INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
IFSP-CAMPUS SÃO PAULO
LICENCIATURA EM MATEMÁTICA
TRABALHO DE CONCLUSÃO DE CURSO

ESTUDO DAS RELAÇÕES DE ISOMORFISMO ENTRE EXTENSÕES ALGÉBRICAS

TRABALHO DE CONCLUSÃO DE CURSO

JOÃO VICTOR DOS SANTOS GONÇALVES

SÃO PAULO-SP
2020

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
IFSP-CAMPUS SÃO PAULO
LICENCIATURA EM MATEMÁTICA
TRABALHO DE CONCLUSÃO DE CURSO

ESTUDO DAS RELAÇÕES DE ISOMORFISMO ENTRE EXTENSÕES ALGÉBRICAS

JOÃO VICTOR DOS SANTOS GONÇALVES

Trabalho de Conclusão de curso apresentado como requisito parcial para obtenção do título de licenciado em Matemática.

Orientador:
Prof. Ms. Leandro Albino Mosca Rodrigues

SÃO PAULO-SP
2020

Gonçalves, João Victor dos Santos
ESTUDO DAS RELAÇÕES DE ISOMORFISMO ENTRE EXTENSÕES ALGÉBRICAS / João Victor dos Santos Gonçalves. -- 2020.
60 f.

Orientador: Leandro Albino Mosca Rodrigues

Trabalho (Conclusão de curso) - Instituto Federal de Educação,Ciência e Tecnologia, IFSP-Campus São Paulo, Licenciatura em Matemática, São Paulo, SP-BR, 2020.

Anel, Polinômio, Extensão, Isomorfismo, Automorfismo. I. Rodrigues, Leandro Albino Mosca, orient. II. Estudo das Relações de Isomorfismo entre Extensões Algébricas.

SERVIÇO PÚBLICO FEDERAL
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO
DIRETORIA GERAL/CAMPUS SAO PAULO
Câmpus São Paulo, (11) 2763-7520, Rua Pedro Vicente, 625, CEP 01109-010, São Paulo (SP)

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Na presente data realizou-se a sessão pública de defesa da Trabalho de Conclusão de Curso intitulada **Estudo das Relações de Isomorfismo entre Extensões Algébricas** apresentada pelo aluno **Joao Victor dos Santos Goncalves (SP1660535)** do Curso **LICENCIATURA EM MATEMÁTICA (Câmpus São Paulo)**. Os trabalhos foram iniciados às **14:00** pelo Professor presidente da banca examinadora, constituída pelos seguintes membros:

Membros	IES	Presença	Aprovação/Conceito *(quando exigido)*
Leandro Albino Mosca Rodrigues (Orientador)	IFSP - SPO	Presente	8,5
Valeria Ostete Jannis Luchetta (Examinadora Interna)	IFSP - SPO	Presente	8,5
Tiago Rodrigo Perdigão (Examinador Externo)	CEFET - MG	Presente	8,5

Observações:

O aluno foi aprovado, devendo fazer as correções indicadas pela banca que será enviada por e-mail ao orientador e encaminhadas ao aluno.

A banca examinadora, tendo terminado a apresentação do conteúdo da monografia, passou à argüição do candidato. Em seguida, os examinadores reuniram-se para avaliação e deram o parecer final sobre o trabalho apresentado pelo aluno, tendo sido atribuído o seguinte resultado:

[x] Aprovado [ ] Reprovado Nota (quando exigido): 8,5

Proclamados os resultados pelo presidente da banca examinadora, foram encerrados os trabalhos e, para constar, eu lavrei a presente ata que assino juntamente com os demais membros da banca examinadora.

SÃO PAULO / SP, 11/09/2020

Leandro Albino M. Rodrigues

Leandro Albino Mosca Rodrigues

Valéria O. Jannis Luchetta

Valeria Ostete Jannis Luchetta

Tiago Rodrigo Perdigão

Tiago Rodrigo Perdigão

Para Kátia, por renovar minhas esperanças todos os dias.

Agradecimentos

> E há de ser tua ciência uma tão íntima conexão de ti mesmo e tua existência, que ninguém suspeitará de nada.
>
> Carlos Drummond de Andrade, do poema *A Luís Maurício, Infante.*

A seção dedicada aos agradecimentos constitui-se como a parte mais difícil deste trabalho. Não somente pela impossibilidade de mencionar todas as pessoas às quais dedico meus sentimentos de gratidão e apreço, mas também pela incapacidade linguística de nosso idioma em encontrar palavras que descrevam fielmente e à altura minha enorme admiração e estima.

Gostaria de agradecer a todas as pessoas que direta ou indiretamente contribuíram para a consecução deste trabalho, bem como àquelas que me acompanharam ao longo dos últimos anos, fornecendo suporte, apoio, carinho e compreensão. Em especial, gostaria de agradecer ao meu avô Antônio, aos professores e aos amigos do Instituto Federal. Meus sinceros agradecimentos ao professor e orientador Leandro, pela dedicação e por me conceder esta oportunidade, e aos amigos Silas, Gabriel e Augusto, os quais, entre outros, me prestigiaram com maravilhoso convívio durante minha estadia no Instituto.

Dedico meus agradecimentos também ao meu amigo Anderson, pelo constante apoio, e à minha amiga Kátia, pelo carinho e compreensão nos momentos mais difíceis. Todas as pessoas citadas nesta seção, entre outras, exerceram considerável influência sobre mim, contribuindo de forma determinante para o ser humano que hoje sou. Não há palavras que possam resumir com exatidão meu sentimento de gratidão.

Resumo

Este trabalho tem como objetivo principal apresentar um estudo das relações de isomorfismo existentes entre extensões algébricas de corpos. Através de uma pesquisa bibliográfica, mostraremos em especial que o número de automorfismos de uma extensão algébrica e finita $L \supset K$ que fixam o corpo K é igual à dimensão do espaço vetorial L sobre K. Para consecução de tal finalidade, apresentamos também um estudo introdutório sobre as teorias de anéis, homomorfismo e álgebra linear, bem como sobre a teoria de polinômios em uma indeterminada.

Palavras-chave: Anel, Polinômio, Extensão, Isomorfismo, Automorfismo.

Abstract

This work has as main objective to present a study about the existing isomorphism relations between algebraic extensions of fields. Through a bibliographic research, it especially demonstrates that the number of automorphisms of a finite and algebraic extension $L \supset K$ fixing K is equal to the dimension of the vector space L over K. To achieve this goal, it also presents an introductory study about the rings, homomorphism, and linear algebra theories, such as about the polynomial in a single indeterminate theory.

Key Words: Ring, Polynomial, Extension, Isomorphism, Automorphism.

Sumário

Introdução **1**

1 Noções Preliminares **3**
1.1 Teoria de Anéis 3
1.2 Homomorfismos 5
1.3 Álgebra Linear 7

2 Polinômios em uma Indeterminada **11**
2.1 Apresentação Geral de Polinômios 11
2.2 Divisibilidade em $K[x]$ 13
2.3 Raízes de um Polinômio 14
2.4 Polinômios Irredutíveis 16
2.5 Irredutibilidade sobre $\mathbb{Q}$ 17

3 Extensões Algébricas de Corpos **21**
3.1 Processo de Adjunção de Raízes 21
3.2 Extensões de Corpos 23

4 Isomorfismos entre Extensões Algébricas **31**
4.1 Extensões Galoisianas e Extensões Normais 31
4.2 Isomorfismos entre Extensões Galoisianas 34
4.3 Automorfismos de Extensões Galoisianas 38

Considerações Finais **41**

Referências Bibliográficas **45**

Introdução

O estudo dos isomorfismos e automorfismos de corpos são de importante relevância no contexto da álgebra abstrata. Sendo estes corpos particularmente extensões de tipo algébrica e finita, somos levados à seguinte questão: é possível determinar o número de automorfismos de uma extensão algébrica e finita $L \supset K$ que fixam o corpo K? Baseando-se nesta problemática, dividimos nosso texto em quatro capítulos.

O primeiro capítulo é dedicado à apresentação de noções basilares sobre as teorias de anéis, homomorfismos e álgebra linear. Aqui demos preferência em apresentar os principais conceitos que estão diretamente relacionados com a nossa posterior construção teórica e com os objetivos de nosso texto. Evidentemente, muitos conteúdos da teoria de anéis, tais quais anéis quocientes e ideais, não estão contemplados neste trabalho, visto que não nos foi necessário referir diretamente a estes tópicos durante a execução de nosso texto. Analogamente, não apresentamos aqui também o estudo matricial da álgebra linear, bem como o estudo específico dos espaços vetoriais $\mathbb{R}^n$ sobre $\mathbb{R}$, encontrados em Winterle e Steinbruch (1987). Ainda, este trabalho foi escrito baseando-se na premissa de que o leitor já saiba previamente alguns tópicos básicos de matemática elementar, tais quais funções e teoria dos conjuntos, números primos, complexos, etc.

O segundo capítulo é dedicado a uma apresentação geral da teoria de polinômios sobre um corpo K e em uma indeterminada x. Demos prioridade em destacar o estudo das raízes de um polinômio, bem como as noções de divisibilidade e irredutibilidade de polinômios sobre o corpo $\mathbb{Q}$.

O terceiro capítulo apresenta um estudo sobre as extensões algébricas de corpos. Aqui apresentamos inicialmente o processo de adjunção de raízes, de fundamental importância em nosso texto, e seguimos com o estudo das extensões L de um corpo K,

com ênfase na apreciação das extensões de tipo algébrica e seus resultados no contexto da álgebra linear.

O capítulo final, e principal em nosso trabalho, apresenta um estudo das relações de isomorfismo entre extensões algébricas. Demos ênfase inicialmente aos conceitos de extensão galoisiana e extensão normal, que são importantes em nosso texto, e seguimos com o estudo dos isomorfismos e automorfismos sobre estas extensões, até a demonstração do teorema final e objetivo último de nosso trabalho, referente ao número de automorfismos de uma extensão algébrica e finita L que fixam o subcorpo $K \subset L$. Para melhor visualização dos resultados obtidos, este capítulo segue com numerosos exemplos referentes às definições e teoremas. Em especial, este capítulo é finalizado com exemplos concretos dos resultados referentes ao teorema principal.

Todas as referências apresentadas ao final deste trabalho foram citadas ao longo do texto. Em particular, esse trabalho segue de perto as contribuições de Gonçalves (1979), Grillet (2007), Hungerford (1974), Dummit e Foote (1991). Nos apoiamos nos demais autores de forma mais pontual e discreta, enquanto os autores citados acima, principalmente Gonçalves (1979), foram mais presentes na estruturação e execução de nosso texto. Em especial, os autores da editora Springer serviram de imprescindível contribuição para a escrita deste trabalho.

Capítulo 1

Noções Preliminares

Neste capítulo apresentaremos noções introdutórias necessárias para um melhor entendimento deste trabalho como um todo. Em especial, apresentaremos alguns resultados básicos da teoria de anéis e da álgebra linear.

1.1 Teoria de Anéis

Definição 1. Seja $A \neq \varnothing$ um conjunto sobre o qual definimos as operações de *adição* e *multiplicação*, indicadas respectivamente por $+$ e $\cdot$

$$\begin{array}{ll} + : A \times A \to A & \cdot : A \times A \to A \\ (a,b) \mapsto a+b & (a,b) \mapsto a \cdot b \end{array}$$

Dizemos que $(A, +, \cdot)$ é um *anel* se as seguintes propriedades são válidas para todos elementos $a, b, c \in A$:

1. $(a+b)+c = a+(b+c)$ (associatividade da adição).

2. $a+b = b+a$ (comutatividade da adição).

3. Existe $0 \in A$ tal que $a+0 = a$ (existência de elemento neutro aditivo).

4. Para todo $a \in A$, existe um único $(-a) \in A$ tal que $a+(-a) = 0$ (existência de elemento oposto aditivo).

5. $a(b+c) = ab+ac$ e $(b+c)a = ba+ca$ (distributiva à direita e à esquerda da operação de multiplicação em relação à adição).

6. $a(bc) = (ab)c$ (associatividade da multiplicação).

Se $(A, +, \cdot)$ é um anel que satisfaz a propriedade:

7. Existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in A$, dizemos que $(A, +, \cdot)$ é um *anel com unidade* 1.

8. $a \cdot b = b \cdot a$, para todos $a, b \in A$, dizemos que $(A, +, \cdot)$ é um *anel comutativo.*

9. Para todos $a, b \in A$, se $a \cdot b = 0$ implicar que $a = 0$ ou $b = 0$, dizemos que $(A, +, \cdot)$ é um *anel sem divisores de zero.*

Ainda, se $(A, +, \cdot)$ é um anel comutativo, com unidade, e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um *domínio de integridade*[1].

Quando estão subentendidas as operações do anel $(A, +, \cdot)$, indica-se este anel somente por A. Ainda, estas operações não necessariamente são as operações usuais de adição e multiplicação.

Definição 2. Seja A um domínio de integridade. Se para todo elemento não nulo $a \in A$ existir algum elemento $b \in A$ tal que $a \cdot b = 1$, dizemos que A é *corpo*. Nestas condições indicamos $b = a^{-1}$.

Exemplo 1. O conjunto $Mat_n(\mathbb{R})$ de todas as matrizes com elementos reais e ordem $n \in \mathbb{N}^*$ munido das operações usuais de adição e multiplicação de matrizes é um anel.

Exemplo 2. Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ munidos das operações usuais de adição e multiplicação são anéis, sendo $\mathbb{Z}$ domínio de integridade e $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ corpos.

Definição 3. Seja A um anel e $B \subset A$ um conjunto não vazio. Se B for um anel com as operações de A dizemos que B é um *subanel* de A.

Definição 4. Se um subanel B de um domínio de integridade A é também domínio de integridade, dizemos que B é *subdomínio* de A. Analogamente, se um subanel B de um corpo A é também corpo, dizemos que B é *subcorpo* de A.

[1] Nestas condições, Monteiro (1969) denomina $(A, +, \cdot)$ *anel de integridade.*

Janesch e Taneja (2011) apontam que sendo $B \subset A$ subanel com unidade e A domínio de integridade, então a unidade de B é a mesma unidade de A.

Exemplo 3. Como $A \supset A$, todo anel A é subanel de si mesmo. Sendo A domínio de integridade ou corpo, vem que A é também subdomínio ou subcorpo de si.

Exemplo 4. $\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$ são subanéis de $\mathbb{C}$, sendo $\mathbb{Q}$ e $\mathbb{R}$ subcorpos.

Teorema 1. Seja A um anel com elemento neutro aditivo $0 \in A$ e $B \subset A$ um conjunto não vazio. Então B é subanel de A se, e somente se, as seguintes condições são atendidas:

1. $0 \in B$

2. $x - y \in B$, para todos $x, y \in B$.

3. $x \cdot y \in B$, para todos $x, y \in B$.

A demonstração do teorema acima pode ser encontrada em Gonçalves (1979) e em Domingues e Iezzi (2003).

1.2 Homomorfismos

Definição 5. Sejam K e K' anéis. Dizemos que a função $f : K \to K'$ é um *homomorfismo* de K em K' se $f(x + y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$, para todos $x, y \in K$.

É importante observar que, nas condições da definição acima, as operações do anel K não necessariamente são as mesmas operações do anel K'.

Se o homomorfismo $f : K \to K'$ for bijetivo, dizemos que f é *isomorfismo* de K sobre K'. Nestas condições, dizemos que K e K' são *isomorfos* e indicamos $K \simeq K'$. Ao isomorfismo $f : K \to K$ chamamos *automorfismo* de K.

Exemplo 5. Sendo K e K' anéis, a função $f : K \to K'$ tal que $f(x) = 0 \in K'$ para todo $x \in K$ é um homomorfismo, denominado *homomorfismo nulo.*

Exemplo 6. A função $f : K \to K$ tal que $f(x) = x$ para todo $x \in K$, denominada *função identidade*, é um isomorfismo de K sobre K e, portanto, um automorfismo de K.

Exemplo 7. A função $f : \mathbb{C} \to \mathbb{C}$ tal que $f(a+bi) = a - bi$, para todos $a + bi \in \mathbb{C}$, define um automorfismo de $\mathbb{C}$.

Teorema 2. Sejam K e K' anéis com elemento neutro aditivo 0 e $0'$, respectivamente. Se $f : K \to K'$ é homomorfismo, então:

1. $f(0) = 0'$

2. $f(-x) = -f(x)$, para todo $x \in K$.

3. Se K e K' são domínios de integridade então $f(x) = 0$ para todo $x \in K$ ou $f(1) = 1'$, sendo 1 e $1'$ as respectivas unidades de K e K'.

4. Se K e K' são corpos então $f(x) = 0$ para todo $x \in K$ ou f é injetiva.

Definição 6. Sejam K e K' anéis e $f : K \to K'$ um homomorfismo. Chama-se *núcleo* do homomorfismo f o conjunto formado por todos elementos $a \in K$ tais que $f(a) = 0$.

Nas condições da definição acima, indicamos o núcleo do homomorfismo f por $Ker f$. Observamos que $Ker f \subset K$ e, pelo item 1 do teorema anterior, $Ker f \neq \varnothing$.

Teorema 3. Sejam K e K' anéis e $f : K \to K'$ um homomorfismo. Então f é injetiva se, e somente se, $Ker f = \{0\}$.

As demonstrações dos Teoremas 2 e 3 podem ser encontradas em Gonçalves (1979) e em Winterle e Steinbruch (1987), respectivamente. Traremos agora algumas definições que serão importantes, em especial, para o último capítulo deste trabalho.

Definição 7. Sejam L, L' e K corpos tais que $L, L' \supset K$. Dizemos que o homomorfismo $f : L \to L'$ é *K-homomorfismo* se $f(x) = x$ para todo $x \in K$.

Nas condições da definição acima, dizemos que o homomorfismo f *fixa* o corpo K. Caso o K-homomorfismo f seja isomorfismo, dizemos que f é *K-isomorfismo.*

Ainda, aos automorfismos de L que fixam K denominamos *K-automorfismos de L*. Indicamos o conjunto de todos os automorfismos de L que fixam K por Aut_K^L, sendo o número de elementos deste conjunto denotado por $|Aut_K^L|$.

Exemplo 8. A função $f : \mathbb{C} \to \mathbb{C}$ tal que $f(a + bi) = a - bi$, para todo $a + bi \in \mathbb{C}$, é um automorfismo de $\mathbb{C}$ que fixa $\mathbb{R}$. Dizemos então que f é um $\mathbb{R}-$automorfismo de $\mathbb{C}$ e indicamos $f \in Aut_{\mathbb{R}}^{\mathbb{C}}$.

1.3 Álgebra Linear

Definição 8. Sejam K corpo e W um conjunto não vazio. Definidas as seguintes operações, denominadas *adição* e *multiplicação por escalar*

$$\begin{array}{ll} +: W \times W \to W & \cdot : K \times W \to W \\ (u, v) \mapsto u + v & (\lambda, u) \mapsto \lambda u \end{array}$$

dizemos que W munido dessas operações é um *espaço vetorial* sobre K se para todos $u, v, w \in W$ e $\lambda, \gamma \in K$ forem válidas as seguintes propriedades:

1. $(u + v) + w = u + (v + w)$ (associatividade da adição).

2. $u + v = v + u$ (comutatividade da adição).

3. Existe $0 \in W$ tal que $u + 0 = u$ (existência de elemento neutro aditivo).

4. Para todo $u \in W$, existe um único $(-u) \in W$ tal que $u + (-u) = 0$ (existência de elemento oposto aditivo).

5. $1u = u$, sendo 1 a unidade do corpo K.

6. $\lambda(u + v) = \lambda u + \lambda v$ e $(\gamma + \lambda)u = \gamma u + \lambda u$.

7. $\lambda(\gamma u) = \gamma(\lambda u) = (\gamma\lambda)u$.

Nas condições da definição acima, os elementos de W são chamados *vetores* e os elementos de K são chamados *escalares*.

Exemplo 9. $\mathbb{C}$ é espaço vetorial sobre $\mathbb{R}$ e $\mathbb{Q}$. Ainda, $\mathbb{R}$ é espaço vetorial sobre $\mathbb{Q}$.

Exemplo 10. De forma geral, sendo W corpo e $K \subset W$ subcorpo, W é espaço vetorial sobre K.

Sahai e Bist (2002) apontam que, nas condições do exemplo acima, as operações que definem o espaço vetorial W sobre K são as operações de adição e multiplicação do corpo W. Deste modo, para todo $\lambda \in K$ e $u \in W$, a multiplicação por escalar λu é a multiplicação dos elementos λ e u em W.

Definição 9. Seja W um espaço vetorial sobre K. Dizemos que um conjunto não vazio $S \subset W$ é um *subespaço vetorial* de W se $(r+s) \in S$ e $\lambda r \in S$, para todos $r, s \in S$ e $\lambda \in K$.

Sahai e Bist (2002) afirmam que, nas condições da definição anterior, o subconjunto $S \subset W$ é subespaço vetorial de W se S é espaço vetorial sobre K com as operações de W.

Exemplo 11. De forma geral, sendo W, S e K corpos tais que $W \supset S \supset K$, temos que S é subespaço vetorial de W, sendo W espaço vetorial sobre K.

Definição 10. Seja W espaço vetorial sobre o corpo K e $\{v_1, v_2, \cdots, v_t\} \subset W$. Chamamos de *combinação linear* dos vetores $v_1, v_2, \cdots, v_t$ a expressão

$$\sum_{i=1}^{t} a_i v_i$$

sendo $a_1, a_2, \cdots, a_t$ escalares em K.

Definição 11. Dizemos que um subespaço vetorial S de um espaço vetorial W sobre K é *gerado* pelos vetores $v_1, v_2, \cdots, v_t \in W$ se

$$S = \left\{ \sum_{i=1}^{t} a_i v_i / a_i \in K \right\}$$

Exemplo 12. Observa-se que o espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$ é gerado pelos vetores $1, i \in \mathbb{C}$ em combinação linear com escalares $a, b \in \mathbb{R}$ pois $\mathbb{C} = \{a + bi / a, b \in \mathbb{R}\}$.

Definição 12. Seja W espaço vetorial sobre o corpo K e $v_1, v_2, \cdots, v_t \in W$. Dizemos que $\{v_1, v_2, \cdots, v_t\}$ é um conjunto de vetores *linearmente independentes* se toda vez que existirem escalares $a_1, a_2, \cdots, a_t \in K$ tais que $a_1 v_1 + a_2 v_2 + \cdots + a_t v_t = 0$, então $a_i = 0$ para $i = 1, 2, \cdots, t$.

Caso os vetores $v_1, v_2, \cdots, v_t \in W$ não sejam linearmente independentes, dizemos que são *linearmente dependentes*.

Definição 13. Seja W espaço vetorial sobre K e $\{v_1, v_2, \cdots, v_t\} \subset W$. Dizemos que o conjunto de vetores $\{v_1, v_2, \cdots, v_t\}$ é uma *base* do espaço vetorial W sobre K se estes vetores são linearmente independentes e geram W.

É importante observar que sendo $\{v_1, v_2, \cdots, v_t\} \subset W$ uma base do espaço vetorial W sobre K, para todo elemento $u \in W$ existem escalares $a_1, a_2, \cdots, a_t \in K$ únicos tais que $u = a_1v_1 + a_2v_2 + \cdots + a_tv_t$. Ainda, Winterle e Steinbruch (1987) afirmam que nestas condições todo subconjunto de W com mais de t vetores será linearmente dependente.

Definição 14. Se o espaço vetorial W sobre K possui uma base com t elementos, dizemos que t é a *dimensão* do espaço vetorial W sobre K e indicamos $[W : K] = t$.

Nas condições da definição acima, se o número de vetores que formam uma base do espaço vetorial W sobre K é finito, dizemos que W é um espaço vetorial de *dimensão finita* sobre K.

Exemplo 13. Temos que $\{1, i\}$ é uma base do espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$ e consequentemente $[\mathbb{C} : \mathbb{R}] = 2$.

Definição 15. Dois espaços vetoriais L e L' sobre K são *isomorfos* se existir uma bijeção $f : L \to L'$ tal que $f(u + v) = f(u) + f(v)$ e $f(\lambda u) = \lambda f(u)$ para todos $u, v \in L$ e $\lambda \in K$.

Exemplo 14. Sendo L, L' e K corpos tais que $L, L' \supset K$ e $f : L \to L'$ um K-isomorfismo, temos que f é isomorfismo dos espaços vetoriais L e L' sobre K. De fato, pela Definição 5, vem que $f(u + v) = f(u) + f(v)$ para todos $u, v \in L$, e para todo $\lambda \in K$ temos que $f(\lambda u) = f(\lambda)f(u) = \lambda f(u)$, pois f é função identidade para todo $\lambda \in K$.

Teorema 4. Sejam L, L' corpos e espaços vetoriais de dimensão finita sobre o corpo K. Então L e L' são isomorfos se, e somente se, $[L : K] = [L' : K]$.

Demonstração. A fim de não nos extendermos demasiadamente, demonstraremos somente a ida deste teorema. Uma demonstração completa pode ser encontrada em Sahai e Bist (2002). Seja $\{u_1, u_2, \cdots, u_t\} \subset L$ uma base do espaço vetorial L sobre K e $f : L \to$

L' isomorfismo. Mostraremos que $\{f(u_1), f(u_2), \cdots, f(u_t)\} \subset L'$ é uma base do espaço vetorial L' sobre K. Mostraremos primeiro que os vetores $f(u_1), f(u_2), \cdots, f(u_t)$ são linearmente independentes. De fato, sendo $a_1, a_2, \cdots, a_t \in K$ tais que

$$a_1 f(u_1) + a_2 f(u_2) + \cdots + a_t f(u_t) = 0$$

como $f : L \to L'$ é isomorfismo de espaços vetoriais, pela Definição 15 temos que

$$f(a_1 u_1 + a_2 u_2 + \cdots + a_t u_t) = 0$$

e como f é bijetiva e $f(0) = 0$, vem que $a_1 u_1 + a_2 u_2 + \cdots + a_t u_t = 0$. Sendo $\{u_1, u_2, \cdots, u_t\}$ uma base do espaço vetorial L sobre K, temos que estes vetores são linearmente independentes e, portanto, $a_i = 0$ para $i = 1, 2, \cdots, t$. Segue que $\{f(u_1), f(u_2), \cdots, f(u_t)\}$ é linearmente independente.

Mostremos agora que $\{f(u_1), f(u_2), \cdots, f(u_t)\}$ gera L'. Devemos mostrar que todo vetor $v \in L'$ pode ser escrito como uma combinação linear de $f(u_1), \cdots, f(u_t)$ com escalares em K. De fato, como f é sobrejetiva, para todo $v \in L'$ existe $u \in L$ tal que $f(u) = v$. Sendo L um espaço vetorial sobre K, sabemos que para todo vetor $u \in L$ existem $b_1, b_2, \cdots, b_t \in K$ tais que

$$u = b_1 u_1 + b_2 u_2 + \cdots + b_t u_t$$

Logo, temos que

$$v = f(u) = f\left(\sum_{i=1}^{t} b_i u_i\right) = \sum_{i=1}^{t} f(b_i) f(u_i) = \sum_{i=1}^{t} b_i f(u_i)$$

e assim $\{f(u_1), f(u_2), \cdots, f(u_t)\}$ gera L', sendo uma base do espaço vetorial L' sobre K. Como f é injetiva, temos que as bases $\{u_1, u_2, \cdots, u_t\}$ e $\{f(u_1), f(u_2), \cdots, f(u_t)\}$ têm o mesmo número de vetores e portanto $[L : K] = [L' : K]$.

Capítulo 2

Polinômios em uma Indeterminada

Neste capítulo faremos um estudo geral da teoria de polinômios em uma indeterminada x. É importante observar que no contexto de nosso trabalho consideraremos L, K e M corpos.

2.1 Apresentação Geral de Polinômios

Definição 16. Um polinômio sobre K em uma indeterminada x é uma expressão formal do tipo $f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ com $a_i \in K$ para todo $i \in \mathbb{N}$ e existe $n \in \mathbb{N}$ tal que $a_t = 0$ para todo $t \geq n$.

Aos elementos $a_i \in K$ chamamos *coeficientes* do polinômio $f(x)$ e denotamos por $K[x]$ o conjunto de todos os polinômios com coeficientes em K.

Dados dois polinômios $f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots \in K[x]$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m + \cdots \in K[x]$ dizemos que $f(x)$ e $g(x)$ são iguais se, e somente se, $a_i = b_i$ para todo $i \in \mathbb{N}$.

Um polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ sobre K é dito *identicamente nulo* se, e somente se, $a_i = 0$ para todo $i \in \mathbb{N}$. Se $a_i = 0$ para todo $i \geq 1$, temos que $f(x) = a_0$, sendo $a_0 \in K$, e chamamos $f(x)$ de *polinômio constante* a_0.

Sendo $f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ um polinômio sobre K tal que $a_n \neq 0$ e $a_t = 0$ para todo $t > n$, dizemos que n é o *grau do polinômio* $f(x)$ e indicamos

$\partial f(x) = n$. Neste caso podemos simplesmente representar o polinômio $f(x)$ por $f(x) = a_0 + a_1x + \cdots + a_nx^n$. De acordo com Gonçalves (1979), o grau do polinômio $f(x) = 0$ é indefinido[1].

Sendo $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio sobre K de grau n, dizemos que a_n é o *coeficiente dominante* de $f(x)$. Se $a_n = 1$ dizemos que $f(x)$ é um *polinômio mônico*.

Sejam $f(x) = a_0 + a_1x + \cdots + a_rx^r + \cdots$ e $g(x) = b_0 + b_1x + \cdots + b_sx^s + \cdots$ polinômios sobre K. Definimos as seguintes operações de *adição* e *multiplicação* sobre o conjunto $K[x]$:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k + \cdots$$

e

$$f(x)g(x) = c_0 + c_1x + \cdots + c_kx^k + \cdots$$

sendo $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$ e de forma geral $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0$. Explicitamente, para um polinômio $f(x)$ de grau r e um polinômio $g(x)$ de grau s, supondo $r \geq s$ temos:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_r + b_r)x^r$$

Observe que considerando $r > s$ temos $b_t = 0$ para $s + 1 \leq t \leq r$. Com relação ao produto, temos:

$$f(x)g(x) = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_rb_sx^{r+s}$$

e como apontado por Gonçalves (1979), a definição do produto é proveniente da regra $x^nx^m = x^{n+m}$.

Teorema 5. $K[x]$ é domínio de integridade com as operações de adição e multiplicação de polinômios definidas acima, sendo $f(x) = 0$ o elemento neutro aditivo e $f(x) = 1$ a unidade de $K[x]$.

[1] Grillet (2007) também define grau somente para polinômios não nulos.

Monteiro (1969) aponta o processo formal[2] de construção do anel de polinômios em uma indeterminada. Uma construção similar também pode ser encontrada em Hungerford (1974). Ainda, através do polinômio constante $f(x) = a_0$ podemos observar a inclusão $K \subset K[x]$.

Uma vez definidas as operações de adição e multiplicação de polinômios, podemos observar as seguintes propriedades com relação ao grau da soma e do produto de polinômios:

Teorema 6. Sejam K corpo e $f(x), g(x)$ polinômios não nulos sobre K. Então $\partial(f(x) + g(x)) \leq max\{\partial f(x), \partial g(x)\}$ se $f(x) + g(x) \neq 0$, e $\partial(f(x)g(x)) = \partial f(x) + \partial g(x)$.

2.2 Divisibilidade em $K[x]$

Seguiremos agora com algumas noções de divisibilidade em $K[x]$ necessárias ao nosso trabalho.

Definição 17. Sejam K corpo e $f(x), g(x) \in K[x]$. Diz-se que o polinômio não nulo $f(x)$ *divide* o polinômio $g(x)$ em $K[x]$, e indica-se $f(x)|g(x)$, se existir um polinômio $h(x) \in K[x]$ tal que $f(x)h(x) = g(x)$.

Neste caso, dizemos também que o polinômio $f(x)$ é um *divisor* de $g(x)$. Domingues e Iezzi (2003) denominam tal divisão de *divisão exata*. Os mesmos autores apontam que, com as notações da definição acima, se $f(x)|g(x)$ então consequentemente $\partial f(x) \leq \partial g(x)$.

Teorema 7. (Algoritmo da Divisão) Sejam K corpo e $f(x), g(x) \in K[x]$, com $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in K[x]$ tais que $f(x) = q(x)g(x) + r(x)$, sendo $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Exemplo 15. Com as notações do teorema acima, para $f(x) = x^3 - 2x^2 + 1$ e $g(x) = x^2 + 2$, temos $q(x) = x - 2$ e $r(x) = -2x + 5$.

[2] Neste tipo formal de construção, Monteiro (1969) define *polinômio* com coeficientes em um anel A comutativo com unidade como uma sucessão de elementos $(a_i \in A)$, sendo $a_i \neq 0$ somente para um número finito de índices $i \in \mathbb{N}$.

Nas condições do teorema anterior, os polinômios $q(x)$ e $r(x)$ são denominados respectivamente *quociente* e *resto* da divisão de $f(x)$ por $g(x)$. A demonstração deste teorema pode ser encontrada em Monteiro (1969)[3] e Gonçalves (1979). Prosseguiremos adiante com o estudo das *raízes* de um polinômio $f(x) \in K[x]$ e sua existência em um corpo $L \supset K$.

2.3 Raízes de um Polinômio

Definição 18. Sejam K corpo e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ um polinômio não nulo. Diz-se que $\alpha \in L \supset K$ é uma *raiz* de $f(x)$ se $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$.

Teorema 8. Sejam K corpo e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ um polinômio não nulo de grau n. Então o número de raízes de $f(x)$ em K é no máximo igual ao $\partial f(x)$.

Demonstração. Se o polinômio $f(x) \in K[x]$ não possui raízes quaisquer no corpo K segue que o teorema está imediatamente demonstrado.

Seja $\alpha \in K$ uma raiz de $f(x)$. Pelo Algoritmo da Divisão, existem únicos $q(x), r(x) \in K[x]$ tais que $f(x) = (x-\alpha)q(x)+r(x)$, sendo $r(x) = 0$ ou $\partial r(x) < 1$. Suponhamos então $r(x) = b_0$ e assim $f(x) = (x-\alpha)q(x)+b_0$. Segue que $f(\alpha) = (\alpha-\alpha)q(\alpha)+b_0$ e portanto $b_0 = 0$. Consequentemente $r(x) = 0$ e $f(x) = (x-\alpha)q(x)$. Agora, pelo Teorema 6 temos que $\partial f(x) = 1 + \partial q(x)$ e assim $\partial q(x) = n-1$. Se $\beta \in K$ é uma raiz de $f(x)$, temos que $f(\beta) = (\beta-\alpha)q(\beta) = 0$. Como K é um anel sem divisores de zero segue que $\beta = \alpha$ ou $q(\beta) = 0$. Logo as raízes de $f(x)$ são α e também as raízes de $q(x)$.

Façamos agora indução sobre $\partial f(x) = n$. Para $n = 0$ segue que $f(x)$ não possui raízes em K e neste caso não há o que demonstrar. Supondo que a hipótese é válida para $q(x)$, como $\partial q(x) = n-1$, segue que $q(x)$ possui no máximo $n-1$ raízes em K. Sendo $f(x) = (x-\alpha)q(x)$ e as raízes de $q(x)$ também raízes de $f(x)$, como $q(x)$ possui no máximo $n-1$ raízes em K e α é raiz de $f(x)$, segue portanto que $f(x)$ possui no máximo n raízes em K.

Corolário 1. Sejam K corpo e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ um polinômio não nulo de grau n. Então o número de raízes de $f(x)$ em qualquer corpo $L \supset K$ é no

[3] Ver ainda neste autor um estudo detalhado sobre anéis euclidianos, a partir da página 359.

máximo igual a $\partial f(x) = n$.

Demonstração. Se $f(x) \in K[x]$ e $L \supset K$, segue que $f(x) \in L[x]$. Assim, aplicando o teorema anterior, temos que $f(x)$ possui no máximo n raízes no corpo L.

Definição 19. Seja K corpo. Dizemos que K é *algebricamente fechado* se para todo polinômio não constante $f(x) \in K[x]$ existir algum elemento $\alpha \in K$ tal que $f(\alpha) = 0$.

Em outras palavras, K é um corpo algebricamente fechado se todo polinômio de grau $n \geq 1$ com coeficientes em K possuir ao menos uma raiz em K.

Teorema 9. (Teorema Fundamental da Álgebra) O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado.

A demonstração do Teorema Fundamental da Álgebra está além das delimitações teóricas deste trabalho, podendo ser encontrada em Monteiro (1969) e Waerden (1985). Para um estudo mais aprofundado, Fine e Rosenberger (1997) dedicam um livro completo a este teorema.

Teorema 10. Sejam $K \subset \mathbb{C}$ e $f(x) \in K[x]$ um polinômio de grau $n \in \mathbb{N}^*$ com raízes distintas $\alpha_1, \alpha_2, \cdots, \alpha_t \in \mathbb{C}$. Então $f(x)$ pode ser decomposto da forma

$$f(x) = c(x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \cdots (x - \alpha_t)^{m_t} \in \mathbb{C}[x]$$

sendo $c \in K$ e m_i um inteiro positivo.

Nas condições do teorema acima, chamamos o inteiro positivo m_i de *multiplicidade* da raiz α_i. Se $m_i = 1$ dizemos que α_i é *raiz simples* de $f(x)$. Observe que nas condições do teorema acima temos $n = m_1 + m_2 + \cdots + m_t$, pelo Teorema 6.

Exemplo 16. O polinômio $f(x) = x^5 - 8x^4 + 25x^3 - 38x^2 + 28x - 8$ possui raízes $\alpha_1 = 1$ e $\alpha_2 = 2$ de multiplicidade 2 e 3, respectivamente, pois pode ser escrito da forma $f(x) = (x - 1)^2(x - 2)^3$.

2.4 Polinômios Irredutíveis

Apresentaremos agora noções sobre um tipo particular de polinômios sobre K, os quais denominamos *polinômios irredutíveis*, que representam no anel $K[x]$ algo análogo ao que os números primos representam no anel $\mathbb{Z}$.

Definição 20. Sejam K corpo e $f(x) \in K[x]$ um polinômio de grau $n \geq 1$. Dizemos que $f(x)$ é *irredutível* sobre K se sempre que existirem $g(x), h(x) \in K[x]$ tais que $f(x) = g(x)h(x)$ então $g(x) = a$ ou $h(x) = b$.

Também dizemos nas condições da definição acima que $f(x)$ é irredutível *em* $K[x]$. Se $f(x)$ não é polinômio irredutível sobre K dizemos que $f(x)$ é *redutível* sobre K. Repare que nas condições da definição acima um polinômio pode ser irredutível sobre K mas redutível em algum corpo $L \supset K$. Ainda, se $f(x) \in K[x]$ é redutível sobre um corpo K e $M \supset K$, então $f(x)$ é redutível sobre M.

Exemplo 17. O polinômio $f(x) = x^2 + 2$ é irredutível sobre $\mathbb{Q}$ e $\mathbb{R}$, mas redutível sobre $\mathbb{C}$ pois $f(x) = (x - \sqrt{2}i)(x + \sqrt{2}i)$.

Exemplo 18. O polinômio $f(x) = x^4 + 4$ é redutível sobre $\mathbb{Q}$ pois pode ser escrito da forma $f(x) = (x^2 - 2x + 2)(x^2 + 2x + 2)$.

Exemplo 19. Pelo Teorema Fundamental da Álgebra e de acordo com o Teorema 10, observamos que todo polinômio $f(x)$ de grau $n > 1$ sobre $K \subset \mathbb{C}$ é redutível sobre $\mathbb{C}$.

Teorema 11. Sejam K corpo e $f(x) \in K[x]$ um polinômio não constante. Então existem $f_1(x), f_2(x), \cdots, f_r(x) \in K[x]$ irredutíveis sobre K (não necessariamente distintos) tais que $f(x)$ pode ser escrito na forma

$$f(x) = f_1(x)f_2(x)\cdots f_r(x)$$

sendo esta forma única a menos da ordem dos fatores.

De acordo com o teorema acima, todo polinômio não constante $f(x) \in K[x]$ pode ser escrito, portanto, de forma única (a menos da ordem dos fatores) como $f(x) = f_1(x)^{m_1} f_2(x)^{m_2} \cdots f_t(x)^{m_t}$, sendo os polinômios $f_i(x) \in K[x]$ irredutíveis sobre K e distintos dois a dois.

Conrad (2020b) aponta que, nas condições do teorema acima, se existem $f_i(x) \in K[x]$ e $p_j(x) \in K[x]$ irredutíveis sobre K tais que $f(x) = f_1(x)f_2(x)\cdots f_r(x)$ e também $f(x) = p_1(x)p_2(x)\cdots p_s(x)$ então $r = s$, isto é, o número de fatores todos irredutíveis na decomposição de $f(x)$ é invariável. Ainda, nestas condições $p_i(x) = c_i f_i(x)$, sendo $c_i \in K^*$.

2.5 Irredutibilidade sobre $\mathbb{Q}$

Apresentaremos agora noções sobre irredutibilidade de polinômios sobre o corpo $\mathbb{Q}$. Sempre que mencionarmos que um polinômio $f(x)$ é redutível (ou irredutível) simplesmente, sem especificar sobre qual corpo, subentende-se que $f(x)$ é redutível (ou irredutível) sobre $\mathbb{Q}$. Em especial, mostraremos um critério que nos dá condições para verificarmos a irredutibilidade de um polinômio sobre este corpo, denominado *Critério de Eisenstein*.

Teorema 12. (Gauss) Seja $f(x) \in \mathbb{Z}[x]$ um polinômio irredutível sobre $\mathbb{Z}$. Então $f(x)$ é irredutível sobre $\mathbb{Q}$.

A demonstração do resultado acima pode ser encontrada em Gonçalves (1979).

Teorema 13. (Critério de Eisenstein) Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Se existe um primo p tal que:

1. $p|a_0, a_1, \cdots, a_{n-1}$
2. $p \nmid a_n$
3. $p^2 \nmid a_0$

Então $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 20. Verifica-se que o polinômio $f(x) = 7x^3 + 12x^2 + 9x + 3$ é irredutível sobre $\mathbb{Q}$ utilizando o Critério de Eisenstein para $p = 3$.

Exemplo 21. Todos os polinômios da forma $f(x) = x^p - q$, com p, q primos positivos, são irredutíveis sobre $\mathbb{Q}$ utilizando o Critério de Eisenstein considerando o próprio primo q.

Apesar do Critério de Eisenstein ser útil para a verificação da irredutibilidade de polinômios sobre $\mathbb{Q}$, é possível ainda a existência de polinômios $f(x) \in \mathbb{Q}[x]$, irredutíveis sobre $\mathbb{Q}$, para os quais não conseguimos aplicar o Critério de Eisenstein. Um tipo de polinômio que ilustra esta situação, que veremos adiante, é o *polinômio ciclotômico* de grau $p-1$, sendo p primo.

Definição 21. Chama-se *polinômio ciclotômico* de grau $n-1$ o polinômio $f(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$.

Observe que o polinômio ciclotômico $f(x)$ de grau $n-1$ pode ser obtido a partir da seguinte divisão

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

e portanto suas raízes são todos números distintos $\zeta \in \mathbb{C}$ tais que $\zeta^n = 1$ e $\zeta \neq 1$. Observe que essas raízes serão da forma $u, u^2, \cdots, u^{n-1}$, sendo $u = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$. Mostraremos agora que o polinômio ciclotômico $f(x)$ de grau $p-1$ é irredutível sobre $\mathbb{Q}$, e para isso precisaremos do seguinte resultado:

Teorema 14. Seja $f(x) \in \mathbb{Q}[x]$ um polinômio de grau $n \geq 1$ e $a \in \mathbb{Q}$. Então $f(x)$ é irredutível sobre $\mathbb{Q}$ se, e somente se, $f(x+a)$ for irredutível sobre $\mathbb{Q}$.

Teorema 15. Seja p um número primo. Então o polinômio ciclotômico $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ é irredutível sobre $\mathbb{Q}$.

Demonstração. Pelo Teorema 14, nos é suficiente mostrar que $f(x+1)$ é irredutível sobre $\mathbb{Q}$. De fato, podemos observar que

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{\binom{p}{p} x^p + \binom{p}{p-1} x^{p-1} + \cdots + \binom{p}{1} x + \binom{p}{0} x^0 - 1}{x}$$

Ou seja

$$f(x+1) = x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{1}$$

Como p divide o binômio $\binom{p}{k}$ para $1 \leq k \leq p-1$, considerando o Critério de Eisenstein para o próprio primo p, segue que $f(x+1)$ é irredutível sobre $\mathbb{Q}$. Portanto $f(x)$ é irredutível sobre $\mathbb{Q}$.

Capítulo 3

Extensões Algébricas de Corpos

Neste capítulo faremos o estudo de extensões algébricas de corpos. É importante observar que todos os anéis L e K trabalhados neste capítulo são subcorpos de $\mathbb{C}$. Primeiramente, apresentaremos o *corpo de decomposição* de um polinômio não nulo $f(x) \in K[x]$. Em seguida, apresentaremos a definição formal de extensão e prosseguiremos com nosso estudo das extensões algébricas no contexto da álgebra linear.

3.1 Processo de Adjunção de Raízes

Definição 22. Sejam K corpo e $\alpha \in L \supset K$. Definimos $K[\alpha] = \{f(\alpha)/f(x) \in K[x]\}$.

Nas condições da definição acima, como apontado por Gonçalves (1979), $K[\alpha]$ é um subdomínio de L contendo K.

Teorema 16. Sejam K corpo e $\alpha \in L \supset K$ raiz de um polinômio não nulo $f(x) \in K[x]$. Então $K[\alpha]$ é subcorpo de L contendo K.

Exemplo 22. Podemos através do Algoritmo da Divisão mostrar que $\mathbb{R}[i] = \mathbb{C}$. Pela definição acima, temos que $\mathbb{R}[i] = \{f(i)/f(x) \in \mathbb{R}[x]\}$. Considerando $f(x) \in \mathbb{R}[x]$ temos que existem $q(x), r(x) \in \mathbb{R}[x]$ tais que $f(x) = (x^2 + 1)q(x) + r(x)$, sendo $r(x) = 0$ ou $\partial r(x) < 2$. Considerando $r(x) = a + bx$, com $a, b \in \mathbb{R}$, temos $f(i) = (i^2 + 1)q(i) + r(i) = 0 + r(i) = a + bi$ e, portanto, $\mathbb{R}[i] = \{a + bi/a, b \in \mathbb{R}\} = \mathbb{C}$.

Exemplo 23. Sendo p primo positivo, por um processo análogo ao do exemplo anterior demonstra-se que $\mathbb{Q}[\sqrt{p}] = \left\{a + b\sqrt{p}/a, b \in \mathbb{Q}\right\}$.

Considere K um subcorpo de $\mathbb{C}$ e $f(x) \in K[x]$ um polinômio não nulo com raízes distintas $\alpha_1, \alpha_2, \cdots, \alpha_t$. Pelo Teorema Fundamental da Álgebra, $\mathbb{C}$ é um corpo algebricamente fechado e consequentemente todas as raízes de $f(x)$ estão em $\mathbb{C}$.

Definição 23. Sejam $L \subset \mathbb{C}$ corpo e $f(x) \in K[x]$ um polinômio com raízes distintas $\alpha_1, \alpha_2, \cdots, \alpha_t$. Dizemos que L é *corpo de decomposição* de $f(x)$, e denotamos $L = Gal(f(x), K)$, se $L \supset K$ e

1. $f(x)$ se decompõe sobre L da forma $f(x) = c(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_t)^{m_t}$, sendo $c \in K$, $\alpha_1, \alpha_2, \cdots, \alpha_t \in L$ e m_i inteiro positivo multiplicidade da raiz α_i.

2. Se existir um corpo L' tal que $L \supset L' \supset K$, então $L = L'$.

Nestas condições, construímos o corpo $Gal(f(x), K)$ através do *processo de adjunção de raízes*. Considerando as seguintes inclusões

$$K \subset K_1 = K[\alpha_1] \subset K_2 = K_1[\alpha_2] \subset \cdots \subset K_{t-1}[\alpha_t] = K_t$$

temos que $Gal(f(x), K) = K_t = K[\alpha_1, \alpha_2, \cdots, \alpha_t]$ é o corpo de decomposição do polinômio $f(x) \in K[x]$. Observe que nem sempre é necessário t etapas para construirmos o corpo de decomposição de $f(x)$. Considerando, por exemplo, o polinômio $f(x) = x^2 + 1$, temos que $Gal(f(x), \mathbb{Q}) = \mathbb{Q}[i, -i] = \mathbb{Q}[i]$, isto é, as duas raízes distintas de $f(x)$ foram obtidas em somente uma única etapa.

Teorema 17. Sejam $K \subset \mathbb{C}$ corpo e $f(x) \in K[x]$ um polinômio de grau $n \in \mathbb{N}^*$. Então:

1. Existe $Gal(f(x), K)$.

2. Se $L, L' \supset K$ são corpos de decomposição de $f(x)$, existe um K-isomorfismo $\sigma : L \to L'$.

As demonstrações dos itens 1 e 2 deste teorema podem ser encontradas em Lang (2005). E como apontado por Gonçalves (1979), $Gal(f(x), K)$ é a intersecção de todos os subcorpos de $\mathbb{C}$ contendo K e todas as raízes de $f(x)$. Podemos observar que este corpo existe pois, como observado por Grillet (2007), Dummit e Foote (1991), a intersecção de subcorpos de $\mathbb{C}$ é, por sua vez, subcorpo de $\mathbb{C}$.

Exemplo 24. Se todas as distintas raízes $\alpha_1, \alpha_2, \cdots, \alpha_t$ de $f(x) \in K[x]$ estão em K, decorre que $Gal(f(x), K) = K[\alpha_1, \alpha_2, \cdots, \alpha_t] = K$.

Exemplo 25. Considerando o polinômio $x^n - 1$ e suas raízes distintas $1, u, u^2, \cdots, u^{n-1}$, temos que $Gal(x^n - 1, \mathbb{Q}) = \mathbb{Q}[u]$, sendo $u = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$.

Exemplo 26. Sendo p, q primos positivos, pelo Critério de Eisenstein temos que $f(x) = x^p - q$ é irredutível, considerando o primo q. Sendo $\theta = \sqrt[p]{q} \in \mathbb{R}$ e $u = cos\left(\frac{2\pi}{p}\right) + isen\left(\frac{2\pi}{p}\right)$, temos que $\theta, \theta u, \cdots, \theta u^{p-1}$ são as raízes de $f(x)$ e $Gal(f(x), \mathbb{Q}) = \mathbb{Q}[\theta, \theta u, \cdots, \theta u^{p-1}] = \mathbb{Q}[\theta, u]$.

Exemplo 27. Considerando o polinômio $f(x) = x^8 - 2$, observamos que suas raízes são $\sqrt[8]{2}\left(cos\left(\frac{2k\pi}{8}\right) + isen\left(\frac{2k\pi}{8}\right)\right)$, com $k \in \mathbb{Z}$ tal que $0 \leq k \leq 7$. Assim temos que $Gal(f(x), \mathbb{Q}) = \mathbb{Q}[\sqrt[8]{2}, i]$.

3.2 Extensões de Corpos

Definição 24. Dizemos que o corpo L é uma *extensão* do corpo K quando K é subcorpo de L.

Quando já está entendido que L e K são corpos, expressamos que L é uma extensão de K somente pela inclusão $L \supset K$. Sendo $L \supset M \supset K$ extensões, usaremos por vezes o seguinte diagrama para ilustrar[1] que L é extensão de M que, por sua vez, é extensão de K.

$$\begin{array}{c} L \\ | \\ M \\ | \\ K \end{array}$$

Exemplo 28. Sendo K corpo é imediato que $K \supset K$ e, portanto, K é uma extensão de si mesmo.

Exemplo 29. Temos que $\mathbb{C}$ é extensão de $\mathbb{R}$ que, por sua vez, é extensão de $\mathbb{Q}$, pois $\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q}$.

[1] Dummit e Foote (1991) utilizam a mesma notação. Lorenz (2006) também a utiliza em sua exposição sobre extensões.

Definição 25. Sejam K corpo e $L \supset K$ uma extensão de K. Dizemos que um elemento $\alpha \in L$ é *algébrico* sobre K se existir algum polinômio não nulo $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Caso contrário dizemos que α é *transcendente*[2] sobre K.

Nestas condições, é imediato que todo elemento $a \in K$ é algébrico sobre K através do polinômio $f(x) = x - a \in K[x]$. Repare que sendo $L \supset M \supset K$ extensões, se $\alpha \in L$ é algébrico sobre K então α é algébrico sobre M.

Exemplo 30. Todas as raízes $\alpha_1, \alpha_2, \cdots, \alpha_t \in \mathbb{C} \supset K$ do polinômio $f(x) \in K[x]$ são elementos algébricos sobre K.

Exemplo 31. O elemento $i \in \mathbb{C}$ é algébrico sobre $\mathbb{R}$ pois, considerando o polinômio $f(x) = x^2 + 1$, temos que $f(i) = 0$.

Exemplo 32. Sendo p um primo positivo, temos que $\sqrt{p}$ é algébrico sobre $\mathbb{Q}$ pois, para $f(x) = x^2 - p$, temos $f(\sqrt{p}) = 0$.

Definição 26. Sejam K corpo, $L \supset K$ extensão de K e $\alpha \in L$ algébrico sobre K. O *polinômio mínimo* de α sobre K, denotado por $irr(\alpha, K)$, é o polinômio mônico, de menor grau, irredutível em $K[x]$, que tem α como raiz.

Como apontado por Gonçalves (1979), nestas condições, o polinômio $irr(\alpha, K)$ é único. Uma demonstração da existência e unicidade do polinômio $irr(\alpha, K)$ pode ser encontrada em Fine e Rosenberger (2007).

Exemplo 33. Como todos os polinômios $f(x) = x - a \in K[x]$ são irredutíveis em $K[x]$, segue que $irr(a, K) = x - a$ para todo $a \in K$.

Exemplo 34. Considerando $a + bi \in \mathbb{C}$, temos que $irr(a + bi, \mathbb{R}) = x^2 - 2ax + (a^2 + b^2)$. Para $a = 0$ e $b = 1$, segue que $irr(i, \mathbb{R}) = x^2 + 1$.

Teorema 18. Se α é um elemento algébrico sobre K e $f(x) \in K[x]$ é um polinômio não nulo tal que $f(\alpha) = 0$, então $irr(\alpha, K) | f(x)$.

[2]Os elementos transcendentes sobre um corpo K não são objetos de estudo em nosso trabalho. Para um estudo mais aprofundado sobre estes elementos consultar Parshin e Shafarevich (1997).

O teorema acima é enunciado como um corolário por Fine e Rosenberger (2007). Podemos observar que se $\alpha \in K$ é raiz de $f(x) \in K[x]$, então $irr(\alpha, K) = x - \alpha$ divide $f(x)$. Este resultado, por sua vez, é enunciado como teorema por Iezzi (1977).

Teorema 19. Sejam K corpo e $f(x) \in K[x]$ um polinômio de grau $n \in \mathbb{N}^*$. Se $f(x)$ é irredutível sobre K então todas suas raízes são simples.

A demonstração do teorema acima pode ser encontrada em Gonçalves (1979). Segue imediatamente que todas as raízes de $irr(\alpha, K)$ são simples.

Definição 27. Dizemos que uma extensão L de um corpo K é uma *extensão algébrica* se todo elemento $\alpha \in L$ for algébrico sobre K.

Exemplo 35. Sendo K corpo, temos que $K \supset K$ é uma extensão algébrica de si mesmo, pois para todo elemento $a \in K$ basta considerar o polinômio $f(x) = x - a \in K[x]$.

Exemplo 36. A extensão $\mathbb{C} \supset \mathbb{R}$ é uma extensão algébrica visto que todo elemento $a + bi \in \mathbb{C}$ é algébrico sobre $\mathbb{R}$ através do polinômio $f(x) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$.

Exemplo 37. A extensão $\mathbb{Q}[i] = \{a + bi/a, b \in \mathbb{Q}\}$ é uma extensão algébrica de $\mathbb{Q}$ por um polinômio de coeficientes racionais análogo ao do exemplo anterior.

Temos que toda extensão L de um corpo K pode ser entendida como um espaço vetorial L sobre K definidas as seguintes operações de adição e multiplicação por escalar:

$$+ : \begin{array}{c} L \times L \to L \\ (u, v) \to u + v \end{array} \qquad \cdot : \begin{array}{c} K \times L \to L \\ (\lambda, u) \to \lambda u \end{array}$$

Veremos adiante que os espaços vetoriais de dimensão finita se relacionam diretamente com as extensões algébricas.

Definição 28. Seja L uma extensão do corpo K. Dizemos que L é uma *extensão finita* de K se $[L : K] = n \in \mathbb{N}^*$.

Sendo $n \in \mathbb{N}^*$ a dimensão do espaço vetorial L sobre K, também dizemos que n é o *grau da extensão* $L \supset K$. De acordo com esta definição, dizemos que a extensão $L \supset K$ é finita quando o número de vetores que constituem uma base do espaço vetorial L sobre K é finito.

Exemplo 38. Sendo K corpo, temos que $K \supset K$ é uma extensão finita pois $[K : K] = 1$.

Exemplo 39. A extensão $\mathbb{C} \supset \mathbb{R}$ é uma extensão finita pois, sendo $\{1, i\}$ uma base do espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$, temos que $[\mathbb{C} : \mathbb{R}] = 2$.

Exemplo 40. De formal geral, sendo $\{\alpha_1, \alpha_2, \cdots, \alpha_n\} \subset L$ uma base do espaço vetorial L sobre K temos que

$$L = \left\{ \sum_{i=1}^{n} a_i \alpha_i / a_i \in K \right\}$$

é uma extensão finita de K e $[L : K] = n$.

Teorema 20. Seja L uma extensão do corpo K. Se $L \supset K$ é uma extensão finita, então $L \supset K$ é uma extensão algébrica.

Demonstração. Sendo $L \supset K$ uma extensão finita, considere $[L : K] = n \in \mathbb{N}^*$ e $\alpha \in L$ um elemento qualquer. Temos que o conjunto de vetores $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ é linearmente dependente pois caso contrário $[L : K] = n + 1$. Deste modo, existem $a_0, a_1, \cdots, a_n \in K$ não todos nulos tais que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Tomando $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, decorre que $f(x)$ é um polinômio não nulo e $f(\alpha) = 0$. Portanto todo elemento $\alpha \in L$ é algébrico sobre K e assim $L \supset K$ é uma extensão algébrica[3].

Teorema 21. Seja L uma extensão do corpo K. Sendo $\alpha \in L$ um elemento algébrico sobre K e $\partial irr(\alpha, K) = n$ então $[K[\alpha] : K] = n$ e $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base do espaço vetorial $K[\alpha]$ sobre K.

Demonstração. Utilizando um processo apontado por Hungerford (1974), considere o polinômio $f(x) = irr(\alpha, K)$, de grau $n \in \mathbb{N}^*$. Para todo polinômio $p(x) \in K[x]$, pelo Algoritmo da Divisão, existem $q(x), r(x) \in K[x]$ únicos tais que $p(x) = f(x)q(x) + r(x)$, sendo $r(x) = 0$ ou $\partial r(x) < \partial f(x) = n$. Considerando então $r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, temos que $p(\alpha) = f(\alpha)q(\alpha) + r(\alpha)$, isto é, $p(\alpha) = 0 \cdot q(\alpha) + r(\alpha)$. Portanto, todo elemento $p(\alpha) \in K[\alpha]$ pode ser escrito da forma

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

[3] Gonçalves (1979) e Hungerford (1974) demonstram o mesmo resultado de forma análoga. Entretando, é importante observar que a recíproca deste teorema não é verdade, pois é possível a existência de uma extensão algébrica infinita. Ver Gonçalves (1979) p.100 e Araujo (2009) p.134.

com $a_i \in K$. Logo, observamos que os vetores $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ geram o espaço vetorial $K[\alpha]$ sobre K. Para mostrar que $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base do espaço vetorial $K[\alpha]$ sobre K, nos falta somente mostrar que os vetores $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ são linearmente independentes. Se $r(\alpha) = 0$ vem que α é raiz de $r(x)$ e como $f(x) = irr(\alpha, K)$, pelo Teorema 18, segue que $f(x)|r(x)$. Sendo $\partial r(x) \leq n-1$ e $\partial f(x) = n$ temos que $r(x) = 0$, isto é, $a_i = 0$. Portanto $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é linearmente independente e uma base do espaço vetorial $K[\alpha]$ sobre K, sendo $[K[\alpha] : K] = n$.

Como consequência imediata, temos que se α é um elemento algébrico sobre K, então

$$K[\alpha] = \left\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} / a_i \in K\right\}$$

é uma extensão finita e algébrica.

Exemplo 41. Sendo $K \supset K$ uma extensão e $a \in K$, como $irr(a, K) = x - a$ decorre que $[K : K] = \partial(x - a) = 1$.

Exemplo 42. Podemos observar que $irr(i, \mathbb{R}) = x^2 + 1$. Considerando a extensão $\mathbb{R}[i] = \mathbb{C} \supset \mathbb{R}$ temos que $[\mathbb{C} : \mathbb{R}] = \partial(irr(i, \mathbb{R})) = 2$.

Exemplo 43. Sendo p, q números primos positivos, temos que $irr(\sqrt[p]{q}, \mathbb{Q}) = x^p - q$. Do teorema anterior temos que $[\mathbb{Q}[\sqrt[p]{q}] : \mathbb{Q}] = \partial(x^p - q) = p$. De fato, podemos observar que

$$\mathbb{Q}[\sqrt[p]{q}] = \left\{a_0 + a_1(\sqrt[p]{q}) + a_2(\sqrt[p]{q})^2 + \cdots + a_{p-1}(\sqrt[p]{q})^{p-1} / a_i \in \mathbb{Q}\right\}$$

é uma extensão algébrica de $\mathbb{Q}$ e um espaço vetorial sobre $\mathbb{Q}$, possuindo o conjunto de vetores $\left\{1, (\sqrt[p]{q}), (\sqrt[p]{q})^2, \cdots, (\sqrt[p]{q})^{p-1}\right\}$ como base.

Teorema 22. Sejam $L \supset H \supset K$ corpos tais que $L \supset H$ e $H \supset K$ são extensões finitas. Então $L \supset K$ é extensão finita e $[L : K] = [L : H] \cdot [H : K]$.

Demonstração. Sejam $L \supset H \supset K$ corpos tais que $[L : H] = m$ e $[H : K] = n$. Utilizando um processo apresentado por Dummit e Foote (1991), podemos observar que sendo $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ uma base do espaço vetorial L sobre H temos que todos os vetores $u \in L$ podem ser escritos da forma

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

com $a_i \in H$. Sendo $\{\beta_1, \beta_2, \cdots, \beta_n\}$ uma base do espaço vetorial H sobre K, temos que cada elemento $a_i \in H$ pode ser escrito como uma combinação linear dos vetores $\beta_1, \beta_2, \cdots, \beta_n$ com escalares em K. Assim, todo elemento $a_i \in H$ pode ser escrito da forma

$$a_i = b_{i1}\beta_1 + b_{i2}\beta_2 + \cdots + b_{in}\beta_n$$

com $b_{ij} \in K$. Portanto, todo vetor $u \in L$ pode ser escrito da forma

$$\sum_{\substack{i=1,2,3,\cdots,m \\ j=1,2,3,\cdots,n}} b_{ij}\beta_j\alpha_i$$

e nos resta agora somente mostrar que $\{\beta_j\alpha_i\}$ é um conjunto de vetores linearmente independente. De fato, considerando

$$\sum_{\substack{i=1,2,3,\cdots,m \\ j=1,2,3,\cdots,n}} b_{ij}\beta_j\alpha_i = 0$$

decorre que $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m = 0$. Como $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ é linearmente independente, temos neste caso que $a_i = 0$ para $i = 1, 2, 3 \cdots, m$. Mas sendo a_i um vetor de H, temos que $b_{i1}\beta_1 + b_{i2}\beta_2 + \cdots + b_{in}\beta_n = 0$. Como $\{\beta_1, \beta_2, \cdots, \beta_n\}$ é linearmente independente, segue que $b_{ij} = 0$ para $j = 1, 2, 3, \cdots, n$. Portanto $\{\beta_j\alpha_i\}$ é um conjunto de vetores linearmente independente e uma base do espaço vetorial L sobre K. Como $\{\beta_j\alpha_i\}$ tem mn elementos, segue que $[L : K] = [L : H] \cdot [H : K]$.

Exemplo 44. Temos que $\mathbb{Q}[\sqrt{5}, i] \supset \mathbb{Q}[i] \supset \mathbb{Q}$ são corpos tais que $\mathbb{Q}[\sqrt{5}, i] \supset \mathbb{Q}[i]$ e $\mathbb{Q}[i] \supset \mathbb{Q}$ são extensões finitas. Nas condições do teorema anterior temos que $\mathbb{Q}[\sqrt{5}, i] \supset \mathbb{Q}$ é finita e:

$$[\mathbb{Q}[\sqrt{5}, i] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{5}, i] : \mathbb{Q}[i]] \cdot [\mathbb{Q}[i] : \mathbb{Q}] = 2 \cdot 2 = 4$$

De fato, também podemos observar que $\left\{1, i, \sqrt{5}, \sqrt{5}i\right\}$ é uma base do espaço vetorial $\mathbb{Q}[\sqrt{5}, i]$ sobre $\mathbb{Q}$.

Exemplo 45. Temos que $\mathbb{Q}[\sqrt[8]{2}, i] \supset \mathbb{Q}[\sqrt[8]{2}] \supset \mathbb{Q}$ são extensões tais que $\mathbb{Q}[\sqrt[8]{2}, i] \supset \mathbb{Q}[\sqrt[8]{2}]$ e $\mathbb{Q}[\sqrt[8]{2}] \supset \mathbb{Q}$ são finitas. De acordo com o teorema anterior, temos que $\mathbb{Q}[\sqrt[8]{2}, i] \supset \mathbb{Q}$ é finita e

$$[\mathbb{Q}[\sqrt[8]{2}, i] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[8]{2}, i] : \mathbb{Q}[\sqrt[8]{2}]] \cdot [\mathbb{Q}[\sqrt[8]{2}] : \mathbb{Q}] = 2 \cdot 8 = 16$$

Exemplo 46. Sejam $p_1, p_2, \cdots, p_t$ primos distintos dois a dois e considere as seguintes extensões:

$$K_0 = \mathbb{Q} \subset K_1 = \mathbb{Q}[\sqrt{p_1}] \subset K_2 = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}] \subset \cdots \subset K_t = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_t}]$$

Temos que $[K_r : K_{r-1}] = 2$ pois $K_r = K_{r-1}[\sqrt{p_r}]$ e $\left\{1, \sqrt{p_r}\right\}$ é base do espaço vetorial K_r sobre K_{r-1}, para $r = 1, 2, \cdots, t$. Considerando as extensões $K_t \supset K_{t-1} \supset \cdots \supset K_1 \supset K_0$, nas condições do teorema anterior, temos que $K_t \supset K_0$ é finita e

$$[K_t : K_0] = [K_t : K_{t-1}] \cdot [K_{t-1} : K_{t-2}] \cdots [K_2 : K_1][K_1 : K_0] = 2^t$$

Portanto, $\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_t}] : \mathbb{Q}] = 2^t$.

Teorema 23. Sejam K corpo e $L \supset K$ uma extensão de K. Se $\sigma \in Aut_K^L$ e $f(x) \in K[x]$, então $\sigma(f(\alpha)) = f(\sigma(\alpha))$ para todo $\alpha \in L$. Em particular, se α é raiz de $f(x)$ então $\sigma(\alpha)$ também é raiz de $f(x)$.

Demonstração. Utilizando um processo apontado por Conrad (2020a), podemos observar que como $\alpha \in L$ e $L \supset K$, então $f(\alpha) \in L$ para todo $f(x) \in K[x]$. Sendo $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $\sigma : L \to L$ um K-automorfismo, temos que $\sigma(a_i) = a_i$ para todo $a_i \in K$, e

$$\sigma(f(\alpha)) = \sigma\left(\sum_{i=0}^{n} a_i\alpha^i\right) = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha)^i = \sum_{i=0}^{n} a_i\sigma(\alpha)^i = f(\sigma(\alpha))$$

Agora, se α é raiz de $f(x)$, então $f(\alpha) = 0$. Logo $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ e, portanto, $\sigma(\alpha)$ também é raiz de $f(x)$.

Teorema 24. Sejam $L \supset K \supset \mathbb{Q}$ extensões tais que $L \supset K$ seja uma extensão finita. Então, existe $u \in L$ tal que $L = K[u]$.

Não teremos ocasião para a demonstração do teorema citado acima. A mesma pode ser encontrada em Gonçalves (1979). Este teorema nos será necessário para a demonstração do corolário que segue:

Corolário 2. Seja $L \supset K \supset \mathbb{Q}$ extensões tais que $L \supset K$ seja finita. Temos então que $|Aut_K^L| \leq [L : K]$.

Demonstração. Sendo $L \supset K$ uma extensão finita, pelo teorema anterior, existe $u \in L$ tal que $L = K[u]$. Considere $f(x) = irr(u, K)$ e $\sigma \in Aut_K^L$. Pelo Teorema 23, temos que sendo $u \in L$ raiz de $f(x)$, então $\sigma(u) = u' \in L$ também será raiz de $f(x)$. Pelo Teorema 21, $[K[u'] : K] = \partial f(x) = [L : K]$, isto é, $K[u']$ e L são espaços vetoriais sobre K de mesma dimensão. Como $u' \in L$ e $L \supset K$, temos que $K[u'] \subset L$. Logo $L = K[u'] = K[u]$.

Sendo $\sigma : L \to L$ um K-automorfismo, pela Definição 7 temos que $\sigma(a) = a$ para todo $a \in K$. Logo, σ fica determinada pelo valor $\sigma(u) = u'$, isto é, pelas raízes de $f(x)$ que pertencem a L. Então $|Aut_K^L|$ é no máximo igual ao número de raízes de $f(x)$ em L. Pelo Corolário 1, o número de raízes de $f(x)$ na extensão $L \supset K$ é no máximo igual a $\partial f(x) = [L : K]$. Portanto $|Aut_K^L| \leq [L : K]$.

Capítulo 4

Isomorfismos entre Extensões Algébricas

4.1 Extensões Galoisianas e Extensões Normais

Com o propósito de demonstrar o principal teorema de nosso trabalho, o qual afirma que o número de automorfismos de uma extensão algébrica e finita $L \supset K$ que fixam o corpo K é igual à dimensão do espaço vetorial L sobre K, estabeleceremos aqui duas definições fundamentais: as definições de *extensão galoisiana* e *extensão normal*. É importante ressaltar que, ao longo deste capítulo, L e K são extensões tais que $\mathbb{C} \supset L \supset K \supset \mathbb{Q}$.

O conceito de normalidade de uma extensão $L \supset K$ se relaciona diretamente com o conceito de *separabilidade*. De acordo com Stewart (2004, p.107) : "Separabilidade é uma propriedade complementar a normalidade". Dizemos que um polinômio $f(x)$ é *separável* se todas suas raízes são simples em seu corpo de decomposição. Sendo K corpo e $L \supset K$, dizemos que um elemento $\alpha \in L$ é *separável sobre* K se α é algébrico sobre K e $irr(\alpha, K)$ é separável. A extensão $L \supset K$ é *separável sobre* K se todos os elementos de L são separáveis sobre K. Sendo $L \supset K$ uma extensão algébrica e $\mathbb{C} \supset L$, pelo Teorema 19 todas as raízes do polinômio $irr(\alpha, K)$ são simples. Logo $L \supset K$ é automaticamente separável e omitiremos o estudo da separabilidade para estas extensões [1].

Definição 29. Seja L uma extensão finita de K. Dizemos que $L \supset K$ é *galoisiana* se

[1] Para um estudo mais aprofundado do conceito de separabilidade consultar Dummit e Foote (1991) e Ribenboim (2001).

existir algum polinômio não nulo $f(x) \in K[x]$ tal que $L = Gal(f(x), K)$.

Decorre desta definição que a extensão finita $L \supset K$ é gailosiana se L é corpo de decomposição de algum polinômio $f(x) \in K[x]$. De forma geral, sendo $f(x) \in K[x]$ um polinômio com raízes distintas $\alpha_1, \alpha_2, \cdots, \alpha_t \in \mathbb{C}$ temos que $K[\alpha_1, \alpha_2, \cdots, \alpha_t] \supset K$ é uma extensão galoisiana.

Exemplo 47. Temos que $K \supset K$ é galoisiana, pois $Gal(x-a, K) = K[a] = K$, para todo $a \in K$.

Exemplo 48. Temos que $\mathbb{C} \supset \mathbb{R}$ é galoisiana, pois $Gal(x^2+1, \mathbb{R}) = \mathbb{R}[i] = \mathbb{C}$.

Exemplo 49. Temos que $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ é extensão galoisiana, pois $Gal(x^4 - 5x^2 + 6, \mathbb{Q}) = Gal((x^2-2)(x^2-3), \mathbb{Q}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Exemplo 50. Considere o polinômio $f(x) = x^3 - 5$ irredutível sobre $\mathbb{Q}$ (Eisenstein para $p = 5$). Temos que $\mathbb{Q}[\sqrt[3]{5}, u] \supset \mathbb{Q}$ é uma extensão galoisiana pois, de fato, $Gal(x^3 - 5, \mathbb{Q}) = \mathbb{Q}[\sqrt[3]{5}, u]$, sendo $u = \cos\left(\frac{2\pi}{3}\right) + isen\left(\frac{2\pi}{3}\right)$.

É importante observar que se $L \supset K$ é uma extensão galoisiana e existe um corpo H tal que $L \supset H \supset K$, então $L \supset H$ também é extensão galoisiana. Como apontado por Lang (2005), temos que todos os isomorfismos de L que fixam H são também isomorfismos de L que fixam K. Logo $Aut_H^L \supset Aut_K^L$ e através de um H-automorfismo $\sigma : L \to L$ temos que $L \supset H$ é isomorfo a $L \supset K$, isto é, L é galoisiana sobre H.

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ | & & | \\ H & & K \end{array}$$

Definição 30. Dizemos que uma extensão algébrica $L \supset K$ é *normal* se para todo polinômio $f(x) \in K[x]$, irredutível sobre K, $f(x)$ ter ao menos uma raiz em L implicar que $f(x)$ possui todas suas raízes complexas em L.

Logo, sendo $L \supset K$ uma extensão normal e $f(x) \in K[x]$ irredutível sobre K, sendo $\alpha_1, \alpha_2, \cdots, \alpha_t \in \mathbb{C}$ todas as raízes distintas de $f(x)$, temos que se $\alpha_1 \in L$ então $\alpha_1, \alpha_2, \cdots, \alpha_t \in L$. Pelo Teorema 10, temos que $f(x)$ se decompõe em $L[x]$ em fatores da forma

$$f(x) = c(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_t)^{m_t}$$

Sendo $c \in K$ e m_i a multiplicidade da raiz α_i, para $i = 1, 2, \cdots, t$.

Exemplo 51. A extensão $\mathbb{C} \supset \mathbb{R}$ é uma extensão normal, pelo Teorema Fundamental da Álgebra.

Exemplo 52. Sejam $\theta, \theta u, \cdots, \theta u^{p-1}$ as raízes do polinômio irredutível $f(x) = x^p - q$, com p, q primos positivos. Temos que $\mathbb{Q}[\theta, u]$ é extensão normal, sendo $\theta = \sqrt[p]{q} \in \mathbb{R}$ e $u = \cos\left(\frac{2\pi}{p}\right) + isen\left(\frac{2\pi}{p}\right)$.

Observaremos adiante que uma extensão finita é galoisiana se, e somente se, é extensão normal. Ribenboim (2001) define uma extensão algébrica L de um corpo K como galoisiana se L é uma extensão normal e separável sobre K. Como a questão da separabilidade será omitida em nosso estudo, neste contexto nos será suficiente mostrar que, para uma extensão finita, ser galoisiana e ser normal são definições equivalentes.

Definição 31. Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma : K \to K'$ isomorfismo. Sendo $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ definimos $f^\sigma(x) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in K'[x]$, para todo $n \in \mathbb{N}$.

Pelo Teorema 11 sabemos que todo polinômio não constante $f(x) \in K[x]$ pode ser escrito de forma única como um produto de polinômios irredutíveis sobre K. Isto é, existem $f_1(x), f_2(x), \cdots, f_r(x) \in K[x]$ irredutíveis sobre K tais que

$$f(x) = f_1(x)f_2(x)\cdots f_r(x)$$

Logo, de acordo com a Definição 31, decorre que

$$f^\sigma(x) = f_1^\sigma(x)f_2^\sigma(x)\cdots f_r^\sigma(x)$$

Sendo $K, K' \supset \mathbb{Q}$ corpos e $\sigma : K \to K'$ isomorfismo, segue imediatamente que se $f_j(x)$ é irredutível sobre K então $f_j^\sigma(x)$ é irredutível sobre K'. Ainda, Dummit e Foote (1991) apontam que podemos obter o isomorfismo $\phi : K[x] \to K'[x]$ como uma extensão do isomorfismo σ, sendo $\phi(f(x)) = f^\sigma(x)$. Daí segue que se todas as raízes de $f(x) \in K[x]$ estão em K, então todas as raízes de $f^\sigma(x) \in K'[x]$ estão em K'.

Teorema 25. Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma : K \to K'$ isomorfismo. Se $f(x) \in K[x]$ possui n raízes distintas, então $f^\sigma(x) \in K'[x]$ possui n raízes distintas.

Demonstração. Sabemos que o polinômio $f(x) \in K[x]$ pode ser escrito da forma $f(x) = f_1(x)^{m_1} f_2(x)^{m_2} \cdots f_r(x)^{m_r}$, sendo $f_i(x)$ polinômios irredutíveis sobre K e distintos dois a dois. Como $\sigma : K \to K'$ é isomorfismo, temos que $f^\sigma(x) = f_1^\sigma(x)^{m_1} f_2^\sigma(x)^{m_2} \cdots f_r^\sigma(x)^{m_r}$, sendo $f_i^\sigma(x)$ polinômios irredutíveis sobre K' e também distintos dois a dois. Como os polinômios $f_i(x), f_i^\sigma(x)$ são irredutíveis sobre K e K', respectivamente, pelo Teorema 19 temos que todas as suas respectivas raízes são simples, isto é, possuem multiplicidade 1. Logo, o número de raízes distintas em $f_i(x)$ e em $f_i^\sigma(x)$ é igual ao seus respectivos graus, de modo que $\partial f_i(x) = \partial f_i^\sigma(x)$, para todo $i = 1, 2, \cdots, r$. Portanto, sendo a soma dos graus de todos polinômios $f_i(x)$ igual a n, temos que a soma dos graus de $f_i^\sigma(x)$ também será n e assim $f^\sigma(x)$ possui também n raízes distintas.

4.2 Isomorfismos entre Extensões Galoisianas

Definição 32. Sejam $L \supset K$ e L' extensões tais que $\hat{\sigma} : L \to L'$ seja isomorfismo. Definimos a função $\hat{\sigma}|_K$ como a restrição do isomorfismo $\hat{\sigma}$ ao corpo K.

Teorema 26. Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma : K \to K'$ isomorfismo. Sendo $f(x) \in K[x]$ e $f^\sigma(x) \in K'[x]$ polinômios irredutíveis sobre K e K', com raízes $\alpha \in \mathbb{C}$ e $\beta \in \mathbb{C}$, respectivamente, existe um único isomorfismo $\hat{\sigma} : K[\alpha] \to K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}|_K = \sigma$.

Demonstração. *Existência:* Sendo α e β raízes dos polinômios irredutíveis $f(x) \in K[x]$ e $f^\sigma(x) \in K'[x]$, respectivamente, adotando $\partial f(x) = \partial f^\sigma(x) = t \in \mathbb{N}^*$, pelo Teorema 21, temos que

$$K[\alpha] = \left\{a_0 + a_1\alpha + \cdots + a_{t-1}\alpha^{t-1} / a_i \in K\right\}$$

$$K'[\beta] = \left\{b_0 + b_1\beta + \cdots + b_{t-1}\beta^{t-1} / b_i \in K'\right\}$$

são espaços vetorias sobre K e K', respectivamente. Ambos com dimensão t e bases $\{1, \alpha, \cdots, \alpha^{t-1}\}$, $\{1, \beta, \cdots, \beta^{t-1}\}$ respectivamente. Como $a_i \in K, b_i \in K'$ e $\sigma : K \to K'$ tal que $\sigma(a_i) = b_i$ é isomorfismo, podemos criar o isomorfismo $\hat{\sigma} : K[\alpha] \to K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}(a_i) = b_i$, para $i = 0, 1, \cdots, t-1$. Observa-se que $\hat{\sigma}|_K = \sigma$, isto é, $\hat{\sigma}(a_i) = \sigma(a_i) = b_i \in K'$, para todo $a_i \in K$.[2]

[2] Uma outra demonstração para este resultado pode ser encontrada em Dummit e Foote (1991), página 431.

Unicidade: Monteiro (1969) aponta um processo pelo qual podemos mostrar a unicidade do isomorfismo $\hat{\sigma} : K[\alpha] \to K'[\beta]$. Suponha que exista um isomorfismo $\lambda : K[\alpha] \to K'[\beta]$ nas mesmas condições de $\hat{\sigma}$, isto é, um isomorfismo $\lambda : K[\alpha] \to K'[\beta]$ tal que $\lambda(\alpha) = \beta$ e $\lambda|_K = \sigma$. Tomando $p(\alpha) = a_0 + a_1\alpha + \cdots + a_{t-1}\alpha^{t-1}$ como um elemento qualquer de $K[\alpha]$, temos que

$$\lambda(p(\alpha)) = \lambda\left(\sum_{i=0}^{t-1} a_i\alpha^i\right) = \sum_{i=0}^{t-1} \lambda(a_i)\lambda(\alpha)^i = \sum_{i=0}^{t-1} \sigma(a_i)\beta^i = \sum_{i=0}^{t-1} \hat{\sigma}(a_i)\beta^i = \hat{\sigma}(p(\alpha))$$

e portanto $\lambda = \hat{\sigma}$.

Corolário 3. Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma : K \to K'$ isomorfismo. Sendo $\alpha \in \mathbb{C}$ raiz de $f(x) \in K[x]$ então existe $\beta \in \mathbb{C}$ tal que $f^\sigma(\beta) = 0$ e $K[\alpha] \simeq K'[\beta]$ nas condições do teorema anterior.

Demonstração. Pelo Teorema 11, sabemos que existem $f_1(x), f_2(x), \cdots, f_r(x) \in K[x]$, irredutíveis sobre K, tais que $f(x) = f_1(x)f_2(x)\cdots f_r(x)$. Deste modo, $f^\sigma(x) = f_1^\sigma(x)f_2^\sigma(x)\cdots f_r^\sigma(x)$, sendo $f_i^\sigma(x) \in K'[x]$ irredutível sobre K' para $i = 1, 2, \cdots, r$. Se $f(\alpha) = 0$, podemos admitir que α é raiz de $f_j(x) \in K[x]$, para algum $j \in \{1, 2, \cdots, r\}$. Sendo $f_j(x)$ irredutível sobre K e β uma raiz qualquer de $f_j^\sigma(x) \in K'[x]$, temos que $f^\sigma(\beta) = 0$ e, pelo teorema anterior, $\hat{\sigma} : K[\alpha] \to K'[\beta]$ é isomorfismo tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}|_K = \sigma$.

Exemplo 53. Considere o polinômio irredutível $f(x) = x^p - q$, com p, q primos positivos, e suas raízes $\theta, \theta u, \cdots, \theta u^{p-1}$. Com as notações do teorema anterior, considerando $K = K' = \mathbb{Q}$ e $\sigma : \mathbb{Q} \to \mathbb{Q}$ como a função identidade, temos que $f(x) = f^\sigma(x)$ e $\hat{\sigma} : \mathbb{Q}[\theta] \to \mathbb{Q}[\theta u]$ é isomorfismo tal que $\hat{\sigma}(\theta) = \theta u$ e $\hat{\sigma}|_{\mathbb{Q}} = \sigma$.

Exemplo 54. Novamente, considerando o polinômio irredutível $f(x) = x^p - q$, com p, q primos positivos, e suas raízes $\theta, \theta u, \cdots, \theta u^{p-1}$, pelo Teorema 26 temos que $\mathbb{Q}[\theta], \mathbb{Q}[\theta u] \supset \mathbb{Q}$ são corpos tais que existe $\varphi : \mathbb{Q}[\theta] \to \mathbb{Q}[\theta u]$ isomorfismo. Considerando o polinômio $p(x) = x^2 + 1$ irredutível sobre $\mathbb{Q}[\theta]$, temos que $p^\varphi(x) = p(x)$ e $\hat{\varphi} : (\mathbb{Q}[\theta])[\alpha] \to (\mathbb{Q}[\theta u])[\beta]$ é isomorfismo tal que $\hat{\varphi}(\alpha) = \beta$ e $\hat{\varphi}|_{\mathbb{Q}[\theta]} = \varphi$, sendo $\alpha, \beta = \pm i \in \mathbb{C}$.

Teorema 27. Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma : K \to K'$ isomorfismo. Sendo $f(x) \in K[x]$ um polinômio com raízes $\alpha_1, \alpha_2, \cdots, \alpha_t \in \mathbb{C}$ distintas, decorre que existe um isomorfismo $\hat{\sigma} : Gal(f(x), K) \to Gal(f^\sigma(x), K')$ tal que $\hat{\sigma}(\alpha_1), \hat{\sigma}(\alpha_2), \cdots, \hat{\sigma}(\alpha_t) \in \mathbb{C}$ são as raízes distintas de $f^\sigma(x) \in K'[x]$ e $\hat{\sigma}|_K = \sigma$.

Demonstração. Se $f(x) \in K[x]$ possui somente uma raiz α_1 de multiplicidade m, decorre que $f(x) = c(x-\alpha_1)^m$. Logo, $\alpha_1 \in K$ e $\sigma(\alpha_1) \in K'$ de forma que $\sigma(\alpha_1)$ é raiz de $f^\sigma(x) \in K'[x]$. Assim $Gal(f(x), K) = K$ e $Gal(f^\sigma(x), K') = K'$. Sendo $K \simeq K'$, podemos adotar $\hat{\sigma} : Gal(f(x), K) \to Gal(f^\sigma(x), K')$ como o isomorfismo $\sigma : K \to K'$.

Sendo $\alpha_1, \alpha_2, \cdots, \alpha_t \in \mathbb{C}$ raízes distintas de $f(x)$, pelo Teorema 25, decorre que existem t raízes distintas de $f^\sigma(x)$. Sejam $\beta_1, \beta_2, \cdots, \beta_t$ estas raízes. Pelo Corolário 3, sabemos que existe $\sigma_1 : K[\alpha_1] \to K'[\beta_1]$ isomorfismo, sendo $\sigma_1(\alpha_1) = \beta_1$ e $\sigma_1|_K = \sigma$.

Denotando $K_1 = K[\alpha_1]$ e $K_1' = K'[\beta_1]$ considere as entensões $K_2 = K_1[\alpha_2]$ e $K_2' = K_1'[\beta_2]$. Como $K_1 \simeq K_1'$ por σ_1, novamente pelo Corolário 3 temos que existe $\sigma_2 : K_1[\alpha_2] \to K_1'[\beta_2]$ isomorfismo, sendo $\sigma_2(\alpha_2) = \beta_2$ e $\sigma_2|_{K_1} = \sigma_1$. Repare que, como $K_2 \supset K_1 \supset K$, temos que $\sigma_2|_K = \sigma_1|_K = \sigma$.

Podemos repetir esse processo sucessivas vezes até obtermos as extensões $K_t = K_{t-1}[\alpha_t]$ e $K_t' = K_{t-1}'[\beta_t]$. Através do isomorfismo $\sigma_{t-1} : K_{t-1} \to K_{t-1}'$, utilizando o Corolário 3, podemos criar o isomorfismo $\sigma_t : K_{t-1}[\alpha_t] \to K_{t-1}'[\beta_t]$ tal que $\sigma_t(\alpha_t) = \beta_t$ e $\sigma_t|_{K_{t-1}} = \sigma_{t-1}$.

Como $\sigma_t : K_t \to K_t'$ é isomorfismo, sendo $K_t = K[\alpha_1, \alpha_2, \cdots, \alpha_t] = Gal(f(x), K)$ e $K_t' = K'[\beta_1, \beta_2, \cdots, \beta_t] = Gal(f^\sigma(x), K')$, decorre que existe um isomorfismo $\sigma_t = \hat{\sigma} : Gal(f(x), K) \to Gal(f^\sigma(x), K')$. E sendo $K_t \supset K_{t-1} \supset \cdots \supset K_1 \supset K$, temos que: $\hat{\sigma}|_K = \sigma_t|_K = \sigma_{t-1}|_K = \sigma_{t-2}|_K = \cdots = \sigma_2|_K = \sigma_1|_K = \sigma$. Ainda, observe que do fato de $\sigma_i|_{K_{i-1}} = \sigma_{i-1} : K_{i-1} \to K_{t-1}'$, para todo $i = 2, 3, \cdots, t$, temos que $\hat{\sigma}(\alpha_i) = \beta_i$ para todo $i = 1, 2, \cdots, t$. Por fim, podemos observar estes isomorfismos no seguinte diagrama:

$$
\begin{array}{ccc}
K_t = K[\alpha_1, \alpha_2, \cdots, \alpha_t] & \underset{\sigma_t = \hat{\sigma}}{\to} & K_t' = K'[\beta_1, \beta_2, \cdots, \beta_t] \\
| & & | \\
\vdots & & \vdots \\
| & & | \\
K_2 = K[\alpha_1, \alpha_2] & \underset{\sigma_2}{\to} & K_2' = K'[\beta_1, \beta_2] \\
| & & | \\
K_1 = K[\alpha_1] & \underset{\sigma_1}{\to} & K_1' = K'[\beta_1] \\
| & & | \\
K & \underset{\sigma}{\to} & K'
\end{array}
$$

Exemplo 55. Sejam $p_1, p_2, \cdots, p_t$ primos distintos dois a dois e considere

$$f(x) = \prod_{i=1}^{t}(x^2 - p_i)$$

Como $\mathbb{Q} \simeq \mathbb{Q}$ pela função $\sigma : \mathbb{Q} \to \mathbb{Q}$ identidade, temos que $f(x) = f^{\sigma}(x)$ e

$$Gal(f(x), \mathbb{Q}) = Gal(f^{\sigma}(x), \mathbb{Q}) = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_t}]$$

Com as notações análogas às notações utilizadas no Teorema 27, sendo $\alpha_i = \sqrt{p_i}$ e $\beta_i = \pm\sqrt{p_i}$ podemos criar os isomorfismos $\hat{\sigma}_i : \mathbb{Q}[\alpha_1, \cdots, \alpha_i] \to \mathbb{Q}[\beta_1, \cdots, \beta_i]$, sendo $\hat{\sigma}_i(\alpha_i) = \beta_i$ e $\hat{\sigma}_i|_{\mathbb{Q}} = \sigma$ para $i = 1, 2, \cdots, t$.

Corolário 4. Sejam H, H' corpos e $L \supset K$ uma extensão galoisiana tal que $L \supset H, H' \supset K$. Sendo $\sigma : H \to H'$ um K-isomorfismo, então existe um automorfismo $\hat{\sigma} \in Aut_K^L$ tal que $\hat{\sigma}|_H = \sigma$.

Demonstração. Sendo $L \supset K$ uma extensão galoisiana, temos que existe $f(x) \in K[x]$ tal que $L = Gal(f(x), K)$. Como $L \supset H, H^{'} \supset K$, temos que $L \supset H, H'$ também é galoisiana. Sendo $\sigma : H \to H'$ um K-isomorfismo, decorre que $f(x) = f^{\sigma}(x)$ e $L = Gal(f(x), H) = Gal(f^{\sigma}(x), H^{'})$. Pelo teorema anterior, sabemos que existe um isomorfismo $\hat{\sigma} : L \to L$ tal que $\hat{\sigma}|_H = \sigma$. Portanto, existe um automorfismo $\hat{\sigma} \in Aut_K^L$ tal que $\hat{\sigma}|_H = \sigma$.

Por um processo análogo, apontado por Stewart (2004), podemos visualizar o seguinte diagrama:

$$\begin{array}{ccc} L & \xrightarrow{\hat{\sigma}} & L \\ | & & | \\ H & \xrightarrow{\sigma} & H' \\ | & & | \\ K & & K \end{array}$$

Teorema 28. Seja $L \supset K$ uma extensão finita. Então L é normal se, e somente se, L é galoisiana.

Demonstração. Seja $L \supset K$ uma extensão finita e normal. Como L é finita, pelo Teorema 24, existe $u \in L$ tal que $L = K[u]$. Considere o polinômio $p(x) = irr(u, K)$. Como $p(x)$ tem uma raiz $u \in L$ e L é normal, pela Definição 30, decorre que todas as demais raízes de $p(x)$ estão em L. Portanto $L = Gal(p(x), K)$, isto é, L é galoisiana.

Por outro lado, considerando L galoisiana sobre K, decorre que existe $f(x) \in K[x]$ tal que $L = Gal(f(x), K)$. Seja $v(x) \in K[x]$ um polinômio irredutível sobre K tal que $v(x)$ possua uma raiz $\alpha \in L$. Mostraremos que qualquer outra raiz β de $v(x)$, distinta de α, também pertence a L.

De fato, como $v(x) \in K[x]$ é irredutível sobre K, pelo Teorema 26 decorre que existe um isomorfismo $\sigma_1 : K[\alpha] \to K[\beta]$, sendo $\sigma_1(\alpha) = \beta$ e podemos considerar $\sigma_1|_K = \sigma : K \to K$ como a função identidade.

Considere agora $L' = Gal(f(x), K[\beta])$. Como $L \supset K[\alpha] \supset K$, temos que $L \supset K[\alpha]$ é galoisiana e assim $L = Gal(f(x), K[\alpha]) = Gal(f(x), K)$. E como $K[\beta] \supset K$, temos que $Gal(f(x), K[\beta]) \supset Gal(f(x), K)$, isto é, $L' \supset L$.

Sendo $\sigma : K \to K$ a função identidade, decorre que $f^{\sigma_1}(x) = f^{\sigma}(x) = f(x)$. Assim, temos que

$$L' = Gal(f(x), K[\beta]) = Gal(f^{\sigma}(x), K[\beta])$$

e como $K[\alpha] \simeq K[\beta]$ por σ_1 podemos, através do Teorema 27, criar o isomorfismo $\sigma_2 : Gal(f(x), K[\alpha]) \to Gal(f^{\sigma}(x), K[\beta])$ tal que $\sigma_2|_{K[\alpha]} = \sigma_1$. Repare que $\sigma_2|_K = \sigma_1|_K = \sigma$, ou seja, σ_2 é K-isomorfismo.

Sendo L e L' espaços vetoriais sobre K isomorfos entre si, pelo Teorema 4 temos que $[L : K] = [L' : K]$. Logo, como $L \subset L'$, temos que $L = L'$. Como $\beta \in L'$ e $L' = L$, segue que $\beta \in L$ e portando L é extensão normal.

4.3 Automorfismos de Extensões Galoisianas

Teorema 29. Seja $L \supset K$ uma extensão finita. Se L é galoisiana, então $|Aut_K^L| = [L : K]$.

Demonstração. Sendo $L \supset K$ uma extensão finita, pelo Teorema 24, existe $u \in L$ tal que $L = K[u]$. Considere o polinômio $f(x) = irr(u, K)$, de grau n. Como L é galoisiana, pelo Teorema 28, temos que L é normal e pela Definição 30 segue que todas as demais raízes de $f(x)$ estão em L. Pelo Teorema 19, sendo $f(x)$ irredutível temos que todas as raízes de $f(x)$ são simples, isto é, $f(x)$ possui n raízes distintas com multiplicidade 1. Sejam $u_1, u_2, u_3, \cdots, u_n \in L$ essas raízes, e considere $u = u_1$.

É imediato que $K \simeq K$ pela função identidade $\varphi : K \to K$. Neste sentido, temos que $p(x) = p^{\varphi}(x)$, para todo $p(x) \in K[x]$. Podemos então considerar u raiz de $f(x)$ e $u_i \in L$ raiz de $f^{\varphi}(x)$, respectivamente. Utilizando o Teorema 26, temos que existe um isomorfismo $\sigma_i : K[u] \to K[u_i]$ tal que $\sigma_i(u) = u_i$ e $\sigma_i|_K = \varphi$, para $i = 1, 2, \cdots, n$. Portanto,

$$\sigma_i(u) = u_i \qquad \sigma_i(a) = \varphi(a) = a \ \ \forall a \in K$$

isto é, $\sigma_i : K[u] \to K[u_i]$ é K-isomorfismo. Mostraremos agora que, para cada $i \in \{1, 2, \cdots, n\}$, existe um $\hat{\sigma}_i$ que é K-automorfismo. Pelo Corolário 4, $L = Gal(f(x), K[u]) = Gal(f^{\sigma_i}(x), K[u_i])$ e existe $\hat{\sigma}_i : L \to L$ tal que $\hat{\sigma}_i|_{K[u]} = \sigma_i$. Logo, $\hat{\sigma}_i|_K = \sigma_i|_K = \varphi : K \to K$. Portanto, $\hat{\sigma}_i \in Aut_K^L$ para $i = 1, 2, \cdots, n$. Pelo Teorema 26 temos que cada isomorfismo σ_i é único. Logo, cada automorfismo $\hat{\sigma}_i$ é único. Portanto L possui pelo menos n K-automorfismos distintos, ou seja, $|Aut_K^L| \geq n$.

Agora, pelo Teorema 21 temos que $[L : K] = \partial f(x) = n$ e de acordo com o Corolário 2 temos que $|Aut_K^L| \leq [L : K] = n$. Logo, como $|Aut_K^L| \geq n$ e $|Aut_K^L| \leq n$, segue que $|Aut_K^L| = n$, isto é, $|Aut_K^L| = [L : K]$.

Exemplo 56. Como $K \supset K$ é galoisiana de acordo com o Exemplo 47, temos que $|Aut_K^K| = [K : K] = 1$. Logo, $Aut_K^K = \{\sigma_1\}$, sendo σ_1 é a função identidade.

Exemplo 57. Como $\mathbb{C} \supset \mathbb{R}$ é extensão galoisiana de acordo com o Exemplo 48, temos que $|Aut_{\mathbb{R}}^{\mathbb{C}}| = [\mathbb{C} : \mathbb{R}] = 2$, visto que $\{1, i\}$ é uma base do espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$. Assim, $Aut_{\mathbb{R}}^{\mathbb{C}} = \{\sigma_1, \sigma_2\}$, sendo σ_1 a função identidade e $\sigma_2(a + bi) = a - bi$, para todo $a + bi \in \mathbb{C}$. Podemos observar que, de forma geral, para todo $c \in \mathbb{R}$:

$$\sigma_1 : \begin{array}{l} c \to c \\ i \to i \end{array} \qquad\qquad \sigma_2 : \begin{array}{l} c \to c \\ i \to -i \end{array}$$

Exemplo 58. De acordo com o Exemplo 49, $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ é extensão galoisiana. Como $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$, utilizando o Teorema 22, temos que

$$|Aut_{\mathbb{Q}}^L| = [L : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 = 4$$

pois $\{1, \sqrt{3}\}$ é uma base do espaço vetorial $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ sobre $\mathbb{Q}[\sqrt{2}]$ e $\{1, \sqrt{2}\}$ é uma base do espaço vetorial $\mathbb{Q}[\sqrt{2}]$ sobre $\mathbb{Q}$. Deste modo $Aut_{\mathbb{Q}}^L = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, sendo $\sigma_i(c) = c$, para todo $c \in \mathbb{Q}$. Sendo $f(x) = (x^2 - 2)(x^2 - 3)$, temos que $Gal(f(x), \mathbb{Q}) = L$. Pelo Teorema 23, sabemos que se $\vartheta \in L$ é raiz de $f(x)$, então $\sigma(\vartheta)$ também é raiz de $f(x)$,

sendo $\sigma \in Aut_{\mathbb{Q}}^{L}$. Deste modo, como $\sqrt{2}$ é raiz de x^2-2, temos que $(\sigma(\sqrt{2}))^2-2=0$. Analogamente, como $\sqrt{3}$ é raiz de x^2-3, temos que $(\sigma(\sqrt{3}))^2-3=0$. Assim, $(\sigma(\sqrt{2}))^2=2$ e $(\sigma(\sqrt{3}))^2=3$, isto é, as possibilidades de imagem para $\sigma(\sqrt{2})$ são $\pm\sqrt{2}$ e as possibilidades de imagem para $\sigma(\sqrt{3})$ são $\pm\sqrt{3}$. Os elementos de $Aut_{\mathbb{Q}}^{L}$ ficam, portanto, determinados da seguinte maneira:

$$\begin{array}{llllllll} \sigma_1: & \sqrt{2}\to\sqrt{2} & \sigma_2: & \sqrt{2}\to-\sqrt{2} & \sigma_3: & \sqrt{2}\to\sqrt{2} & \sigma_4: & \sqrt{2}\to-\sqrt{2} \\ & \sqrt{3}\to\sqrt{3} & & \sqrt{3}\to\sqrt{3} & & \sqrt{3}\to-\sqrt{3} & & \sqrt{3}\to-\sqrt{3} \end{array}$$

Exemplo 59. Pelo Exemplo 50, temos que $L=\mathbb{Q}[\sqrt[3]{5},u]\supset\mathbb{Q}$ é extensão galoisiana, sendo $u=\cos\left(\frac{2\pi}{3}\right)+isen\left(\frac{2\pi}{3}\right)$. Como $\mathbb{Q}[\sqrt[3]{5},u]\supset\mathbb{Q}[u]\supset\mathbb{Q}$, utilizando o Teorema 22, temos que:

$$|Aut_{\mathbb{Q}}^{L}|=[L:\mathbb{Q}]=[L:\mathbb{Q}[u]]\cdot[\mathbb{Q}[u]:\mathbb{Q}]=3\cdot 2=6$$

pois $\left\{1,(\sqrt[3]{5}),(\sqrt[3]{5})^2\right\}$ é base do espaço vetorial $\mathbb{Q}[\sqrt[3]{5},u]$ sobre $\mathbb{Q}[u]$ e $\{1,u\}$ é base do espaço vetorial $\mathbb{Q}[u]$ sobre $\mathbb{Q}$. Logo, $Aut_{\mathbb{Q}}^{L}=\{\sigma_1,\sigma_2,\cdots,\sigma_6\}$, sendo $\sigma_i(c)=c$, para todo $c\in\mathbb{Q}$. Sendo $f(x)=x^3-5$, temos que $Gal(f(x),\mathbb{Q})=L$. Utilizando novamente o Teorema 23, temos que sendo $\vartheta\in L$ raiz de $f(x)$, então $\sigma(\vartheta)$ também será raiz de $f(x)$, para todo $\sigma\in Aut_{\mathbb{Q}}^{L}$. Assim $(\sigma(\sqrt[3]{5}))^3=5$ e temos $\sqrt[3]{5},\sqrt[3]{5}u,\sqrt{5}u^2$ como possibilidade de imagem para $\sigma(\sqrt[3]{5})$. Analogamente, considere o polinômio ciclotômico $g(x)=x^2+x+1$ com raízes u e u^2. Temos que $Gal(g(x),\mathbb{Q})=\mathbb{Q}[u]$ e como u é raiz de $g(x)$, novamente pelo Teorema 23, decorre que $\sigma(u)$ também é raiz de $g(x)$. Assim, temos u e u^2 como possibilidades de imagem para $\sigma(u)$. Os elementos de $Aut_{\mathbb{Q}}^{L}$ ficam determinados, portanto, da seguinte maneira:

$$\begin{array}{lll} \sigma_1: \begin{array}{c}\sqrt[3]{5}\to\sqrt[3]{5}\\ u\to u\end{array} & \sigma_2: \begin{array}{c}\sqrt[3]{5}\to\sqrt[3]{5}u\\ u\to u\end{array} & \sigma_3: \begin{array}{c}\sqrt[3]{5}\to\sqrt[3]{5}u^2\\ u\to u\end{array} \\ \sigma_4: \begin{array}{c}\sqrt[3]{5}\to\sqrt[3]{5}\\ u\to u^2\end{array} & \sigma_5: \begin{array}{c}\sqrt[3]{5}\to\sqrt[3]{5}u\\ u\to u^2\end{array} & \sigma_6: \begin{array}{c}\sqrt[3]{5}\to\sqrt[3]{5}u^2\\ u\to u^2\end{array} \end{array}$$

Exemplo 60. Com as notações do Exemplo 52, temos que $\theta,\theta u,\theta u^2,\cdots,\theta u^{p-1}$ são as raízes do polinômio irredutível $f(x)=x^p-q$, com p,q primos positivos, e $L=\mathbb{Q}[\theta,u]\supset\mathbb{Q}$ é extensão normal. Pelo Teorema 28, decorre que $L\supset\mathbb{Q}$ é extensão galoisiana. De fato, podemos observar que $L=Gal(x^p-q,\mathbb{Q})$. Como $\mathbb{Q}[\theta,u]\supset\mathbb{Q}[u]\supset\mathbb{Q}$, utilizando o Teorema 22, temos que

$$|Aut_{\mathbb{Q}}^{L}|=[L:\mathbb{Q}]=[L:\mathbb{Q}[u]]\cdot[\mathbb{Q}[u]:\mathbb{Q}]=p(p-1)$$

pois $\{1,\theta,\theta^2,\cdots,\theta^{p-1}\}$ uma base do espaço vetorial $\mathbb{Q}[\theta,u]$ sobre $\mathbb{Q}[u]$ e $\{1,u,\cdots,u^{p-2}\}$ é base do espaço vetorial $\mathbb{Q}[u]$ sobre $\mathbb{Q}$. Utilizaremos novamente o Teorema 23, o qual

afirma que sendo $\vartheta \in L$ raiz de $f(x)$, então $\sigma(\vartheta)$ é raiz de $f(x)$, para todo $\sigma \in Aut_{\mathbb{Q}}^{L}$. Deste modo, $(\sigma(\theta))^p = q$ e temos $\theta, \theta u, \theta u^2, \cdots, \theta u^{p-1}$ como opções de imagem para $\sigma(\theta)$. Considerando agora o polinômio ciclotômico $c(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, com raízes $u, u^2, \cdots, u^{p-1}$, temos que $Gal(c(x), \mathbb{Q}) = \mathbb{Q}[u]$. Sendo u raiz de $c(x)$, utilizando novamente o Teorema 23, decorre que $\sigma(u)$ também é raiz de $c(x)$. Logo, temos $u, u^2, \cdots, u^{p-1}$ como possibilidades de imagem para $\sigma(u)$. Deste modo, os elementos de $\sigma \in Aut_{\mathbb{Q}}^{L}$ são determinados da seguinte forma:

$$\sigma(\theta) \in \left\{\theta, \theta u, \theta u^2, \cdots, \theta u^{p-1}\right\} \qquad \sigma(u) \in \left\{u, u^2, \cdots, u^{p-1}\right\}$$

e temos $p(p-1)$ possibilidades distintas para formação do automorfismo σ.

Considerações Finais

Este trabalho apresentou um estudo teórico e demonstrativo em álgebra abstrata, com ênfase nos isomorfismos e automorfismos das extensões algébricas L de um corpo K. Demonstrou-se, entre outras coisas, que o número de automorfismos de uma extensão algébrica e finita $L \supset K$ que fixam o corpo K é igual à dimensão do espaço vetorial L sobre K. Mais que isso, apresentou-se também exemplos concretos dos resultados referentes a este teorema, como o número de automorfismos da extensão $\mathbb{C}$ do corpo $\mathbb{R}$ e de algumas extensões algébricas dos racionais.

Ainda, como encontrado em Gonçalves (1979), este trabalho apresentou alguns tópicos introdutórios ao estudo da teoria de Galois elementar. De acordo com Hungerford (1974, p.230) : "A idea chave da teoria de Galois é relacionar a extensão F do corpo K com o grupo de todos os automorfismos de F que fixam K". Entretanto, evidentemente a apreciação da teoria de Galois em particular não foi contemplada como objetivo de nosso texto e necessita de conteúdos que estão além das delimitações teóricas desta pesquisa.

Este trabalho possibilitou um entedimento mais generalizado dos conceitos de extensão, isomorfismo, automorfismo, entre outros, e suas correlações. A inclusão de tópicos de álgebra linear e espaços vetoriais, além de necessárias ao objeto de estudo da pesquisa, possibilitou melhor compreensão de algumas propriedades referentes às estruturas algébricas de corpos. De fato, segundo Araújo (2009, p.116): "A estrutura de espaço vetorial subjacente à uma extensão de corpos é fundamental no estudo de extensões de corpos".

Espero que este trabalho possa servir de auxílio às pessoas que se dedicam a estudar os tópicos apresentados em álgebra abstrata, bem como àquelas que se interessam por matemática de forma independente.

Referências Bibliográficas

ARAUJO, K. V. de. *Estruturas Algebricas II*. Sergipe: UFS, 2009.

CONRAD, K. *The Galois Correspondence (artigo.)*. Disponível em https://kconrad.math.uconn.edu/blurbs/: Acesso 22/04, 2020.

CONRAD, K. *Unique fatorization in $\mathbb{Z}$ and $F[t]$ (artigo)*. Disponível em https://kconrad.math.uconn.edu/blurbs/: Acesso 30/04, 2020.

DOMINGUES, H.; IEZZI, G. *Algebra moderna*. São Paulo: Atual Editora, 2003.

DUMMIT, D. S.; FOOTE, R. M. *Abstract Algebra*. New Jersey, USA: Prentice-Hall,Inc, 1991.

FINE, B.; ROSENBERGER, G. *The Fundamental Theorem of Algebra*. New York: Springer-Verlag, 1997.

FINE, B.; ROSENBERGER, G. *Number Theory: An introduction via the distribution of primes*. Boston: Birkhauser Boston, 2007.

GONÇALVES, A. *Introdução à álgebra*. Rio de Janeiro: Livros Técnicos e Científicos S.A, 1979.

GRILLET, P. A. *Abstract Algebra*. New York, USA: Springer, 2007.

HUNGERFORD, T. W. *Algebra*. New York, USA: Springer, 1974.

IEZZI, G. *Fundamentos de Matemática Elementar: complexos, polinômios e equações*. São Paulo: Atual Editora, 1977.

JANESCH, O. R.; TANEJA, I. J. *Álgebra I*. Santa Catarina: UFSC, 2011.

LANG, S. *Undergraduate algebra*. New Haven, EUA: Springer, 2005.

LORENZ, F. *Algebra, vol I: Fields and Galois Theory*. USA: Springer, 2006.

MONTEIRO, L. H. J. *Elementos de álgebra*. Rio de Janeiro: Ao Livro Técnico S.A, 1969.

PARSHIN, A.; SHAFAREVICH, I. *Encyclopaedia of Mathematical Sciences.Number Theory IV: Transcendental Numbers*. -: Springer, 1997.

RIBENBOIM, P. *Classical Theory of Algebraic Numbers*. New York: Springer, 2001.

SAHAI, V.; BIST, V. *Linear Algebra*. India: Alpha Science International Ltda., 2002.

STEWART, I. *Galois Theory*. USA: Chapman Hall, 2004.

WAERDEN, B. van der. *A History of Algebra: from Al Khwarizmi to Emmy Noether*. Berlin: Springer, 1985.

WINTERLE, P.; STEINBRUCH, A. *Álgebra Linear*. São Paulo: Pearson Education, 1987.