{bc}{3} + d \end{aligned}$$

□

Proposição 4.46. *Sejam $f(x)$ e $f(y)$, polinômios irredutiveis dados no Lema 4.45.* $\Delta_{f(x)} = \Delta_{f(y)}$.

Olhando a demonstração do Lema 4.45, vemos que se α_i é raíz de $f(x)$ então $\beta_i = \alpha_i + \frac{b}{3}$, para $i \in \{1,2,3\}$, pois $x = y - \frac{b}{3}$, neste caso $(\alpha_i - \alpha_i) = ((\alpha_i + \frac{b}{3}) - (\alpha_j + \frac{b}{3})) = (\beta_i - \beta_j)$, para qualquer par $(i,j) \in \{1,2,3\}$. Como a diferença das raízes se conserva com tal mudança de variável, e a discriminante é calculada com produto das diferenças, então $\Delta_{f(x)} = \Delta_{f(y)}$.

Lema 4.47. *Seja $f(x) \in F[x]$ um polinômio irredutível de grau 3. Se $f(y) \in F[x]$ é o polinômio estabelecido pela troca de variável dada no Lema 4.45, então $\Delta_{f(y)} = -4p^3 - 27q^2$.*

Demonstração. Sendo as raízes de $f(y)$ os algébricos y_1, y_2, y_3 , como $f \in F[x]$ é irredutível, logo separável(Proposição 4.18) ,pela Definição 3.37 podemos assumir que

$$\begin{aligned} y^3 + py + q &= (y - y_1)(y - y_2)(y - y_3) \\ &= y^3 + (y_1 + y_2 + y_3)y^2 + (y_1y_2 + y_1y_3 + y_2y_3)y - y_1y_2y_3, \end{aligned}$$

desta forma

$$\begin{aligned} 0 &= y_1 + y_2 + y_3 \\ p &= y_1y_2 + y_1y_3 + y_2y_3 \\ q &= y_1y_2y_3, \end{aligned}$$

Pela Definição 4.37, o discriminante de $f(y)$ é $\Delta_{f(y)} = (y_1 - y_2)^2(y_1 - y_3)^2(y_2 - y_3)^2$, fazendo as substituições cabíveis, apartir das expressões dadas acima, encontramos que $\Delta_{f(y)} = -4p^3 - 27q^2$. □

Teorema 4.48. *Se $f \in F[x]$ é cubico e irredutível então seu corpo de decomposição $F(y_1, y_2, y_3) = F(\sqrt{\Delta}, y_1)$, onde Δ é seu discriminante.*

Demonstração. Por definição $\Delta = (y_1 - y_2)^2(y_1 - y_3)^2(y_2 - y_3)^2$, logo $\sqrt{\Delta} = (y_1 - y_2)(y_1 - y_3)(y_2 - y_3)$, o que justifica $\sqrt{\Delta} \in F(y_1, y_2, y_3)$, uma expressão das raízes. Por outro lado, dada a função $f(y) = y^3 + py + q = (y - y_1)(y - y_2)(y - y_3)$, como $y_1 \in F(\sqrt{\Delta}, y_1)$ o fator $(y - y_1)$ divide f logo $f = (y - y_1)g$, onde $g = (y - y_2)(y - y_3) = y^2 - (y_3 + y_2)y + y_2y_3$ tem seus coeficientes em $F(\sqrt{\Delta}, y_1)$, ou seja, $(y_3 + y_2) \in F(\sqrt{\Delta}, y_1)$. O polinômio quociente, $g(y_1)$, pertence ao corpo $F(\sqrt{\Delta}, y_1)$, o que nos leva a:

$$g(y_1) = (y_1 - y_2)(y_1 - y_3) \in F(\sqrt{\Delta}, y_1).$$

Como $g(y_1), \sqrt{\Delta} \in F(\sqrt{\Delta}, y_1)$, que é um corpo, podemos fazer a seguinte divisão. Usando a definição da discriminante teremos:

$$\frac{\sqrt{\Delta}}{g(y_1)} = \frac{\sqrt{\Delta}}{(y_1 - y_2)(y_1 - y_3)} = y_2 - y_3.$$

Agora temos que $(y_2 + y_3), (y_2 - y_3) \in F(\sqrt{\Delta}, y_1)$. Somando e subtraindo esses elementos chegamos que $y_2, y_3 \in F(\sqrt{\Delta}, y_1)$.

Isto é suficiente para dizer que $F(\sqrt{\Delta}, y_1) = F(y_1, y_2, y_3)$ □

Corolário 4.49. *Seja $f \in F[x]$ irredutível onde $deg(f) = 3$. Se $\sqrt{\Delta} \in \mathbb{Q}$,então $Gal(f) \cong A_3$, caso contrário $Gal(f) \cong S_3$.*

Demonstração. Sabemos que para um polinômio $f \in F[x]$ de grau 3, $Gal(f) \cong G \leqslant S_3$ (Teorema 4.24). Sabemos que para todo $\sigma \in Gal(f), \sigma$ preserva os elementos de F, ou seja $\sigma(q) = q$, para todo $q \in F$. Ora se a raiz da discriminante, $\sqrt{\Delta}$, pertence a F, então $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$ (Lema 4.39) e sabemos que quando isso ocorre, $\sigma \in A_3$ (Corolário 4.40). $Gal(f) \neq \langle 1 \rangle$, pois existe alguma isomorfismo σ, em que $\sigma(\alpha_1) = -\alpha_1$, para alguma α_1 que não pertence a F. Logo $Gal(f) \cong A_3$, pois é o único subgrupo não trivial de S_3, que só contem permutações pares. Caso $\sqrt{\Delta}$ não pertença a F, existe $\sigma \in Gal(f)$ tal que σ é impar , e $\sigma(\Delta) = -\Delta$, assim como visto no mesmo Lema, pois $Gal(f) \cong S_3$, já que não pode ser subconjunto das permutações pares, então é o próprio S_3. □

Exemplo 4.50. Tomemos o polinômio irredutível $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$. É um polinômio que já esta escrito na forma reduzida, com $p = -3$, $q = 1$. Podemos então calcular a discriminante deste polinômio.

$$\Delta(f) = -4p^3 - 27q^2$$
$$\Delta(f) = 81$$

Vemos que a discriminante Δ possui raiz racional, o que nos leva a afirmar que O grupo de Galois $G(K/\mathbb{Q}) \cong A_3$ (Corolário 4.40). Tomando o polinômio $g = f(x - 1)$,

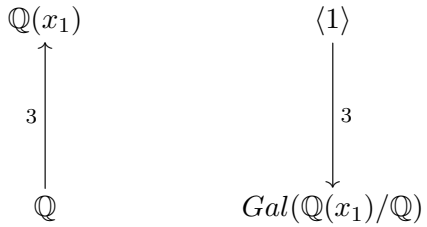
$$g = f(x - 1)$$
$$g = x^3 - 3x^2 + 3$$

Os coeficientes desse polinômios, exceto o do termo de maior grau, são múltiplos de 3, assim como exigido pelo critério. Mas 3, o termo de grau nulo, não é um quadrado em $\mathbb{Z}$, logo são

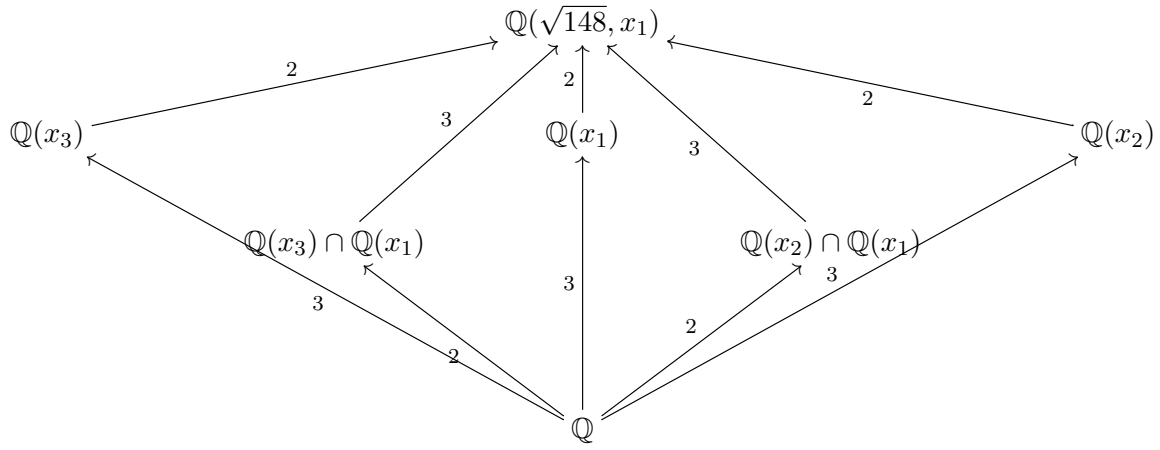
satisfeitas as condições para que g seja irredutível sobre $\mathbb{Q}$. Como $g = f(x-1)$, f também será irredutível.

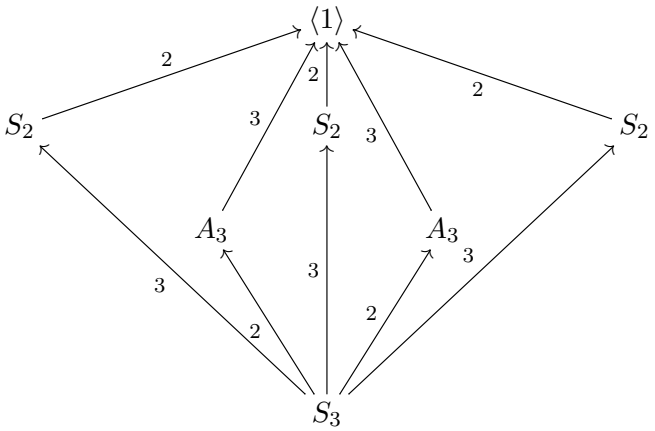
O Teorema 4.48, nos diz que quando nosso polinômio cúbico é irredutível, então o corpo de raízes deste polinômio $\mathbb{Q}(x_1, x_2, x_3) = \mathbb{Q}(\sqrt{\Delta}, x_1)$ ou seja $\mathbb{Q}(x_1)$ pois Δ é um quadrado em $\mathbb{Q}$, para este polinômio, onde x_1, x_2, x_3 , são suas raízes.

Podemos construir o diagrama que relaciona os subgrupos de Galois deste corpo de decomposição sobre $\mathbb{Q}$.



Exemplo 4.51. Ao contrário do exemplo acima temos o polinômio $h = x^3 - 4x + 2$, cúbico em sua forma reduzida, não possui discriminante quadrática, ou seja $\sqrt{\Delta(h)}$ não pertence a $\mathbb{Q}$. Sua discriminante $\Delta = 148 = 2^2 \cdot 37$. Usando o mesmo raciocínio, vemos que o corpo de decomposição desse polinômio sobre $\mathbb{Q}(\sqrt{(148)}, x_1)$, dessa forma seu grupo de Galois correspondente é isomorfo a S_3 pelo Corolário 4.40. Vejamos o diagrama





4.3.4 Polinômio de grau 4

Definição 4.52. *(cúbica resolvente) Sejam as combinações lineares,*

$$\begin{aligned} t_1 =& \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ t_2 =& \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ t_3 =& \alpha_1\alpha_4 + \alpha_2\alpha_3, \end{aligned}$$

onde $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ são as raízes do polinômio de quarto grau $f \in F[x]$.

Nos chamamos de cúbica resolvente o polinômio $r(x)$ do terceiro grau, que contêm t_1, t_2, t_3 como raízes, ou seja

$$r(x) = (x - t_1)(x - t_2)(x - t_3)$$

Lema 4.53. *Se $f(x) = x^4 + ax^3 + bx^2 + cx + d \in F[x]$ então sua cúbica resolvente será*

$$r(x) = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2 \in F[x]$$

Demonstração. Basta substituir as raízes, que conseguimos através da fórmula resolutiva de quárticas sobre a definição de cúbica resolvente. Omitiremos neste texto o cálculo, pois é simples mas exaustivo. □

Lema 4.54. *Sejam $f \in F[x]$ e $r \in F[x]$ polinômios que satisfazem as condições da Definição 4.52. Se $K = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, corpo de decomposição de $f \in F[x]$, cuja as raízes são $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ e $R = F(t_1, t_2, t_3)$, corpo de decomposição de $r \in F[x]$, cuja as raízes são t_1, t_2, t_3, então*

$$F \subset R \subset K$$

.

Demonstração. As raízes de $r \in F[x]$ pertencem a K, pois são combinações dos elementos deste corpo, logo pela Definição 3.27 temos que, $F \subset R \subset K$. □

Proposição 4.55. *As discriminantes Δ_f e Δ_r de um polinômio f de quarto grau e sua cúbica resolvente possuem o mesmo valor.*

Demonstração. Por definição

$$\sqrt{\Delta_f} = (\alpha_4 - \alpha_1)(\alpha_4 - \alpha_2)(\alpha_4 - \alpha_3)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)(\alpha_2 - \alpha_1)$$

onde α_j são raízes do polinômio f. Já a discriminante de r, é

$$\Delta_r = (t_3 - t_1)^2(t_3 - t_2)^2(t_2 - t_1)^2$$

onde,

$$\begin{aligned} t_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ t_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ t_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3 \end{aligned}$$

conforme a definição acima. Substituindo os valores de t_i temos:

$$\begin{aligned} \Delta_r &= (\alpha_1\alpha_4 + \alpha_2\alpha_3 - \alpha_1\alpha_2 - \alpha_3\alpha_4)^2(\alpha_1\alpha_4 + \alpha_2\alpha_3 - \alpha_1\alpha_3 - \alpha_2\alpha_4)^2(\alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4)^2 \\ &= (\alpha_4 - \alpha_1)^2(\alpha_4 - \alpha_2)^2(\alpha_4 - \alpha_3)^2(\alpha_3 - \alpha_1)^2(\alpha_3 - \alpha_2)^2(\alpha_2 - \alpha_1)^2 \\ &= \Delta_f. \end{aligned}$$

O que se faz demonstrada a Proposição. □

Classificação de polinômios de quarto grau

Lema 4.56. *Os subgrupos transitivos de S_4 são:*
(1) S_4 (o único de ordem 24)
(2) A_4 (o único de ordem 12)
(3) K_4 (o subgrupo de Klein)
(4) D_4 (Diedral de ordem 8)
(5) C_4 (Cíclico de ordem 4)

Demonstração. A demonstração deste Lema se encontra na página 301 do Livro [8], de nossa bibliografia. □

Teorema 4.57. *Seja $f \in F[x]$ polinômio irredutível de grau 4, e $r(f)$ sua cúbica resolvente, onde K e R são seus respectivos corpos de decomposição e $[R : F] = m$*

(i) $Gal(f) \cong S_4$ se e somente se, $r(f) \in F[x]$ é irredutível, e Δ_f não é um quadrado perfeito em F, se e somente se, $m = 6$.

(ii) $Gal(f) \cong A_4$ se e somente se, $r(f) \in F[x]$ é um polinômio irredutível, e Δ_f é um quadrado perfeito em F, se e somente se, $m = 3$.

(iii) $Gal(f) \cong K_4$ se e somente se, $r(f) \in F[x]$ se decompõe sobre F, se e somente se $m = 1$.

(iv)$Gal(f) \cong C_4$ se e somente se, $r(f) \in F[x]$ tem uma única raiz $t \in F$, $f \in R[x]$ for redutível e $m = 2$.

(v) $Gal(f) \cong D_4$ se e somente se, $r(f) \in F[x]$ tem uma única raiz $t \in F$, $f \in R[x]$ for irredutível e $m = 2$.

Demonstração. Vamos estabelecer condições gerais apartir de nossa hipótese.

Seja a Torre $K \subset R \subset F$, pelo Teorema 3.9 $[K : R] \leq 4$, pois $K = R(\alpha_1)$, onde α_1 é uma das raízes de $f \in F[x]$ e pelo Teorema 3.24, $[K : R] = deg(m_\alpha) \leq 4$, pois α é raiz de um polinômio de grau 4, e o polinômio mínimo m_α divide f, pelo Lema 3.18. $[K : R] = 4$ se só se existir um único automorfismo em $Gal(K/R)$ que fixa os elementos de K.

Quanto a cúbica resolvente $r \in F[x]$, Sabemos que $[R : F] \leq 6$, pois $[R : F] \leq 3!$, assim como dito no Teorema 3.30. Se $r \in F[x]$ é irredutível, e $R = F(t_1, t_2, t_3)$, onde t_1, t_2, t_3 são as raízes de $r \in F[x]$, por definição de *Compositum* (Definição 4.26), $R = F(t_3)(t_2, t_1)$, então asseguramos que $m = 3$ ou $m = 6$, pois

$$[R : F] = [R : F(t_3)][F(t_3) : F] = [R : F(t_3)]deg(m_{t_3}),$$

como visto no Teorema da Torre e no Teorema 3.24, ou seja,

$$[R : F] = [R : F(t_3)]deg(m_{t_3}) = 3 \cdot [R : F(t_3)].$$

Se $r \in F[x]$ tem uma única raíz em F, se só se $m = 2$, pois neste caso o polinômio mínimo das outras duas raízes seria de grau 2.

Se $r \in F[x]$ é redutível, neste caso digo, se decompõe completamente, então $[R : F] = 1$, pois para todo $\phi \in Gal(r)$, $\phi(x) = x$ para todo $x \in R$, já que R/F é de Galois pelo Teorema 3.62.

(i) Suponha que $r \in F[x]$, seja irredutível e Δ_r não é um quadrado perfeito em F. Como visto no Corolário 4.40, isso acontece se somente se $Gal(r) \cong S_3$, logo $m = 6$ (Corolário 3.59), e por consequência $Gal(f) \cong S_4$, já que $\Delta_r = \Delta_f$ (Proposição 4.55).

(ii) Similarmente, $r \in F[x]$, seja irredutível e Δ_r é um quadrado perfeito em F se só se $Gal(f) \cong A_4$ de acordo com o Corolário 4.40.

(iii) Se $m = 1$ então $[K : F] = 4$, Proposição 4.24, como $f \in F$ é irredutível, então $Gal(f)$ é isomorfo a um subgrupo transitivo de S_4, que contem 4 elementos. Vimos no primeiro parádiagrama desta demonstração que $K = F(\alpha_1)$, já que $R = F$ por $r \in F[x]$ ter todas as raízes em F. Com isso sabemos que temos 4 automorfismos em $Gal(f)$, portanto $Gal(f) \cong K_4$, pois é o único subgrupo transitivo de ordem 4 entre os subgrupos transitivos de S_4 (Lema 4.56).

As duas últimas afirmações são a respeito de $m = 2$. Como $[K : F] \leq 4$, já que não existem subgrupo transitivos de S_4 de grau menor que 4, sabemos que $[K : F] = 4$, neste caso $G(f) \cong C_4$, pois outro único subgrupo transitivo de ordem 4 seria K_4, o que não pode ocorrer pois $m \neq 1$, como visto no item (iii), ou

(v) $[K : F] = 8$, onde $Gal(f) \cong D_4$, o único subgrupo transitivo de S_4 de ordem 8. $Gal(f) \cong D_4$ se somente se $m = 2$ (Teorema da Torre), e $f \in R[x]$ for irredutível, pois f é o minimal de α_1, onde $deg(f) = [K : R] = 4$, visto no Teorema 3.24. (iv) o quarto item deste Teorema é dado por exclusão, já que já foram listados todos os outros possíveis subgrupos transitivos de S_4, como visto no Lema 4.56. □

4.3.5 Alguns exemplos

Exemplo 4.58. Seja $f(x) = x^3 + 3x + 1 \in \mathbb{Q}[x]$. Sabemos que este polinômio é irredutível, através do Critério de "Eisenstein". Calculando a discriminante deste polinômio (Lema 4.45), temos

$$\Delta_f = -27 - 4 * 27 = -137,$$

o que claramente não é um quadrado em $\mathbb{Q}$, em vista que todos os quadrados em $\mathbb{Q}$ são positivos. Com isso, pelo Lema 4.42, o grupo de Galois deste polinômio é isomorfo a S_3.

Exemplo 4.59. O polinômio $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$, também é irredutível pelo critério de "Eisenstein", e sua discriminante é

$$\Delta_f = -27 + 4 * 27 = 81,$$

cujo a raiz quadrada é 9. Portanto, pelo Lema 4.42, seu grupo de Galois é isomorfo a A_3.

Exemplo 4.60. Vamos encontrar o grupo de Galois do polinômio $f(x) = x^4 - 4x^2 + x + 1 \in \mathbb{Q}$. Pelo Lema 4.53, vemos que sua cúbica resolvente é $r(f) = x^3 + 4x^2 - 4x - 17 \in \mathbb{Q}[x]$ cuja a discriminante determinada pelo Lema 4.47, é $\Delta_r = 1957$ que não é um quadrado em $\mathbb{Q}$. Com isso sabemos que $Gal(r(f)) \cong S_3$, pelo Lema 4.42, o que nos leva a concluir que $Gal(f) \cong S_4$, segundo o Teorema 4.57.

Exemplo 4.61. Vamos trabalhar com generalizações. Seja o polinômio irredutível, $f = x^4 + ax^3 + bx^2 + ax + 1 \in F[x]$. Neste caso a sua cúbica resolvente é

$$r(f) = x^3 - bx^2 + (a^2 - 4)x - 2a^2 + 4b$$
$$r(f) = (x - 2)(x^2 + (2 - b)x + a^2 - 2b)$$

Neste caso nossa resolvente se decompõe em F se somente se $(2-b)^2+4(2b-a^2)$ for um quadrado em F, pois neste caso $(x^2 + (2 - b)x + a^2 - 2b) \in F[x]$, é um polinômio redutível, segundo a fórmula de resolução de equações quadráticas, onde $(2 - b)^2 + 4(2b - a^2)$ é sua determinante. Como neste caso $[R : F] = 1$, pelo Teorema 4.57, $Gal(f) \cong K_4$. E sua discriminante é $\Delta_f = (4b - a^2 - 8)^2(b - 2a + 2)(b + 2a + 2)$, uma vez que $\Delta_r(f) = \Delta_f$ (Proposição 4.55), e pelo Lema 4.47. Com isso se $(b-2a+2)(b+2a+2) = b^2-4(a-1)^2$ for um quadrado em F, então $G(f) \cong K_4$

Exemplo 4.62. Seja agora o polinômio irredutível $f = x^4 + bx^2 + d \in F[x]$, onde d não é um quadrado em F. Calculando sua cúbica resolvente (Lema 4.53) temos que

$$r(f) = x^3 - bx^2 + (ac - 4d)x - c^2 - a^2d + 4bd$$
$$r(f) = x^3 - bx^2 - 4dx + 4bd$$
$$r(f) = x^3 - bx^2 - 4dx + 4bd$$

usando a troca de variável dada no Lema 4.45, nos temos,

$$r(f) = x^3 - bx^2 - 4dx + 4bd$$
$$r(f) = (x - b)(x^2 - 4d)$$

Calculando sua discriminante, através da definição (Definição 4.37), temos que

$$\Delta_f = 16d(b^2 - 4d)^2$$

Claramente, $r(f)$ será um polinômio redutível se $d \in F$ for um quadrado. Neste caso $G(f) \cong K_4$, pelo Teorema 4.57.

Caso $r(f)$ não seja redutível sobre F, então seu corpo de decomposição será $R = F(\sqrt{d}, \Delta_r) = F(\sqrt{d})$, de acordo com o Teorema 4.48, e pelo Teorema 4.57 sabemos que grupo de Galois $Gal(f) \cong C_4$, se f tiver todas suas raízes em R, ou $Gal(f) \cong D_4$, se $f \in F[x]$ não tiver todas suas raízes em R, pois $[R : F] = 2$.

Exemplo 4.63. Um outro caso que podemos analisar é o do polinômio $f = x^4-d \in \mathbb{Q}[x]$. Usando a teoria estudada na última seção vemos que a resolvente desta quártica é $r(f) = x^3 + 4dx =$

$x(x^2+4d)$. A discriminante deste polinômio é $\Delta_f = -16^2d^3$, pois se trata do caso $b=0$ para o exemplo anterior, substituindo d, por $-d$, em vista da diferença de sinal do último coeficiente entre os exemplos.

Logo o corpo de decomposição de $r(f) \in \mathbb{Q}[x]$ será,

$$R = \mathbb{Q}(\sqrt{-16^2d^2d}, \sqrt{-4d}) = \mathbb{Q}(16d\sqrt{-d}, 4\sqrt{-d}) = \mathbb{Q}(16d\sqrt{-d}, 4\sqrt{-d}) = \mathbb{Q}(\sqrt{-d}, \sqrt{-d}) = \mathbb{Q}(\sqrt{-d})$$

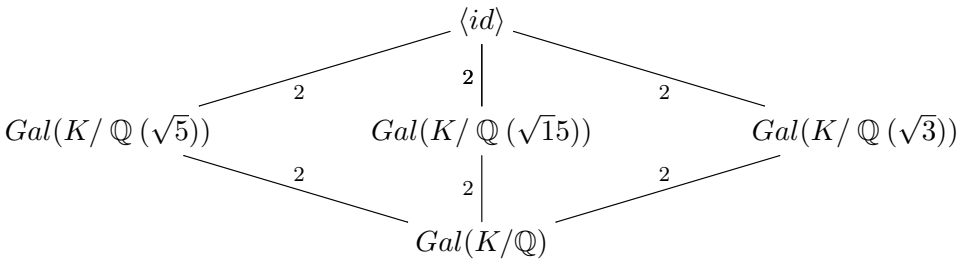
.

Temos então algumas possibilidades:
se $-d$ for um quadrado em $\mathbb{Q}$, então $[R:\mathbb{Q}] = 1$ e com isso, $Gal(f) \cong K_4$
se d for um quadrado em $\mathbb{Q}$, então $[R:\mathbb{Q}] = 2$, e neste caso $f = (x^2 - \sqrt{d})(x^2 + \sqrt{d}) \in \mathbb{Q}[x]$, terá o mesmo corpo de decomposição que $r(f) = x(x^2+4d) \in \mathbb{Q}(x)$. Com isso o grupo de Galois de f será isomorfo a D_4 ou K_4, de acordo com as condições estabelecidas no último Teorema.

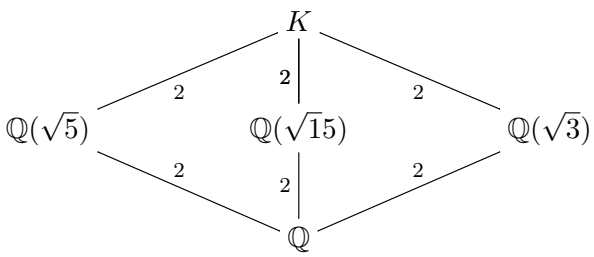
Exemplo 4.64. Seja $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, o corpo de decomposição de $f(x) = (x^2-3)(x^2-5) \in \mathbb{Q}[x]$. A dimensão de $K/\mathbb{Q}$ é 4, em vista do Teorema da Torre e do Teorema 3.30, um vez que $[K:\mathbb{Q}] = [K:\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = deg(m_{\sqrt{5}}) \cdot deg(m_{\sqrt{3}}) = 4$. De acordo com o Corolário 3.59 $Gal(K/\mathbb{Q})$, possui quatro automorfismos

$$\begin{aligned} id &: \sqrt{3} \to \sqrt{3}, \sqrt{5} \to \sqrt{5}; \\ \phi &: \sqrt{3} \to -\sqrt{3}, \sqrt{5} \to \sqrt{5}; \\ \gamma &: \sqrt{3} \to \sqrt{3}, \sqrt{5} \to -\sqrt{5}; \\ \phi\gamma &: \sqrt{3} \to -\sqrt{3}, \sqrt{5} \to -\sqrt{5}. \end{aligned}$$

Logo $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2\,\mathbb{Z} \oplus \mathbb{Z}\,/2\mathbb{Z}$, cujo os subgrupos são, $\langle id \rangle$, $\langle \phi \rangle$, $\langle \gamma \rangle$, $\langle \phi\gamma \rangle$ e $Gal(K/\mathbb{Q})$.



Pelo Teorema Fundamental da Teoria de Galois, suas extensões correspondente são respectivamente K/K, $K/\,\mathbb{Q}\,(\sqrt{3})$, $K/\,\mathbb{Q}\,(\sqrt{5})$,$K/\,\mathbb{Q}\,(\sqrt{15})$ e $K/\mathbb{Q}$.



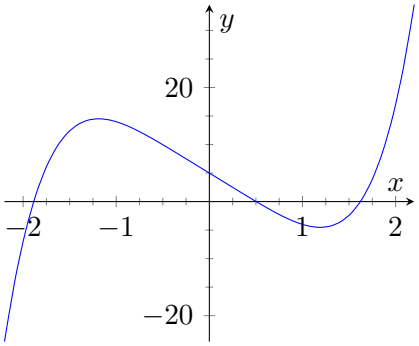
Exemplo 4.65. Não é possível ter uma fórmula resolutiva para um polinômio de quinto grau em $\mathbb{C}[x]$.

Só podemos construir uma fórmula genérica para resolução de polinômios se garantirmos que suas raízes são solúveis (Definição 4.30). Isso por sua vez, não é possível de ocorrer para polinômios de quinto grau sobre $\mathbb{C}$, pois se isso ocorresse certamente seu grupo de Galois seria um grupo isomorfo a um subgrupo de S_5 (Teorema 4.24). É sabido que S_5 não é solúvel, pois se assim fosse todos os seus subgrupos seriam (Lema 4.8), mas A_5 não é (Lema 4.14). A não possibilidade de uma fórmula deriva do fato de que, só podemos falar de fórmula resolutiva para polinômios de quinto grau, ou graus mais altos, se garantirmos a solubilidade de seu grupo de Galois antes,(Teorema 4.36) já que $S_5 \leqslant S_n$, para todo $n \geq 5$.

Um exemplo do fato é o polinômio $f(x) = x^5 - 10x + 5 \in \mathbb{Q}[x]$.

O polinômio em questão é irredutível pelo critério de Eisenstein, basta tomarmos $p = 5$. Com isso vemos $Gal(f)$ tem um subgrupo de ordem 5, pois a extensão $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) = deg(m_\alpha) = 5$, onde α é uma das raízes de f.

Pela análise do gráfico abaixo vemos que nosso polinômio tem exatamente 3 raízes reais.



Logo temos duas raízes complexas conjugadas, ou seja temos em nosso grupo de Galois uma transposição.

Como $Gal(f) = S_5$ é um grupo de Galois com um subgrupo cíclico de ordem 5 e uma transposição, concluímos que este grupo é isomorfo a S_5 pois é um subgrupo de S_5, que contém um elemento de $\mathbb{Z}_5$ e uma transposição (este resultado pode ser visto na página 128 do livro [5]).

Podemos concluir que $f(x)$ não é solúvel por radicais pois seu grupo de Galois correspondente S_5 não é um grupo solúvel.

Capítulo 5

Conclusão

Com base no estudo feito, e nas linhas aqui escritas, vimos que é possível analisar polinômios e extensões de Corpos a partir de seu grupo de Galois. A Teoria de Galois tem como fim, fazer a correspondência entre o estudo de grupos e o estudo de corpos.

Como já dito anteriormente, o presente texto só explora extensões de característica nula e algébricas, ficando por sugestão para trabalhos futuros o estudo da teoria de Galois para extensões transcendentes e ou de característica prima. Outro possível estudo é fazer uma exploração mais aprofundada sobre a "Teoria de Galois", observando outros resultados, como a ligação da teoria com a construção de figuras planas a partir de régua e compasso, abordando casos famosos como a trissecção de um ângulo, ou da possibilidade de construir um $n-$ágono regular. Também é possível, trabalharmos com a solubilidade, analisar o cálculo de polinômios de graus mais altos, assim como a obtenção de fórmulas resolutiva de equações solúveis.

Em fim, existe um mundo de ideias que se pode explorar a partir daqui, ou seja, que nosso trabalho seja apenas um caminho para futuros textos.

Referências Bibliográficas

[1] SNAITH, Victor Percy. **Groups, rings and Galois theory**. World Scientific, 2003.

[2] MORANDI, Patrick. **Field and Galois Theory**. Springer Science & Business Media, 1996.

[3] KAPLANSKY, Irving. **Introdução à teoria de Galois**. Instituto de Matemática Pura e Aplicada, Conselho Nacional de Pesquisas, 1958.

[4] STEWART, Ian. **Galois Theory**, Chapman Hall/CRC Mathematics Series. 2003.

[5] ROTMAN, Joseph. **Galois theory**. Springer Science & Business Media, 1998.

[6] WEINTRAUB, Steven. **Galois theory**. Springer Science & Business Media, 2008.

[7] COX, David A. **Galois theory**. John Wiley & Sons, 2004.

[8] MARTIN, Paulo A. **Grupos, corpos e teoria de Galois**. Editora Livraria da Física, 2010.