UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

DJERLY SIMONETTI

EXTENSÕES GALOISIANAS: ADENTRANDO AO PROBLEMA INVERSO DE GALOIS

TRABALHO DE CONCLUSÃO DE CURSO

TOLEDO - PR
2015

DJERLY SIMONETTI

EXTENSÕES GALOISIANAS: ADENTRANDO AO PROBLEMA INVERSO DE GALOIS

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Conclusão de Curso 2, do Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná - UTFPR, Câmpus Toledo.

Orientador Prof. Dr. Wilian Francisco de Araujo

TOLEDO

20/11/2015

TERMO DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado Extensões Galoisianas: adentrando ao Problema Inverso de Galois foi considerado **APROVADO** de acordo com a ata da banca examinadora N° 004 de 20/11/2015.

Fizeram parte da banca examinadora os professores:

Prof. Dr. Wilian Francisco de Araujo

Prof. Dr. Edson Carlos Licurgo Santos

Prof. Ms. Larissa Hagedorn Vieira

Tu te tornas eternamente responsável por aquilo que cativas.

(O Pequeno Príncipe - Antonie de Saint-Exupéry)

AGRADECIMENTOS

À Deus, energia máxima que me conduz!

Agradeço, especialmente, ao Professor Wilian Francisco de Araujo acima de tudo pela paciência, e por acreditar, muitas vezes, mais do que eu, de que o esforço te faz ir mais longe.

Também, não posso deixar de agradecer ao meu amor, que acompanhou-me em toda esta caminhada, mesmo com pouco entendimento teórico, mas com muito apreço em todos os momentos de dificuldade e felicidade desse processo.

De modo especial, agradeço o apoio de todos que enviaram boas energias para a realização dessa obra; sei que a torcida foi grande.

Ao Programa de Bolsas de Fomento às Ações de Graduação que apoiou os dois últimos meses deste trabalho.

Meu muito obrigada a todos vocês.

RESUMO

O objetivo deste trabalho é apresentar o Problema Inverso de Galois, o qual consiste em descobrir em que condições podemos determinar um polinômio que tenha G como grupo de Galois. Para tanto, a Teoria de Galois é abordada, discorrendo-se sobre extensões algébricas, extensões cíclicas, extensões galoisianas e exemplificando o Teorema Fundamental de Galois.

Palavras-chave: Extensão galoisiana. Grupo de automorfismos de Galois. O Problema Inverso de Galois.

ABSTRACT

The objective of this paper is to present the Inverse Problem of Galois, which is to discover under what conditions we can determine a polynomial that has G as a Galois group. Therefore, the Galois Theory is addressed, if discoursing on algebraic extensions, cyclic extensions and exemplifying the Fundamental Theorem of Galois.

Keywords: Galoisiana extension. Galois group of automorphisms. The Inverse Problem of Galois.

LISTA DE SÍMBOLOS

$(G, *)$	grupo com a operação $*$
$o(G)$	ordem de G
$\mathbb{Z}_m$	conjunto das classes de resto módulo m
S_n	grupo de permutação
$N(\Psi)$	núcleo da função Ψ
$Aut\ G$	automorfismo de G
$\simeq$	isomorfismo
$K[x]$	conjunto de polinômios sobre K em uma indeterminada x
$(K[x], +, \cdot)$	anel de polinômios sobre o corpo K
$\partial p(x)$	grau do polinômio $p(x)$
$p(x) = irr(\alpha, K)$	polinômio mônico irredutível de menor grau sobre K onde $p(\alpha) = 0$
$L\|K$	extensão de corpos, onde L é uma extensão do corpo K
$Aut_K L$	conjunto dos $K-$automorfismos de L
$\sigma\|_K$	restrição de σ sobre o corpo K
$\varnothing$	conjunto vazio
$L = Gal(f, K)$	corpo de decomposição de $f(x)$ sobre o corpo K
$[L : K]$	grau da extensão $L\|K$
$\|Aut_K L\|$	cardinalidade do conjunto $Aut_K L$
$W_n(K)$	Conjunto das raízes n-ésimas da unidade em K
K^*	grupo multiplicativo do corpo K
$o(\zeta)$	ordem de ζ no grupo K^*
$\mathfrak{R}$	conjunto das raízes do polinômio $x^p - a$
$\vartheta(M, K)$	conjunto de corpos intermediários de $M\|K$

SUMÁRIO

INTRODUÇÃO

A Teoria de Galois descreve uma maneira de permutar as raízes de um polinômio, gerando com essas raízes um grupo. Tal grupo é conhecido por grupo de automorfismos de Galois. Sendo que, a ideia central da teoria deste matemático, Evariste Galois, é determinar o grupo de Galois correspondente a um dado polinômio.

No presente trabalho discorremos sobre a Teoria de Galois com intuito de apresentar o Problema Inverso de Galois, decorrente dessa Teoria. A saber, o problema consiste em descobrir em que condições podemos determinar um polinômio que tenha G como grupo de Galois.

Nas próximas páginas, o leitor encontrará no Capítulo 1, algumas noções básicas que fundamentam conceitos utilizados no decorrer do trabalho. Já no Capítulo 2 são apresentadas as extensões algébricas, extensões galoisianas, e extensões cíclicas, exemplificando sempre que possível os resultados abordados. E por fim, no Capítulo 3, temos a definição de extensão normal, grupo de Galois, e claro, o Teorema Fundamental de Galois. Nesse último capítulo explicitamos o Problema Inverso de Galois.

1 PRELIMINARES

Neste prelúdio são apresentados alguns conceitos básicos para o desenvolvimento deste trabalho. Especificamente, abordarmos grupos, aneis e corpos. As demonstrações serão omitidas, já que não se caracterizam como o foco do estudo, e, podem ser encontradas em qualquer livro básico de Álgebra.

1.1 GRUPOS E SUBGRUPOS

Nesta seção apresentamos alguns resultados que são conhecidos, porém elencados aqui com intuito de facilitar as demonstrações dos próximos capítulos, quando necessários.

Primeiramente, veja a acepção de grupo:

Definição 1.1.1. Um grupo $(G, *)$ é um conjunto não vazio onde existe uma operação $* : G \times G \to G$, satisfazendo os seguintes axiomas:

(1) $(x * y) * z = x * (y * z)$, quaisquer que sejam $x, y, z \in G$ (associatividade);

(2) $\exists\ e \in G$ tal que $e * x = x * e = x$, $\forall\ x \in G$ (existência do elemento neutro);

(3) Para todo $x \in G$ existe um $x^{-1} \in G$ tal que $x * x^{-1} = x^{-1} * x = e$ (existência de elemento simétrico/inverso);

Se além disso satisfazer:

(4) $x * y = y * x$, quaisquer que sejam $x, y \in G$ (comutatividade). Nesse caso o grupo é denominado *grupo abeliano* ou *grupo comutativo*.

Se G é finito denominamos *grupo finito*, caso contrário, *grupo infinito*. E a quantidade de elementos de G será chamada de *ordem de* G representada por $o(G)$. Denotaremos o grupo $(G, *)$ simplesmente por G.

Exemplo 1.1.2. O grupo aditivo das classes de resto módulo m, $(\mathbb{Z}_m, +)$ é um grupo finito cuja $o(\mathbb{Z}_m, +) = m$.

Um dos grupos importantes para o estudo da teoria de Galois é o *grupo de permutações de* n elementos de um conjunto M. Considere $\Omega = \{1, 2, ..., n\}$ e $S_n = \{f : \Omega \to \Omega : f \text{ bijetiva}\}$. Assim, temos que $(S_n, \circ)$, onde $\circ$ denota a composição de funções, é um grupo de permutações finito, contendo $n!$ elementos e não abeliano para $n \geq 3$. Os elementos de S_n são também chamados de permutações de Ω.

Definição 1.1.3. Um grupo G é *cíclico* quando ele pode ser gerado por um elemento, isto é, quando $G = \langle g \rangle$ para algum $g \in G$.

Especificamente, um *grupo multiplicativo* é cíclico se $G = \{a^m \mid m \in \mathbb{Z}\}$ para algum $a \in G$, e no caso aditivo, $G = \{m \cdot a \mid m \in \mathbb{Z}\}$. E não necessariamente, um grupo cíclico é gerado por apenas um elemento.

Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se H for ele próprio um grupo com a mesma operação de G.

Proposição 1.1.4. *[2] Seja G um grupo. Para que uma parte não vazia $H \subset G$ seja um subgrupo de G, é necessário e suficiente que $x * y^{-1}$ seja um elemento de H sempre que x e y pertencer a esse conjunto.*

Pela ideia de subgrupos, podemos ter grupos diferentes que preservam as mesmas propriedades. Veremos agora que para determinar se dois grupos quaisquer são do mesmo arquétipo, é preciso ser possível estabelecer uma bijeção entre esses grupos.

Definição 1.1.5. Damos o nome de *homomorfismo* de um grupo $(G, *)$ em um grupo $(G', \cdot)$ a toda aplicação $\Psi : G \to G'$ tal que $\Psi(x * y) = \Psi(x) \cdot \Psi(y)$, quaisquer que sejam $x, y \in G$.

Definição 1.1.6. Seja $\Psi : G \to G'$ um homomorfismo de grupos. Se e indica o elemento neutro de G', o seguinte subconjunto de G será chamado de núcleo de Ψ e denotado por $N(\Psi)$:

$$N(\Psi) = \{x \in G \text{ tal que } \Psi(x) = e\}$$

Caso o homomorfismo $\Psi : G \to G'$ for bijetivo, dizemos que Ψ é um *isomorfismo*. E se o isomorfismo for $\Psi : G \to G$ temos um *automorfismo*, o qual denotaremos por $Aut\ G$.

Teorema 1.1.7. *[5] (Teorema de homomorfismo) Sejam G e G' grupos com e e e', respectivamente e $\Psi : G \to G'$ um homomorfismo. Então,*

(a) $Im\Psi = \Psi(G) = \{\Psi(g)$ *tal que* $g \in G\}$ *é um subgrupo de* G'*.*

(b) $N(\Psi) = \{g \in G$ *tal que* $\Psi(g) = e'\}$ *é um subgrupo normal de* G *e mais,* Ψ *é injetiva se, e somente se,* $N(\Psi) = \{e\}$*.*

(c) $G/N(\Psi) \simeq Im\Psi$*.*

No teorema anterior $G/N(\Psi)$ é um grupo do conjunto quociente das classes de equivalência módulo $N(\Psi)$, ou seja, o conjunto $G/N(\Psi) = \{\bar{g} \mid g \in G\}$ onde $\bar{g} = \{ng \mid n \in N(\Psi)\}$.

1.2 ALGUNS RESULTADOS DE CORPOS

Como todo corpo é um anel, iniciemos com a definição de anel, antes de adentrar ao conceito de corpo:

Definição 1.2.1. Seja A um conjunto não vazio, munido de duas operações binárias, denominadas *soma* e *produto*, $+$ e $\cdot$, respectivamente. Assim,

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

Dizemos que $(A, +, \cdot)$ possui estrutura de *anel*, desde que as seguintes propriedades sejam satisfeitas, para quaisquer $a, b, c \in A$:

(i) A soma é associativa, isto é, $(a + b) + c = a + (b + c)$.

(ii) Existe elemento neutro para a soma: $\exists\ 0 \in A$ tal que $a + 0 = a = 0 + a$.

(iii) Existe elemento inverso em relação a soma: para cada $a \in A$, existe $b \in A$ denotado $b = -a$, tal que $a + b = 0 = b + a$.

(iv) A soma é comutativa, isto é, $a + b = b + a$.

(v) O produto é associativo, isto é, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(vi) O produto é distributivo em relação a soma; a esquerda e a direita: $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

Vale ressaltar que em um anel qualquer, o elemento neutro é único.

Chamamos de *anel comutativo* se $x \cdot y = y \cdot x$ para todo $x, y \in A$.

Podemos ter um anel com *divisores de zero* se existem $x, y \in A$, de modo que $x \cdot y = 0$ para $x \neq 0$ e $y \neq 0$. Sendo que, todo anel comutativo sem divisores de zero, onde a unidade, 1_A, (elemento neutro multiplicativo) for diferente de zero, é denominado *anel de integridade*.

Definição 1.2.2. Sejam $(A, +, \cdot)$ um anel e L um subconjunto não vazio de A. Dizemos que L é um subanel de A se:

(i) L é fechado para as operações que fazem o conjunto A ter estrutura de anel;

(ii) $(L, +, \cdot)$ também é um anel.

Definição 1.2.3. Sejam A e A' dois aneis com unidade. Uma aplicação $f : A \to A'$ é um homomorfismo de aneis se ela é compatível com as estruturas de aneis, isto é, se

(i) $f(x + y) = f(x) + f(y), \forall\, x, y \in A$.

(ii) $f(x \cdot y) = f(x) \cdot f(y), \forall\, x, y \in A$.

(iii) $f(1_A) = 1_{A'}$.

Caso f seja um homomorfismo bijetivo, dizemos que f é um isomorfismo. E dois aneis são isomorfos se $f : A \to A'$ for um *isomorfismo*. Além disso, os isomorfismos de A sobre si mesmo são reconhecidos por *automorfismos* de A.

Semelhante ao Teorema 1.1.7 temos o seguinte:

Teorema 1.2.4. *[5] (Teorema de isomorfismo) Sejam A e A' anéis e $f : A \to A'$ um homomorfismo. Então,*

(a) $Im\ f = \{f(a) : a \in A\}$ *é um subanel de* A'.

(b) $N(f) = \{a \in A : f(a) = 0'\}$ *é um subanel de* A *e,* f *é injetiva se, e somente se,* $N(f) = 0$.

(c) $A/N(f) \simeq Im\ f$.

Um *corpo* é um anel de integridade onde todo elemento não-nulo é invertível em relação à multiplicação.

Definição 1.2.5. Seja K um domínio de integridade. Se para todo $x \in K - \{0\}$, existe $y \in K$ tal que $x \cdot y = 1$, K recebe o nome de *corpo*.

Caso um *subanel* $(B, +, \cdot)$ de um *corpo K* seja também um corpo, dizemos que $(B, +, \cdot)$ é um *subcorpo*.

Seja K um corpo qualquer. Vamos denotar $K[x]$ o conjunto de todos os polinômios $p(x)$ sobre K, em uma indeterminada x sendo, $p(x) = a_0 + a_1x + ... + a_mx^m$ onde $a_i \in K$, $\forall\, i \in \mathbb{N}$ e $\exists\, n \in \mathbb{N}$ tal que $a_j = 0\ \forall j \geq n$.

Perceba que $(K[x], +, \cdot)$ é um anel de integridade, onde se $p(x), q(x) \in K[x]$, sendo $p(x) = \sum a_ix^i$ e $q(x) = \sum b_ix^i$, as operações são definidas por:

$$p(x) + q(x) = c_1 + ... + c_kx^k + ..., \text{ onde } c_i = (a_i + b_i) \in K$$

$$p(x) \cdot q(x) = \sum c_kx^k \text{ onde } c_k = \sum_{i=0}^{k} a_ib_{k-i}$$

e mais ainda, o elemento neutro de $(K[x], +, \cdot)$ é o polinômio nulo $p(x) = 0$. Assim, se $r(x) \cdot s(x) = 0$, temos que ter, ou $r(x) = 0$ ou $s(x) = 0$, logo, *sem divisores de zero*. A *unidade* é o polinômio constante $f(x) = 1$ e, claramente, o anel é *comutativo*, dado que o produto dos coeficientes a_ib_{k-i} é comutativo.

Os polinômios que possuem inverso multiplicativo são os polinômios constantes não nulos em $K[x]$, pois, sendo $p(x), q(x) \in K[x] - \{0\}$, se $p(x) \cdot q(x) = 1$, só pode que $p(x) = a$ ou $q(x) = a$, assim, nos referimos a um *polinômio inversível*.

Se n é o maior inteiro tal que $a_n \neq 0$, então dizemos que n é o *grau do polinômio* e escrevemos $\partial p(x) = n$.

Dado um polinômio $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$, definimos a derivada formal de $f(x)$ como sendo o polinômio $f'(x) = a_1 + 2a_2x + ... + na_nx^{n-1} \in K[x]$.

Se $f(x), g(x) \in K[x]$ e $a \in K$ segue imediatamente as seguintes regras: $(f(x)+g(x))' = f(x)'+g(x)'$, $(a \cdot f(x))' = a \cdot f(x)'$; $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.

Teorema 1.2.6. *[6] Seja $p(x) = a_nx^n + ... + a_0$ um polinômio em K. Suponhamos ainda que $p(x)$ tenha grau $n \geq 0$, isto é, $p(x) \neq 0$. Então, $p(x)$ tem no máximo n raízes em K.*

Ao se trabalhar com raízes de um polinômio pode ocorrer que um mesmo polinômio tenha raízes múltiplas, dado esse fato, podemos fatorar um polinômio em função de suas raízes, do seguinte modo:

Definição 1.2.7. Se $f(x) \in \mathbb{R}[x]$ é um polinômio de grau $n \geq 1$ e $\alpha_1, \alpha_2, ..., \alpha_r$ são todas as distintas raízes de $f(x)$ em $\mathbb{C}$ temos que, $f(x) = c \cdot (x - \alpha)^{m_1}...(x - \alpha_r)^{m_r}$ em $\mathbb{C}[x]$

onde $c \in K$ e $r, m_1, ..., m_r$ são inteiros positivos.

Denominamos o inteiro m_i de *multiplicidade da raiz* α_i. E no caso de $m_i = 1$ dizemos que α_i é uma *raiz simples* de $f(x)$.

Teorema 1.2.8. *[5] (Algoritmo da divisão) Sejam* $f(x), g(x) \in K[x]$ *e* $g(x) \neq 0$. *Então, existem únicos* $q(x), r(x) \in K[x]$ *tais que* $f(x) = q(x) \cdot g(x) + r(x)$ *onde ou* $r(x) = 0$ *ou* $\partial r(x) < \partial g(x)$.

Definição 1.2.9. Um polinômio não nulo e não inversível $p(x) \in K[x]$ se diz irredutível sobre K se uma decomposição de $p(x)$ em um produto de dois fatores de $K[x]$ só for possível com um dos fatores inversível, ou seja, $p(x) = f(x) \cdot g(x)$, então, $f(x)$ é inversível ou $g(x)$ é inversível.

Se $p(x)$ não for irredutível sobre K dizemos que $p(x)$ é redutível.

Seja $p(x) = a_0 + a_1x + a_2x^2 + ... + x^n$ um polinômio não nulo de $K[x]$. Denominamos $p(x)$ de *polinômio mônico* em $K[x]$. E ao único polinômio $p(x) \in K[x]$ mônico (de menor grau) irredutível em $K[x]$ tal que $p(\alpha) = 0$ e $\alpha \in L \supset K$ representaremos por $p(x) = irr(\alpha, K)$.

Definição 1.2.10. Seja $p(x) \in K[x]$. Quando $p(x)$ e sua derevida forem primos entre si, o polinômio $p(x)$ é dado como polinômio separável.

Em particular, se $p(x) \in K[x]$ for irredutível em $K[x]$, então, $p(x)$ é separável.

Definição 1.2.11. Seja K um corpo. Se $L \supset K$ é um corpo, L é uma extensão de K.

Denotamos toda *extensão de corpos* por $L|K$. Vale ressaltar, que um polinômio pode ser irredutível em K e não ser irredutível em uma extensão L de K.

Para o próximo teorema, precisamos explorar um subanel especial, o *ideal de um anel* e *ideal maximal*, vejamos:

Definição 1.2.12. [4] Seja $(A, +, \cdot)$ um anel e I um subconjunto não vazio de A. Dizemos que I é um *ideal* de A se

(i) $x + y \in I$, para todo $x, y \in I$

(ii) $ax \in I$, para todo $x \in I$ e para todo $a \in A$.

Definição 1.2.13. Seja M um ideal em um anel comutativo A. Dizemos que M é um *ideal maximal* se $M \neq A$ e se os únicos ideiais de A que contêm M são o próprio M e A.

Teorema 1.2.14. *[5] Seja A um anel e J um ideal de A. Se $\overline{x} = x + J$ e $A/J = \{\overline{x} : x \in A\}$, então:*

(a) $$\begin{array}{rcccccccc} + & : & A/J \times A/J & \to & A/J & \qquad \cdot & : & A/J \times A/J & \to & A/J \\ & & (\overline{x}, \overline{y}) & \mapsto & \overline{x} + \overline{y} & & & (\overline{x}, \overline{y}) & \mapsto & \overline{x} \cdot \overline{y} \end{array}$$
definem duas operações denominadas soma e produto em A/J.

(b) $(A/J, +, \cdot)$ *é um anel (chamado anel quociente de A por J).*

(c) Se 1 *é a unidade de* A *então* $\overline{1}$ *é a unidade de* A/J.

(d) Se A *é comutativo então* A/J *é comutativo.*

Teorema 1.2.15. *[5] Sejam K um corpo e $p(x) \in K[x]$. Então, as seguintes condições são equivalentes:*

(a) $p(x)$ *é irredutível sobre* K.

(b) $J = K[x] \cdot p(x)$ *é um ideal maximal em* $K[x]$.

(c) $K[x]/J$ *é um corpo, onde* $J = K[x] \cdot p(x)$.

No teorema anterior $K[x]/J$ é um anel do conjunto das classes de equivalência módulo J, ou seja, $K[x]/J = \{\bar{p} : p \in K[x]\}$ onde $\bar{p} = p + J$.

Teorema 1.2.16. *[5] (Critério de Eisenstein) Seja $f(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio em $\mathbb{Z}[x]$. Suponhamos que exista um inteiro primo p tal que:*

(a) $p \nmid a_n$

(b) $p | a_0, a_1, ..., a_{n-1}$

(c) $p^2 \nmid a_0$

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

Exemplo 1.2.17. Seja p um número primo qualquer e seja $p(x) = x^n - p$ um polinômio de grau $n \geq 1$ sobre $\mathbb{Q}$. O próprio primo p se aplica no *critério de Einsenstein*, e portanto $p(x)$ é irredutível sobre $\mathbb{Q}$.

Vamos agora nos ater aos conceitos envolvidos especificamente com as extensões de corpos, dado que, nos próximos capítulos trabalharemos fortemente com essas ideias.

Proposição 1.2.18. *Seja $p(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio não nulo de grau n em $K[x]$. Então, $f(x)$ possui no máximo n raízes em qualquer extensão L de K.*

Definição 1.2.19. Seja $L \supset K$ uma extensão de corpos. Um automorfismo $\sigma : L \to L$ é um $K-$automorfismo se, e somente se, $\sigma(\alpha) = \alpha$, para todo $\alpha \in K$.

Um $K-$ *automorfismo* será designado da seguinte forma: $Aut_K L$.

Proposição 1.2.20. *Seja $L \supset K$ uma extensão de corpos. Então, $G = Aut_K L = \{\sigma$ tal que $L \to L$, automorfismo tal que $\sigma|_K = I\}$ é um grupo com a operação de composição de funções.*

Proposição 1.2.21. *Seja $L|K$ uma extensão de corpos e seja G o grupo dos automorfismos de L, isto é, $G = Aut\ L$. Podemos provar facilmente que $H = Aut_K L = \{\sigma \in G$ tal que $\sigma(a) = a\ \forall\ a \in K\}$ é um subgrupo de G.*

Proposição 1.2.22. *Seja $f(x) \in K[x]$ e seja L um corpo de raízes de $f(x)$ sobre K. Se $\sigma : L \to L$ é um K-automorfismo de L e α é uma raiz de $f(x)$, então $\sigma(\alpha)$ também é uma raiz de $f(x)$.*

2 EXTENSÕES

No presente capítulo, são abordadas as extensões de corpos vinculadas as equações polinomiais, dado que, ao considerar determinado subcorpo, este pode não possuir todas as raízes de um polinômio que o pertença, mas, podemos determinar outro corpo que contenha o subcorpo, pelo processo de adjunção de raízes do polinômio, caracterizando o novo corpo como uma "cópia" do subcorpo inicial.

Algumas extensões possuem características próprias, como as *extensões algébricas, extensões transcendentes, extensões cíclicas*. Essas extensões citadas, são apresentadas no decorrer deste capítulo, juntamente com algumas definições de *Álgebra Linear* com propósito de explicitar equivalências úteis para o próximo capítulo.

2.1 EXTENSÕES ALGÉBRICAS

Considere a extensão $L|K$ onde $\alpha \in L|K$ e $\alpha \notin K$ uma raiz de um polinômio $p(x)$ não-nulo tal que $p(x) \in K[x]$.

Definição 2.1.1. Suponhamos que $L|K$ é uma extensão, e que $\alpha \in L$. Se houver um polinômio $p = a_n x^n + ... + a_0 \in K[x]$ para o qual $p(\alpha) = 0$, então, dizemos que α é algébrico sobre K. Caso contrário, dizemos que α é transcendente sobre K.

Perceba que, na Definição 2.1.1 explicitamos quando um elemento é algébrico, mas também, podemos definir uma *extensão algébrica*:

Definição 2.1.2. Para todo $\alpha \in L|K$, α é algébrico sobre K, a extensão é dita *algébrica*.

Caso $\alpha \in L|K$, vamos denotar $K[\alpha] = \{p(\alpha) : p(x) \in K[x]\}$.

Vamos agora explorar algumas extensões que são algébricas, e mostrar que há elementos algébricos nessas extensões, cada qual associado a um polinômio.

Exemplo 2.1.3. Seja $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\}$. Temos que $\mathbb{Q}[\sqrt{2}]$ é uma *extensão algébrica* de $\mathbb{Q}$. Para $\alpha = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ e $f(x) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x]$, temos que,

$f(x) = (x-a)^2 - 2b^2$ sendo $f(\alpha) = 0$, donde podemos afirmar que $\alpha = a + b\sqrt{2}$ é algébrico sobre $\mathbb{Q}$.

Exemplo 2.1.4. Seja $L \supset \mathbb{Q}$, $L = \mathbb{Q}[\sqrt[4]{2}]$ e $f(x) = x^4 + 3x - 2 \in \mathbb{Q}[x]$. Assim, $f(\sqrt[4]{2}) = (\sqrt[4]{2})^4 + 3\sqrt[4]{2} - 2 = 3\sqrt[4]{2} \in \mathbb{Q}[\sqrt[4]{2}]$.

Vale ressaltar que o número π, bem como $\sqrt{\pi}$ são *transcendentes* sobre $\mathbb{Q}$. Mas, $\alpha = \sqrt{\pi}$ é algébrico em $\mathbb{Q}[\pi]$ pois $\alpha^2 - \pi = 0$.

Nesse contexto, podemos pensar quanto as equivalências entre as extenções algébricas, por exemplo, entre $\mathbb{Q}[\alpha]$ e $\mathbb{Q}[\beta]$, onde $\alpha = \sqrt[3]{2}$ e $\beta = \sqrt[3]{2}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) \in \mathbb{C}$ sendo α e β raízes de $p(x) = x^3 - 2 \in \mathbb{Q}$. Essa relação de equivalência estabelecemos com base nos isomorfismos entre corpos. Vejamos o seguinte teorema:

Teorema 2.1.5. *[5] Se $\alpha \in L|K$ e se $\Psi : K[x] \to L$ é definida por $\Psi(f(x)) = f(\alpha)$, então Ψ é um homomorfismo tal que:*

(i) $Im\ \Psi = K[\alpha]$, $K \subset K[\alpha] \subset L$.

(ii) α *é transcendente sobre* $K \Leftrightarrow N(\Psi) = 0$.

(iii) se α *é algébrico sobre* K *e* $p(x) = irr(\alpha, K)$, *então* $N(\Psi) = K[x] \cdot p(x)$ *é um ideal maximal de* $K[x]$.

(iv) $\frac{K[x]}{N(\Psi)} \simeq K[\alpha]$.

Demonstração:

(i) Seja $f(x) \in K[x]$, $f(x) = a_0 + a_1x + ... + a_nx^n$. Temos que, $f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n$, logo, $f(\alpha) \in K[\alpha]$. Portanto, $Im\ \Psi \subset K[\alpha]$. Vamos agora, mostrar que $K[\alpha] \subset Im\ \Psi$. Considere $f(x) \in K[x]$. Como $\alpha \in L|K$, $f(\alpha) \in K[\alpha]$ e $f(\alpha) \in L$, logo, $K[\alpha] \subset Im\ \Psi$. Agora, seja $k \in K$. Para todo $p(x) \in K[x]$ sendo $p(x) = k_0 + k_1x + k_2x^2 + ... + k_nx^n$, basta considerar $k_i = 0 \in K$, $i \in \{1, ..., n\}$ que teremos $p(x) = k_0$, donde $p(\alpha) = k_0 \in K[\alpha]$, então, $K[\alpha]|K$.

(ii) Seja α transcendente sobre K, ou seja, $\forall f(x) \in K[x]$ onde $f(x) \neq 0$, $f(\alpha) \neq 0$. Sabemos que $N(\Psi) = \{f(x) \in K[x] : f(\alpha) = 0\}$, mas como α é transcendente, segue que, o núcleo da Ψ só pode ser composto pelo polinômio nulo $f(x) = 0$. Por outro lado, suponha $N(\Psi) \neq \{0\}$ e seja $f(x) \in N(\Psi)$ assim $f(\alpha) = 0$ absurdo, pois, $f(\alpha) \neq 0$, logo, $N(\Psi) = 0$.

(iii) Seja $h(x) \in N(\Psi)$, donde $h(\alpha) = 0$. Pelo algoritmo da divisão 1.2.8, $h(x) = f(x)p(x) + r(x)$, onde $r(x) = 0$ ou $\partial r(x) < \partial p(x)$, no caso, segue que $r(x) = 0$, logo, $h(x) = f(x)p(x) \in K[x] \cdot p(x)$ e $h(\alpha) = f(\alpha)p(\alpha)$ implica $h(\alpha) = 0$, consequentemente, $h(x) = 0 \in N(\Psi)$. Portanto, $N(\Psi) \subset K[x] \cdot p(x)$. Por outro lado, seja $h(x) \in K[x] \cdot p(x)$. Assim $h(x) = p(x)f(x)$ onde $p(x), f(x) \in K[x]$. Segue que $h(\alpha) = 0$ implica em $p(\alpha) = 0$ ou $f(\alpha) = 0$, donde temos, sem perda de generalidade, que $h(x) \in K[x] \cdot p(x)$. Por isso, $K[x] \cdot p(x) \subset N(\Psi)$. Dessa forma, $N(\Psi) = K[x] \cdot p(x)$.

(iv) Considere $N(\Psi) \neq \varnothing$ dado que $f(x) \in N(\Psi)$. Pelo item (iii) desse teorema, $N(\Psi)$ é um ideal maximal, portanto, a demonstração é de imediato pelo Teorema 1.2.4.

□

Exemplo 2.1.6. Seja $\alpha = \sqrt[3]{2} \in \mathbb{R}$ e $f(x), p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Perceba que, pelo Algoritmo da Divisão 1.2.8, existe $q(x), r(x) \in \mathbb{Q}[x]$ tais que $f(x) = q(x)p(x) + r(x)$, onde, para $f(\alpha) = 0$ temos que ter $q(x)(x^3 - 2) = 0$ e $r(x) = 0$, portanto, basta considerar $x = \sqrt[3]{2}$ em $(x^3 - 2)$ e como, $r(x) = a + bx + cx^2$ com $a, b, c \in \mathbb{Q}$, segue que, $r(\sqrt[3]{2}) = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$. Pelo Teorema 2.1.5, sabemos que, $\frac{Q[x]}{Q[x]p(x)} \simeq Q[\alpha]$, no caso, $\frac{Q[x]}{Q[x](x^3-2)} \simeq Q[\sqrt[3]{2}]$.

Os dois próximos corolários, podem ser demonstrados com base no Teorema 2.1.5.

Corolário 2.1.7. *Seja $\alpha \in L|K$.*

(a) Se α é algébrico sobre K, então $K[\alpha]$ é um subcorpo de L que contém K.

(b) Se α é transcendente sobre K, então $K[\alpha]$ é um subdomínio de L isomorfo ao domínio $K[x]$ dos polinômios em uma indeterminada x.

Demonstração: Seja $\alpha \in L|K$ e $\Psi : K[x] \to L$ definida por $f(x) \mapsto f(\alpha)$.

(a) Seja α algébrico sobre K. Considere $p(x) \in K[x]$ de modo que $p(x) = irr(\alpha, K)$. Como, pelo item (iii) do Teorema 2.1.5 $N(\Psi) = K[x] \cdot p(x)$ é um *ideal maximal*, e pelo item (iv) $\frac{K[x]}{N(\Psi)} \simeq K[\alpha]$, então, $K[\alpha]$ é um corpo.

(b) Seja α transcendente sobre K. Pelo item (ii) do Teorema 2.1.5 segue que $N(\Psi) = 0$. E pelo item (iv) temos que $\frac{K[x]}{N(\Psi)} \simeq K[\alpha]$, portanto, $K[\alpha] \simeq K[x]$.

□

Corolário 2.1.8. *Se $\alpha, \beta \in L|K$ são raízes de um mesmo polinômio irredutível sobre K, então $K[\alpha]$ e $K[\beta]$ são corpos isomorfos.*

Demonstração: Seja $\alpha, \beta \in L$ raízes de um mesmo polinômio $p(x)$ tal que $p(x) = irr(\alpha, K) = irr(\beta, K)$. Considere $\Psi : K[x] \to L$ definida por $f(x) \mapsto f(\alpha)$. Pelo item (iii) do Teorema 2.1.5, sabemos que $N(\Psi) = K[x] \cdot p(x)$, e pelo item (iv), temos que $\frac{K[x]}{N(\Psi)} \simeq K[\alpha]$ e $\frac{K[x]}{N(\Psi)} \simeq K[\beta]$, logo, $K[\alpha] \simeq K[\beta]$. □

No Corolário 2.1.8 fica explícito que a relação de equivalência que pode ser estabelecidade entre corpos adjuntados a diferentes raízes de um mesmo polinômio irredutível é o isomorfismo entre esse corpos.

Proposição 2.1.9. *Seja $L|K$, $\alpha \in L$ algébrico sobre K. Se o grau do polinômio irredutível é n, então*

(a) $\forall f(x) \in K[x]$, $f(\alpha)$ *pode ser expresso de modo único na forma*

$f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$, *onde* $a_i \in K$.

(b) $K[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in K\}$ *é um subcorpo de L que contém K.*

(c) se $K = \mathbb{Z}_p$, então $K[\alpha]$ é um corpo contendo exatamente p^n elementos.

Demonstração: [5], página 90.

□

Observação 2.1.10. Para todo $\alpha = \sqrt[n]{p} \in \mathbb{R}$ com n sendo um número inteiro maior ou igual a dois e p primo maior ou igual a dois, que é uma raiz real do polinômio $x^n - p$ irredutível sobre $\mathbb{Q}$, de acordo com o *critério de Eisenstein* 1.2.16, teremos que $\mathbb{Q}[\alpha]$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$ e, mais ainda,

$$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}, i = 0, ..., n-1\}.$$

Vimos que $K[\alpha]$ é um corpo, e sabendo que $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$ com $\alpha \in L|K$, pode acontecer que a inclusão de um elemento ao menor corpo da extensão seja o próprio corpo da extensão:

Definição 2.1.11. Uma extensão $L|K$ tal que $L = K[\alpha]$ para algum $\alpha \in L$ denominamos de *extensão simples*.

Exemplo 2.1.12. Seja a extensão $L|\mathbb{R}$ e o polinômio $p(x) = x^2 + 1 \in \mathbb{R}$. Perceba que, $i \in \mathbb{C}$ é uma raiz de $p(x)$ e, logo, $L = \mathbb{R}[i]$, e mais ainda, $\mathbb{R}[i] \simeq \frac{\mathbb{R}[x]}{\mathbb{R}[x]p(x)} \simeq \mathbb{C}$, portanto, temos que o conjunto $\mathbb{C}$ é uma *extensão simples* dos $\mathbb{R}$. Vale ressaltar que, pela Proposição 2.1.9, $\mathbb{R}[i] = \{a_0 + a_1 i + ... + a_{n-1} i^{n-1} : a_j \in \mathbb{R}, j = 0, ..., n-1\}$.

Em alguns casos, podemos ter extensões de corpos que são *extensões simples [2.1.11]* adjuntadas com mais de um elemento, embora, é possível obter outra *extensão algébrica* adjuntada com somente um elemento, igual a extensão inicial.

Exemplo 2.1.13. Considere $L \supset \mathbb{Q}$ com $L = \mathbb{Q}[i, -i, \sqrt{5}, -\sqrt{5}]$. Vamos mostrar que essa extensão é simples. Considere $L' = \mathbb{Q}[i + \sqrt{5}]$. Provemos que $L = L'$. É fácil ver que $L' \supset L$, pois $i, \sqrt{5} \in L$, logo, a operação desses elementos resulta em um elemento de L, então, temos que $i + \sqrt{5} \in L$. Agora, precisamos ter $L \supset L'$, mais precisamente, que $i, \sqrt{5} \in L'$. Sabemos que $(i + \sqrt{5})^2 \in L'$, e sendo $(i + \sqrt{5})^2 = 4 + 2i\sqrt{5}$, operando $-1(i+\sqrt{5})(4+2i\sqrt{5}) = -14i-2\sqrt{5}$. Agora, fazendo $(-14i-2\sqrt{5})+2(i+\sqrt{5})$ resulta em $-12i$, portanto, $-12i \in L'$, bem como, i, então, $(i + \sqrt{5}) - i = \sqrt{5} \in L'$. Portanto, $L' \subseteq L$. Assim, concluímos que $\mathbb{Q}[i, -i, \sqrt{5}, -\sqrt{5}]|\mathbb{Q}$ é uma *extensão simples*.

Na Definição 1.2.7 temos a fatoração de um polinômio e a multiplicidade de suas raízes. Vejamos agora, uma proposição que diz respeito a um polinômio somente com raízes de multiplicidade 1:

Proposição 2.1.14. *Seja $f(x) \in K[x]$, $\partial f(x) = n \geq 1$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$. Então,*

(a) α é raiz simples de $f(x) \Leftrightarrow f(\alpha) = 0$ e $f'(\alpha) \neq 0$.

(b) se $f(x)$ é irredutível sobre K, então todas as raízes de $f(x)$ são simples.

Demonstração:

(a) Seja $f(x) \in \mathbb{K}[x]$ com multiplicidade $m \geq 1$ onde $f(\alpha) = 0$ com $\alpha \in \mathbb{C}$. Se $\alpha \in \mathbb{C}$, segue que, $f(x) = (x - \alpha)^m \cdot g(x)$ onde $g(x) \neq 0 \in \mathbb{K}[x]$ e $g(\alpha) \neq 0$, uma vez que, se $g(x) = 0$, $f(x)$ também o será, e não o é, dado que, $\partial f(x) \geq 1$. Derivando $f(x)$ temos que $f'(x) = m \cdot (x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x)$. Assim, para $m = 1$, segue que $f(x) = (x - \alpha) \cdot g(x)$ sendo que $f(\alpha) = (\alpha - \alpha) \cdot g(\alpha) = 0 \cdot g(\alpha) = 0$ e, mais ainda, $f'(x) = g(x) + (x-\alpha) \cdot g'(x) \Rightarrow f'(\alpha) = g(\alpha) + (\alpha - \alpha) \cdot g'(\alpha)$ donde $f'(\alpha) \neq 0$. Agora, fica fácil perceber que, se $f(\alpha) = 0$ e $f'(\alpha) \neq 0$, α só será raiz simples de $f(x)$ se $\partial f(x) \geq 2$, visto que, para $m = 2$ temos

$$f'(x) = 2 \cdot (x - \alpha) \cdot g(x) + (x - \alpha)^2 \cdot g'(x) \Rightarrow f'(\alpha) = 0,$$

mas por hipótese, $f(\alpha) \neq 0$.

(b) Seja $f(x) = irr(\alpha, K)$ e $p(x) = irr(\alpha, K)$. Pelo Algoritmo da Divisão 1.2.8 segue que $\exists\, q(x), r(x) \in K[x]$ tais que: $f(x) = q(x)p(x) + r(x)$ onde $r(x) = 0$ ou $\partial r(x) < \partial p(x)$. Como α é uma raiz de $f(x)$ temos que $f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = 0 \Rightarrow r(\alpha) = f(\alpha) - q(\alpha)p(\alpha) \Rightarrow r(\alpha) = 0$. Como $p(x)$ é irredutível e $p(\alpha) = 0$ segue que $r(x) = 0$. Daí $f(x) = q(x)p(x)$. Sabemos que $f(x)$ é irredutível, portanto, temos que $f(x) = a \cdot p(x)$, com $a \in K$. Se $m > 1$, pelo item (a) desta proposição temos $f'(\alpha) = a \cdot p'(\alpha) = 0 \Rightarrow p'(\alpha) = 0$, mas isso contradiz o fato da minimalidade do grau de $p(x)$, já que $\partial p'(x) < \partial p(x)$. Portanto, $m = 1$ e α é raiz simples.

□

A partir da caracterização de *raiz simples* definimos *corpo de decomposição* de um polinômio $f(x) \in K[x]$ sobre K:

Definição 2.1.15. Seja $L|K$ uma extensão e $f(x) \in K[x]$ com $\partial f(x) \geq 1$ tal que f tem uma decomposição em L da seguinte forma: $f(x) = c \cdot (x - \alpha_1)...(x - \alpha_n)$, onde $c \in L$ e $L = K[\alpha_1, ..., \alpha_n]$; denominamos L o corpo de decomposição de f sobre K.

Um *corpo de decomposição* denotaremos por $L = Gal(f, K)$. Esse corpo é o menor subcorpo de L que contém K e todas as raízes de $f(x)$ pertencem a $\mathbb{C}$, uma vez que, podemos dizer que esse corpo é gerado somente por *raízes simples* de $f(x)$.

Vamos ver outra forma de definir um $Gal(f, K)$: seja $f(x) \in K[x]$ e $\alpha_1, ..., \alpha_r$ as *raízes simples* de $f(x) \in \mathbb{C}$. Consideremos, $K_0 = K$, $K_1 = K[\alpha_1]$, $K_2 = K_1[\alpha_2]$, ..., $K_r = K_{r-1}[\alpha_r]$, sendo $K \subset K_1 \subset K_2 \subset ... \subset K_r$. Perceba que, K_r é o menor subcorpo de $\mathbb{C}$ contendo K e $\alpha_1, ..., \alpha_r$ e, portanto, $K_r = Gal(f, K)$, e como $K_r = K_{r-1}[\alpha_r]$ podemos denotar que $K_r = K[\alpha_1, ..., \alpha_r] = Gal(f, K)$. Vale ressaltar que, qualquer que seja a ordem que pegamos as raízes, ainda temos um *corpo de decomposição*. Este processo é conhecido por *adjunção de raízes*.

Exemplo 2.1.16. Considere $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. O polinômio $p(x)$ possui três raízes, donde duas são não-reais, a saber: $\alpha = \sqrt[3]{2}$, $\beta = -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2}\sqrt{3}i}{2}$ e $\overline{\beta} = -\frac{\sqrt[3]{2}}{2} - \frac{\sqrt[3]{2}\sqrt{3}i}{2}$. Assim, podemos dizer que o *corpo de decomposição* de $p(x)$ sobre $\mathbb{Q}$ é $\mathbb{Q}[\alpha, \beta, \overline{\beta}]$. Mas, observe que, sendo $\beta = \alpha(-\frac{1}{2} + \frac{\sqrt{3}i}{2})$ e $\overline{\beta} = \alpha(-\frac{1}{2} - \frac{\sqrt{3}i}{2})$ ao fazermos β^2 obtemos justamente $\alpha^2\overline{\beta}$, portanto, $Gal(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta, \overline{\beta}] = \mathbb{Q}[\alpha, \beta]$.

Adentraremos agora a acepção de *grau de uma extensão*. Obviamente, o grau de uma extensão possui relação com o grau do polinômio mônico irredutível da extensão. Para tal, se faz necessário abordar alguns conceitos de *Álgebra Linear* como *espaço vetorial, base, dimensão*, os quais serão expostos em apêndice A.

Consideremos a seguir, L como um $K-$*espaço*, ou seja, um *espaço vetorial* sobre K. A dimensão do $K-$*espaço* L é denotada por $[L : K]$ e conhecida como *o grau da extensão* $L|K$. Desse modo, temos que *o grau da extensão* é a cardinalidade de qualquer base de L sobre K.

Definição 2.1.17. Seja L uma extensão de K. Se L for um espaço vetorial de dimensão finita sobre K, temos que L é uma *extensão finita*.

Caso contrário, diremos que $L|K$ é uma *extensão infinita*.

Exemplo 2.1.18. O espaço vetorial $\mathbb{R}$ sobre $\mathbb{Q}$ é infinito, obviamente, a extensão $E \supset \mathbb{Q}$ com $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}, ..., \sqrt{p}, ...]$ também não é finita, já que, E é um subcorpo dos $\mathbb{R}$ pelo fato de $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}] \subset ...$ ser uma *cadeia ascendente* própria, sendo a *extensão algébrica*.

Proposição 2.1.19. *Seja K um corpo e $L|K$ uma extensão de K. Então,*

(a) se $L|K$ é finita, então $L|K$ é algébrica.

(b) se $\alpha \in L|K$ é um elemento algébrico sobre K e grau de $p(x) = irr(\alpha, K)$ é igual a n, então $1, \alpha, ..., \alpha^{n-1}$ é uma base do espaço vetorial $K[\alpha]$ sobre K e $[K[\alpha] : K] = n < \infty$.

(c) se $\alpha \in L|K$ é um elemento transcendente sobre K, então $K[\alpha]|K$ é uma extensão infinita.

Demonstração:

(a) Seja $[L : K]$ uma extensão finita. Então, por Definição de *extensão finita (2.1.17)*, $[L : K] = n < \infty$, isto é, L tem dimensão finita quando visto como espaço vetorial sobre K. Assim, o conjunto de quaisquer $n + 1$ vetores não nulos é linearmente dependente. Seja $\alpha \in L$ e consideremos $1, \alpha, ..., \alpha^n$. Então, existem $c_o, c_1, ..., c_n \in K$, não todos nulos, tais que $c_0 + c_1\alpha + ... + c_n\alpha^n = 0$. Deste modo, α é raiz do polinômio não nulo $f(x) = c_0 + c_1x + ... + c_nx^n$. Logo, α é algébrico sobre K.

(b) Seja $\alpha \in L|K$ um elemento algébrico sobre K tal que grau de $irr(\alpha, K) = n$. Mas, pela Proposição 2.1.9 todo elemento de $K[\alpha]$ pode ser escrito de modo único como combinação linear de $1, \alpha, ..., \alpha^{n-1}$ sobre K. Assim, $1, \alpha, ..., \alpha^{n-1}$ é uma base de $K[\alpha]$ sobre K. Logo, $[K[\alpha] : K] = n$.

(c) Decorre imediatamente dessa proposição, pois usando a contrapositiva, suponha que $K[\alpha] \supset K$ é uma extensão algébrica, logo, pelo item *(a)*, α é algébrico.

□

Pela proposição anterior, fica evidente que a recíproca do item (a) não é verdadeira, para tanto, podemos pensar que, se a extensão $\mathbb{R} \supset \mathbb{Q}$ fosse finita, seria também algébrica pela Proposição 2.1.19 e, claramente, π seria algébrico sobre os $\mathbb{Q}$, o que é um absurdo. Portanto, nem toda extensão algébrica é finita, reveja o exemplo 2.1.18.

Corolário 2.1.20. *Seja $\alpha \in L|K$. Então as seguintes afirmações são equivalentes:*

(i) α *é algébrico sobre* K

(ii) $[K[\alpha] : K] = n < \infty$

(iii) $K[\alpha]$ *é uma extensão algébrica de* K.

Demonstração:

$(i) \Rightarrow (ii)$ Note que, se α é algébrico sobre $L|K$, então, existe $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Seja $p(x) = irr(\alpha, K)$, com $\partial p(x) = n$. Pela minimalidade do grau de $p(x)$ e pelo item *(b)* da Proposição 2.1.19 temos que $1, \alpha, ..., \alpha^{n-1}$ é uma base de $K[x]$ e $[K[\alpha] : K] = n < \infty$.

$(ii) \Rightarrow (iii)$ Suponha $[K[\alpha] : K] = n < \infty$. Então, pela Proposição 2.1.19 item (a) temos que $K[\alpha]$ é uma extensão algébrica de K.

$(iii) \Rightarrow (i)$ Sendo $K[\alpha]$ uma extensão algébrica sobre K, por definição α é algébrico sobre K. □

Teorema 2.1.21. *[6] Seja L uma extensão finita de K, e seja M uma extensão finita de L. Então, M será uma extensão finita de K, e $[M : K] = [M : L] \cdot [L : K]$.*

Demonstração: Seja $\{\alpha_1, ..., \alpha_n\}$ uma base para o espaço vetorial L sobre K, e $\{\beta_1, ..., \beta_m\}$ uma base de M sobre L. Deste modo, para todo $i \in \{1, ..., n\}$ temos $\alpha_i \in L$ e para todo $j \in \{1, ..., m\}$ temos $\beta_j \in M$. Vamos mostrar que $\{\alpha_i\beta_j\}$ formam uma base para o espaço vetorial M sobre K. Primeiramente, vamos mostrar que $\{\alpha_i\beta_j\}$ é linearmente independente.

Consideremos $\sum_{i,j} x_{ij}\alpha_i\beta_j = 0$, $x_{i,j} \in K$. Como $x_{ij}\alpha_i \in L$ e L é um corpo, temos que $\sum_i x_{ij}\alpha_i \in L$; assim, podemos escrever $\sum_j (\sum_i x_{ij}\alpha_i)\beta_j = 0$. Da independência linear de $\beta_1, ..., \beta_m$ sobre L, concluímos que $\sum_i x_{ij}\alpha_i = 0$, para cada j, e, da idependência de $\alpha_1, ..., \alpha_n$ sobre K, segue que $x_{ij} = 0$ para todos i, j, portanto, os elementos $\alpha_i\beta_j$ são linearmente independentes.

Agora, vamos mostrar agora que qualquer elemento do espaço vetorial de M sobre K pode ser escrito como combinaçao linear de $\alpha_i\beta_j$. Seja $v \in M$. Temos que $v = \sum_j w_j\beta_j = w_1\beta_1 + ... + w_m\beta_m$, com alguns elementos $w_j \in L$. Podemos exprimir w_j como uma combinação linear de $\alpha_1, ..., \alpha_n$ com coeficientes em K, ou seja, $w_j = \sum_i c_{ij}\alpha_i$. Substituindo, temos $v = \sum_j \sum_i c_{ij}\alpha_i\beta_j = \sum_{i,j} c_{ij}\alpha_i\beta_j$, e assim, os elementos $\alpha_i\beta_j$ geram M sobre K. □

Corolário 2.1.22. *(Lei da Torre) Se* $K_0 \subseteq K_1 \subseteq ... \subseteq K_n$ *são subcorpos de* $\mathbb{C}$*, então,* $[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}]...[K_1 : K_0]$.

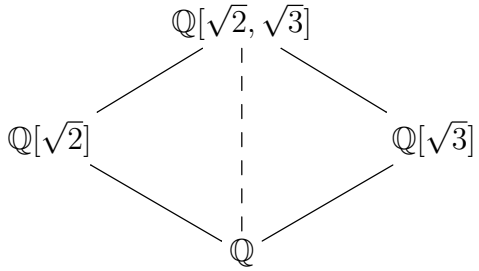
Demonstração: Basta usar o Teorema 2.1.21 e indução sobre n. □

Exemplo 2.1.23. Seja a extensão $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$. Sabemos que $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ é uma extensão finita e de acordo com a Proposição 2.1.19, uma de suas bases é $\{1, \sqrt{2}\}$, pois a raiz do *polinômio mônico irredutível* $x^2 - 2$ sobre $\mathbb{Q}$ é $\alpha = \sqrt{2}$. Já na extensão finita $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}[\sqrt{2}]$ uma de suas bases é $\{1, \sqrt{3}\}$. Então, podemos verificar que

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$
$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2$$
$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

De acordo com o diagrama a seguir, poderíamos ter pensado também em

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

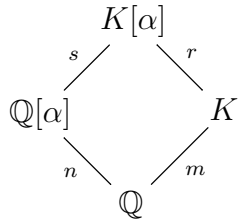


(1)

Observe que, realmente a dimensão da extensão $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ sobre $\mathbb{Q}$ é 4, porque, uma base para a mesma seria $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$, já que $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\ |a,b,c,d \in \mathbb{Q}\}$.

Corolário 2.1.24. *Seja $K \supset \mathbb{Q}$ tal que $[K:\mathbb{Q}] = m$ e seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau n. Se o máximo divisor comum (M.D.C.) de m e n é igual a 1, então $p(x)$ é um polinômio irredutível sobre K.*

Demonstração: Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Considere os corpos $K[\alpha]|\mathbb{Q}[\alpha]$ e suponhamos que $[K[\alpha]:K] = r$ e $[K[\alpha]:\mathbb{Q}[\alpha]] = s$. Como $\partial p(x) = n$ e $p(x) \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$, segue que $[\mathbb{Q}[\alpha]:\mathbb{Q}] = n$ e $[K[\alpha]:K] = r = n$. Assim, pelo Teorema 2.1.21 temos $[K[\alpha]:\mathbb{Q}] = [K[\alpha]:\mathbb{Q}[\alpha]]\cdot[\mathbb{Q}[\alpha]:\mathbb{Q}]$ possui dimensão $s\cdot n$ e $[K[\alpha]:\mathbb{Q}] = [K[\alpha]:K]\cdot[K:\mathbb{Q}] = r\cdot m$, como podemos ver



(2)

donde segue que $s\cdot n = r\cdot m$ e como M.D.C. $\{n,m\} = 1$ vem $n|r$. Mas $r \leq n$ nos diz que $n = r$ e assim $p(x)$ é também irredutível sobre K. □

O próximo corolário aborda o fato de a dimensão de $L|K$ ser a mesma da cardinalidade do conjunto $Aut_K L = \{f \in AutL : f(\lambda) = \lambda, \forall\ \lambda \in K\}$.

Corolário 2.1.25. *Seja $L \supset K \supset \mathbb{Q}$ tal que $[L:K] < \infty$. Então, $[L:K] \geq |Aut_K L|$.*

Demonstração: Introdução à Álgebra [5] página 102. □

O corolário anterior nos garante que $[L:K] \geq |Aut_K L|$ se $L|K \supset \mathbb{Q}$, mas veremos no próximo capítulo que, se $L = Gal(f,K)$ teremos $[L:K] = |Aut_K L|$.

2.2 EXTENSÕES CÍCLICAS

Definimos o *expoente* $exp(G)$ de G como o mínimo múltiplo comum de $\{o(z) \mid z \in G\}$ se existe, caso contrário, $exp(G) < \infty$. Sendo que, $exp(G)$ divide a ordem $o(G)$ do grupo G se está for finita.

Lema 2.2.1. *Seja $exp(G) < \infty$. Então,*

a) existe um $y \in G$ tal que $exp(G) = o(y)$;

b) $exp(G) = o(G)$ se e somente se G for cíclico.

Demonstração: [3], página 107. □

Definição 2.2.2. Seja $L|K$ uma extensão finita. Se existe $f(x) \in K[x]$ tal que $L = Gal(f, K)$, a *extensão $L|K$ é galoisiana*.

Diremos que uma extensão $L|K$ é *cíclica* se $L|K$ for galoisiana e $Aut_K L$ for um grupo cíclico.

Denotaremos por $W_n(K)$ o conjunto das raízes n-ésimas da unidade em K do polinômio $x^n - 1$, ou seja, $W_n(K) = \mathfrak{R}_{x^n-1} \cap K$.

Teorema 2.2.3. *Seja V um subgrupo de $K^* = K - \{0\}$ tal que $exp(V) = m < \infty$. Então, $V = W_m(K)$, e V é cíclico de ordem m.*

Demonstração: Para todo $v \in V$, $o(v)$ divide m, logo, $v \in W_m(K)$; portanto, $V \subseteq W_m(K)$ e $o(v) \leq o(W_m(K)) \leq m$. Por outro lado, $m = exp(V)$ divide $o(V)$; portanto $o(V) = m$ e $V = W_m(K)$. Do Lema 2.2.1 temos que V é cíclico. □

Decorre do teorema anterior o seguinte corolário, o qual a demonstração é de imediato, logo, será omitida.

Corolário 2.2.4. *Seja V um subgrupo de K^* e $o(V) = m$. Então, $V = W_m(K)$, e V é cíclico.*

Denotaremos $\mathscr{P}_n(K)$ o conjunto das raízes primitivas n-ésimas da unidade de K, isto é, dos $\zeta \in K^*$ tais que $o(\zeta) = n$. Considere Ω um corpo fechado que contém K.

Proposição 2.2.5. *Sendo p a característica de K, para qualquer $n \geq 1$ as seguintes condições são equivalentes:*

(i) $W_n(K)$ *tem ordem* n*.*

(ii) $\mathscr{P}_n(K) \neq \varnothing$*.*

(iii) $p \nmid n$ *e* $x^n - 1$ *fatora-se em* $K[x]$ *em fatores lineares.*

Demonstração:

(i) $\Rightarrow$ (ii): Seja $o(W_n(K)) = n$. Existe $z \in W_n(K)$ de modo que $exp(W_n(K)) = o(z)$. Então, $o(W_n(K)) = o(z)$, logo, $W_n(K) = \langle z \rangle$, ou seja, $W_n(K)$ é cíclico. Assim, $o(z) = n$, ou seja, $z \in \mathscr{P}_n(K)$.

(ii) $\Rightarrow$ (iii): Seja $z \in \mathscr{P}_n(K)$. Se p fosse um divisor de n, então teríamos que $p \neq 0$ e $(z^{\frac{n}{p}})^p = z^n = 1$, logo, $z^{\frac{n}{p}} = 1$, o que é impossível. Considere as distintas raízes $1, z, z^2, ..., z^{n-1} \in K$ do polinômio $x^n - 1$, portanto, $x^n - 1 = \prod_{j=0}^{n-1}(x - z^j)$.

(iii) $\Rightarrow$ (i): O polinômio $x^n - 1$ é separável, veja 1.2.10; assim na fatoração $x^n - 1 = (x - y_1) \cdot ... \cdot (x - y_n)$ em $K[x]$ os elementos $y_1, ...y_n$ são distintos dois a dois, logo $W_n(K) = \{y_1, ...y_n\}$ consiste de n elementos. □

Lema 2.2.6. *(a) Para todo $a \in K^*$ temos em $\Omega[x]$ a fatoração*

$$x^n - a = (x - \alpha_1) \cdot (x - \alpha_2) \cdot ... \cdot (x - \alpha_{n-1}) \cdot (x - \alpha_n)$$

com $\{\alpha_j \cdot \alpha_1^{-1} \mid j = 1, ..., n\} = W_n(\Omega) \subseteq K(\mathfrak{R}_{x^n - a})$.

(b) Se n não for divisível por $car(K)$, então, $x^n - a$ será separável e

$$x^n - a = \prod_{\eta \in W_n(\Omega)} (x - \eta \cdot \alpha)$$

ao mesmo tempo que $x^n - a = \prod_{j=0}^{n-1}(x - \zeta^j \cdot \alpha)$, $\forall\ \alpha \in \mathfrak{R}_{x^n - a}$ e todo $\zeta \in \mathscr{P}_n(\Omega)$.

Demonstração: [3], página 125. □

Teorema 2.2.7. *(Abel) Para todo $a \in K^*$ e todo número primo p, as seguintes condições são equivalentes:*

(i) $x^p - a$ *é irredutível em* $K[x]$*;*

(ii) $x^p - a$ *não tem nenhuma raiz em* K*;*

(iii) $a \notin K^p$ *(isto é,* $a \neq c^p$ *para todo* $c \in K$*).*

Demonstração:

$(i) \Rightarrow (ii)$ Seja $x^p - a$ irredutível em $K[x]$; segue que, K não é o corpo de decomposição de $x^p - a$, portanto, as raízes desse polinômio não estão em K.

$(ii) \Rightarrow (iii)$ Suponha que exista um $c \in K$ tal que $c^p = a$. Então, $c^p - a = 0$, já que, $c = \sqrt[p]{a}$, mas, isso contraria o fato de $x^p - a$ ser irredutível em K.

$(iii) \Rightarrow (i)$ Suponha $x^p - a$ redutível em $K[x]$, e seja g um divisor mônico de $x^p - a$, com $\partial g = r < p$; então, existem $\alpha \in \mathfrak{R}_{x^p - a}$ e $\beta_1, \beta_2, ..., \beta_r \in W_p(\Omega)$ tais que $g = (x - \beta_1 \cdot \alpha) \cdot (x - \beta_2 \cdot \alpha) \cdot ... \cdot (x - \beta_r \cdot \alpha)$, logo, $(-1)^r \cdot \beta_1 \cdot ...\beta_r \cdot \alpha^r = g(o) \in K$. Seja $c = \beta_1 \cdot ... \cdot \beta_r \cdot \alpha^r$; então, $c \in K$ e $c^p = \alpha^{p \cdot r} = a^r$. Como $MDC(p, r) = 1$, existem $l, m \in \mathbb{Z}$ tais que $l \cdot r + m \cdot p = 1$; portanto, $a = a^{l \cdot r + m \cdot p} = c^{p \cdot l} \cdot a^{p \cdot m} \in K^p$. □

O próximo teorema nos fornece uma caracterização das extensões cíclicas L de grau n de um dado corpo K, levando em conta que $\mathscr{P}_n(K) \neq \varnothing$.

Teorema 2.2.8. *Seja* $L = K(\mathfrak{R}_{x^n - a})$ *para algum* $a \in K^*$ *e suponhamos que* $\mathscr{P}_n(K) \neq \varnothing$*. Então,*

(a) $L = K(\alpha)$ *para qualquer* $\alpha \in \mathfrak{R}_{x^n - a}$*.*

(b) $L|K$ *é galoisiana, e* $Aut(L|K)$ *é canonicamente isomorfo a um subgrupo de* $W_n(K)$*; portanto,* $Aut(L|K)$ *é cíclico e* $o(Aut(L|K)) = [L : K]$ *divide* n*.*

(c) $[L : K] = n$ *se e somente se* $x^n - a$ *for irredutível em* $K[x]$*.*

Demonstração:

(a) Seja $z \in \mathscr{P}_n(K)$. Pelo Lema 3.2.1 temos $\mathfrak{R}_{x^n - a} = \{z^j \cdot \alpha \mid j = 0, ..., n-1\} \subseteq K(\alpha)$, logo, $L \subseteq K(\alpha) \subseteq L$.

(b) Como $x^n - a$ é separável, a extensão $L|K$ é galoisiana. Para todo $\sigma \in Aut(L|K)$ temos $\sigma\alpha \in \mathfrak{R}_{x^n - a}$, logo, $\frac{\sigma\alpha}{\alpha} \in W_n(\Omega) = W_n(K)$. A aplicação $Aut(L|K) \to W_n(K)$, definida por $\sigma \mapsto \frac{\sigma\alpha}{\alpha}$, é um homomorfismo, pois, $\frac{\sigma\alpha}{\alpha} \cdot \frac{\rho\alpha}{\alpha} = \frac{\sigma\alpha}{\alpha} \cdot \sigma(\frac{\rho\alpha}{\alpha}) = \frac{\sigma(\rho\alpha)}{\alpha}$ $(\sigma, \rho \in Aut(L|K))$; este é injetivo, pois, $\frac{\sigma\alpha}{\alpha} = 1$ se e somente se $\sigma\alpha = \alpha$, se e somente se $\sigma = id_L$. Além disso, ele independe da escolha de $\alpha \in \mathfrak{R}_{(x^n - a)}$, pois $\frac{\sigma(y \cdot \alpha)}{y \cdot \alpha} = \frac{\sigma\alpha}{\alpha}$ para todo $y \in W_n(K)$. Portanto, é um isomorfismo canônico sobre um subgrupo do grupo cíclico $W_n(K)$, logo, $o(Aut(L|K))$ divide $o(W_n(K)) = n$. Como há esse isomorfismo, temos que $Aut(L|K)$ é cíclico, e assim, $o(Aut(L|K)) = [L : K]$.

(c) Seja $x^n - a$ redutível em $K[x]$, assim, o corpo de decomposição desse polinômio é K, logo, a dimensão da extensão $L|K$ é diferente de n.

□

3 TEORIA DE GALOIS

No presente capítulo apresentamos a Teoria de Galois, onde extensões de corpos normais são associadas ao grupo de automorfismos dessas extensões, constituindo o grupo de Galois.

Também é abordado um dos principais resultados da Teoria de Galois: o *Teorema Fundamental de Galois*, o qual estabelece uma correspondência entre extensões intermediárias e subgrupos do grupo de automorfismos de uma extensão galoisiana.

3.1 EXTENSÕES NORMAIS E GALOISIANAS

Os conceitos de extensão normal e extensão galoisiana são fundamentais para adentrar à *correspondência de Galois*, abordada no próxima seção; sendo que, mostraremos que essas extensões possuem uma estrita relação.

Definição 3.1.1. [7] Seja $L|K$ uma extensão. Se cada polinômio irredutível f sobre K que tem pelo menos uma raiz em L possui todas as raízes em L, a extensão é dita *normal*.

Exemplo 3.1.2. Considere a extensão $\mathbb{Q}[\sqrt[4]{2}, i]|\mathbb{Q}$. Considere $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Claramente, $f(x)$ é irredutível sobre $\mathbb{Q}$ e pode ser decomposto em $(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-i\sqrt[4]{2})(x+i\sqrt[4]{2})$ donde, todas as suas raízes pertencem a $\mathbb{Q}[\sqrt[4]{2}, i]$. Portanto, $\mathbb{Q}[\sqrt[4]{2}, i]|\mathbb{Q}$ é uma *extensão normal*.

Definição 3.1.3. Seja L e M duas extensões de $\mathbb{Q}$. Um $\mathbb{Q}$-isomorfismo de M para L é um isomorfismo de corpos $\sigma : L \to M$ tal que $\sigma(k) = k$, para todo $k \in \mathbb{Q}$. Se $f(x) = a_0 + a_1x + ... + a_nx^n \in L[x]$, definimos $f^\sigma(x) = b_0 + b_1x + ... + b_nx^n \in M[x]$ onde $b_i = \sigma(a_i)$; $i = 0, 1, ..., n$.

Observação 3.1.4. Se todas as raízes de $f(x)$ estão em L segue que $f(x)$ pode ser decomposto em polinômios de grau um, como afirmado em 2.1.15. E pela proposição 1.2.22 podemos afirmar que toda σ aplicada nos fatores dessa decomposição também terá grau um, logo, todas as raízes f^σ estão em M.

Exemplo 3.1.5. Considere a extensão $\mathbb{C}|\mathbb{R}$ finita e tome o isomorfismo $\sigma : \mathbb{C} \to \mathbb{C}$. Temos que σ fixa os elementos de $\mathbb{R}$, ou seja, $\sigma|_{\mathbb{R}} = I$. Sabemos que os elementos do conjunto $\mathbb{C}$ é da forma $z = a + bi$ com $a, b \in \mathbb{R}$. Assim, $\sigma(z) = \sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i)$. Percebam que os elementos da imagem ficam completamente determinados por $\sigma(i) \in \mathbb{C}$. Então, como $\sigma(-1) = -1$ mas $\sigma(-1) = \sigma(i^2)$ que por sua vez é igual a $\sigma(i)\sigma(i)$, temos que $\sigma(i)\sigma(i) = 1 \cdot (-1)$, portanto, $\sigma(i)$ só pode ser i ou $-i$, o que nos mostra $\sigma_1(z) = z$ e $\sigma_2(z) = \overline{z}$. Assim, fica claro que $Aut_{\mathbb{R}}\mathbb{C} = \{id, \sigma_2\}$.

Proposição 3.1.6. *Sejam $K, K' \supset \mathbb{Q}$ corpos e $\sigma : K \to K'$ um isomorfismo, e $h(x) \in K[x]$ um polinômio irredutível sobre K. Se α é uma raiz de $h(x)$ em $\mathbb{C}$ e β é uma raiz de $h^\sigma(x)$ em $\mathbb{C}$, então existe um único isomorfismo $\hat{\sigma} : K[\alpha] \to K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}|_K = \sigma$.*

Demonstração: Seja α uma raiz qualquer de $h(x) \in K[x]$ e β uma raiz de $h^\sigma(x) \in K'[x]$. Como $h(x)$ é irredutível em $K[x]$, então $h^\sigma(x)$ é irredutível em $K'[x]$. Sabemos que $K[\alpha]$ e $K'[\beta]$ são corpos, pelo Corolário 2.1.8, segue que:

(1) $K[\alpha] = \{a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1} : a_i \in K\}$ e $1, \alpha, \alpha^2, ..., \alpha^{m-1}$ é uma base do espaço vetorial $K[\alpha]$ sobre o corpo K.

(2) $K'[\beta] = \{a'_0 + a'_1\beta + ... + a'_{m-1}\beta^{m-1} : a'_i \in K'\}$ e $1, \beta, \beta^2, ..., \beta^{m-1}$ é uma base do espaço vetorial $K'[\beta]$ sobre o corpo K'.

Verifiquemos que $\hat{\sigma} : K[\alpha] \to K'[\beta]$ definido por $\hat{\sigma}(a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1}) = \sigma(a_0) + \sigma(a_1)\beta + ... + \sigma(a_{m-1})\beta^{m-1}$ é um isomorfismo de corpos, tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}|_K = \sigma$:

a) Tome $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in K[x]$. Temos que $\hat{\sigma}f(\alpha) = \hat{\sigma}(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}) = \sigma(a_0) + \sigma(a_1)\beta + ... + \sigma(a_{n-1})\beta^{n-1} = f^\sigma(\beta)$. Sejam $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in K[x]$ e $g(x) = b_0 + b_1x + ... + b_{n-1}x^{n-1} \in K[x]$, e seja $h(x) = f(x) + g(x) \in K[x]$. Daí, $\hat{\sigma}(f(\alpha) + g(\alpha)) = \hat{\sigma}(h(\alpha)) = h^\sigma\beta$. Por outro lado, $h^\sigma(x) = f^\sigma(x) + g^\sigma(x) \Rightarrow h^\sigma(\beta) = f^\sigma(\beta) + g^\sigma(\beta) = \hat{\sigma}(f(\alpha)) + \hat{\sigma}(g(\alpha))$. Agora, vamos mostrar que $\hat{\sigma}(f(\alpha)g(\alpha)) = f^\sigma(\beta)g^\sigma(\beta)$. Sabemos que $f(\alpha)g(\alpha) = q(x)h(x) + r(x)$ com $q(x), h(x), r(x) \in K[x]$, onde $\partial r(x) < m$. Segue que, $f(\alpha)g(\alpha) = r(\alpha)$, pois $h(\alpha) = 0$. Assim, $\hat{\sigma}(f(\alpha)g(\alpha)) = \hat{\sigma}(r(\alpha)) = r^\sigma(\beta)$. Por outro lado, $f^\sigma(\alpha)g^\sigma(\alpha) = q^\sigma(x)h^\sigma(x) + r^\sigma(x)$, donde $f^\sigma(\beta)g^\sigma(\beta) = r^\sigma(\beta)$ pois $h^\sigma(\beta) = 0$. Logo, $f^\sigma(\beta)g^\sigma(\beta) = \hat{\sigma}(f(\alpha)g(\alpha))$. Portanto, $\hat{\sigma}$ é um homomorfismo.

b) Agora, para mostrar que $\hat{\sigma}$ é injetor, temos que, $K[\alpha]$ é um corpo e $\hat{\sigma} \neq 0$, então, $N(\hat{\sigma}) = \{0\}$, logo, é injetor.

c) Seja $g(\beta) = b_0 + b_1\beta + ... + b_{r-1}\beta^{r-1} \in K'[\beta]$. Como σ é um isomorfismo, então, existem $a_0, a_1, ..., a_{r-1} \in K$ tais que $\sigma(a_j) = b_j$; $j = 1, ..., r-1$. Então, $\hat{\sigma}(a_0 + a_1\alpha + ... + a_{r-1}\alpha^{r-1} = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + ... + \sigma(a_{r-1})\sigma(\alpha^{r-1}) = \sigma(a_0) + \sigma(a_1)\beta + ... + \sigma(a_{r-1})\beta^{r-1} = b_0 + b_1\beta + ... + b_{r-1}\beta^{r-1}$. Logo, $\hat{\sigma}$ é sobrejetor.

Como $\alpha \in K[\alpha]$ então, $\alpha = 0 + 1\alpha$. Assim, $\hat{\sigma}(\alpha) = \sigma(0) + \sigma(1)\sigma(\alpha) = \beta$, logo, $\hat{\sigma}(\alpha) = \beta$. E mais ainda, $\hat{\sigma}(a_0) = \sigma(a_0)$, logo, $\hat{\sigma}|_K = \sigma$, e claramente, $\hat{\sigma}$ é o único com essas duas condições. □

Proposição 3.1.7. *Sejam $K, K' \supseteq \mathbb{Q}$ corpos e $\sigma : K \to K'$ um isomorfismo, $f(x) \in K[x]$ e α uma raiz qualquer de $f(x)$ em $\mathbb{C}$. Então $\exists\ \beta$ raiz de $f^\sigma(x)$ em $\mathbb{C}$ e existe um isomorfismo $\sigma_1 : K[\alpha] \to K'[\beta]$ tal que $\sigma_1(\alpha) = \beta$ e $\sigma_1|_K = \sigma$.*

Observe o diagrama da proposição:

$$\begin{array}{ccc} K & \longrightarrow & K[\alpha] \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma_1} \\ K' & \longrightarrow & K'[\beta] \end{array} \tag{1}$$

A demonstração será omitida dado que a existência do isomorfismo pode ser provada a partir da proposição anterior.

Teorema 3.1.8. *Sejam $K, K' \supseteq \mathbb{Q}$ corpos, $\sigma : K \to K'$ um isomorfismo, $f(x) \in K[x]$ e $\alpha_1, ..., \alpha_r$ as distintas raízes de $f(x)$ em $\mathbb{C}$. Se $L = Gal(f, K)$ e $L' = Gal(f^\sigma, K')$ então, $\exists\ \hat{\sigma} : L \to L'$ um isomorfismo tal que $\hat{\sigma}|_K = \sigma$ e mais ainda $\hat{\sigma}(\alpha_1), ..., \hat{\sigma}(\alpha_r)$ são as distintas raízes de $f^\sigma(x)$ em $\mathbb{C}$.*

Demonstração: Se $f(x) \in K[x]$ possui uma única raiz α_1, então, temos $f(x) = (x - \alpha_1)^m$ em $\mathbb{C}[x]$, o que implica em $\alpha_1 \in K$ já que $f(x) \in K[x]$, e portanto, $\sigma(\alpha_1) \in K'$ é a única raiz de $f^\sigma(x) \in \mathbb{C}$ e teremos $L = K$, $L' = K'$ e $\hat{\sigma} = \sigma : L \to L'$.

Se $f(x) = f_1(x)^{m_1}...f_k(x)^{m_k}$ onde $f_i(x) \in K[x]$ são distintos polinômios irredutíveis sobre K temos que $f^\sigma(x) = f_1^\sigma(x)^{m_1}...f_k^\sigma(x)^{m_k}$ onde $f_i^\sigma(x) \in K'[x]$ são distintos polinômios irredutíveis sobre K'. Da Proposição 2.1.14, temos que $f(x)$ em $\mathbb{C}$ possui r raízes distintas, assim, $f^\sigma(x)$ em $\mathbb{C}$ também.

Sejam $\beta_1, \beta_2, ..., \beta_r$ as r distintas raízes em $\mathbb{C}$ do polinômio $f^\sigma(x) \in K'[x]$.

Seja $K_1 = K[\alpha_1]$, $K_2 = K_1[\alpha_2]$, $K_3 = K_2[\alpha_3], ..., K_r = K_{r-1}[\alpha_r]$. Assim, temos que $L = K[\alpha_1, \alpha 2, ..., \alpha_r] = K_r$.

Pela proposição anterior $\exists\ \beta \in \{\beta_1, ..., \beta_r\}$ e existe o isomorfismo $\sigma_1 : K[\alpha_1] \to K'[\beta]$ tal que $\sigma_1(\alpha_1) = \beta$ e $\sigma_1|_K = \sigma$. Chamando $\beta_1 = \beta$ temos então que $\exists\ \beta_1 \in \{\beta_1, ..., \beta_r\}$ e o isomorfismo $\sigma_1 : K[\alpha_1] \to K'[\beta_1]$ tal que $\sigma_1(\alpha_1) = \beta_1$ e $\sigma_1|_K = \sigma$.

Seja $K'[\beta_1] = K_1'$. Assim $\exists\ \sigma_1 : K_1 \to K_1'$ isomorfismo tal que $\sigma_1(\alpha_1) = \beta_1$ e $\sigma_1|_K = \sigma$. Como $f(x) \in K[x]$ e $\sigma_1|_K = \sigma$ implica em $f(x) \in K_1[x]$, logo, $\sigma_1 : K_1[x] \to K_1'[x]$ é um isomorfismo, pois $\sigma_1|_K = \sigma$, e $f^{\sigma_1}(x) = f^\sigma(x)$.

Agora, para $K_1, K_1' \supseteq \mathbb{Q}$ e $\sigma_1 : K \to K_1'$. Existe $\beta \in \{\beta_1, ..., \beta_r\}$ (vamos chamar de β_2). Existe um isomorfismo $\sigma_2 : K_1[\alpha_2] \to K_1'[\beta_2]$ tal que $\sigma_2(\alpha_2) = \beta_2$ e $\sigma_2|_K = \sigma_1$. Como $\sigma_1|_K = \sigma$ implica que $\sigma_2|_K = \sigma$ e $\sigma_2 : K[\alpha_1, \alpha_2] \to K'[\beta_1, \beta_2]$ é um isomorfismo.

Supondo que existe $\sigma_{k-1} : K[\alpha_1, ..., \alpha_{k-1}] \to K'[\beta_1, ..., \beta_{k-1}]$ um isomorfismo tal que $\sigma_{k-1}(\alpha_i) = \beta_i$ onde $i = 1, 2, ..., k-1$ e $\sigma_{k-1}|_K = \sigma$ temos que $f(x) \in K_{k-1}[x]$ e $f^{\sigma_{k-1}}(x) = f^\sigma(x)$.

Aplicando novamente a Proposição 3.1.7 para $K_{k-1} = K[\alpha_1, ..., \alpha_{k-1}]$ e $K_{k-1}' = K'[\beta_1, ..., \beta_{k-1}]$ com $\sigma_{k-1} : K_{k-1} \to K_{k-1}'$, temos que existe β (chamaremos de β_k) raiz de $f^\sigma(x)$ e existe um isomorfismo $\sigma_k : K_{k-1}[\alpha_k] \to K_{k-1}'[\beta_k]$ tal que $\sigma_k|_K = \sigma_{k-1}$ e $\sigma_k(\alpha_k) = \beta_k$.

Donde segue que, existe $\sigma_k : K[\alpha_1, ..., \alpha_k] \to K'[\beta_1, ..., \beta_k]$ um isomorfismo tal que $\sigma_i(\alpha_i) = \beta_i$ para todo $i \in \{1, 2, ..., k\}$ e $\sigma_k|_K = \sigma$. Desse modo, $L = K_r = K[\alpha_1, ..., \alpha_r]$, logo, é de imediato que $\sigma(\alpha_1,), ..., \sigma(\alpha_r)$ são as distintas raízes de $f^\sigma(x)$.

□

Corolário 3.1.9. *Seja $L|K$ uma extensão galoisiana e sejam M, M' subcorpos de L contendo K. Se $\sigma : M \to M'$ é um isomorfismo tal que $\sigma(a) = a\ \forall\ a \in K$ então existe $\hat{\sigma} \in Aut_L K$ tal que $\hat{\sigma}|_M = \sigma$.*

A demonstração segue diretamente do teorema anterior.

Corolário 3.1.10. *Seja $L|K$ uma extensão finita. Então, $L|K$ galoisiana $\Leftrightarrow$ $L|K$ normal.*

Demonstração: Seja $L|K$ finita. Suponha que $L = Gal(f, K)$. Assim, seja, $g(x) \in K[x]$ um polinômio irredutível tal que existe $\alpha \in L$, $g(\alpha) = 0$. Vamos provar que $\forall$

$\beta \in \mathbb{C}$, $g(\beta) = 0$ temos $\beta \in L$. De fato, seja $\beta \neq \alpha$ uma raiz de $g(x)$ em $\mathbb{C}$. Pela Proposição 3.1.6, existe $\sigma : K[\alpha] \to K[\beta]$ isomorfismo tal que $\sigma(\alpha) = \beta$ e $\sigma(a) = a \ \forall$ $a \in K$. Sejam $M = K[\alpha]$, $M' = K[\beta]$ e $L' = Gal(f, M')$. Como $K \subset M \subset L$ e $K \subset M'$ temos $L = Gal(f, K) = Gal(f, M)$ e $L = Gal(f, K) \subset L' = Gal(f, M')$. Agora, $\sigma(a) = a$ $\forall\ a \in K$ nos diz que $f^\sigma = f$ e pelo Teorema 3.1.8 existe um isomorfismo $\hat{\sigma} : L \to L'$ ou $\hat{\sigma} : L = Gal(f, M) \to L' = Gal(f^\sigma, M')$ tal que $\hat{\sigma}|_M = \sigma$, ou seja, $\hat{\sigma}(a) = a \ \forall\ a \in K$. Em particular temos, $[L : K] = [L' : K]$, sendo que, assim, $L = L'$, e isto termina a demonstração.

Por outro lado, como $L|K$ é normal, para todo $g(x) \in K[x]$ irredutível sobre K, $u \in L$ tal que $g(u) = 0$, logo, segue que $L = Gal(g, K)$ □

Exemplo 3.1.11. Tome o corpo $\mathbb{Q}[\sqrt[4]{2}]$ sobre $\mathbb{Q}$; essa extensão não é normal. De fato, $p(x) = x^4 - 2 \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$, embora, não seja possível expressar uma decomposição (veja 2.1.15) de $p(x)$ em $\mathbb{Q}[\sqrt[4]{2}]$, dado que há raízes imaginárias que não pertencem a $\mathbb{Q}[\sqrt[4]{2}]$. Consequentemente, a extensão $\mathbb{Q}[\sqrt[4]{2}]|\mathbb{Q}$ também não é galoisiana.

Corolário 3.1.12. *Seja $L|K$ galoisiana, então*

(a) $[L : K] = |Aut_K L|$.

(b) Se $\alpha \in L - K$, $\exists\ \sigma \in Aut_K L$ *tal que* $\sigma(\alpha) \neq \alpha$.

Demonstração:

(a) Seja $L = K[u]$. Se $h(x) = irr(u, K)$, pelo Corolário 3.1.10, $L = Gal(h(x), K)$ e L contém todas as raízes de $h(x)$. Caso o grau de $h(x) = n$ temos $[L : K] = n$ e pela Proposição 2.1.14 temos que $h(x)$ possui n raízes distintas. Pela Proposição 3.1.6 existe um isomorfismo $\sigma_1 : K[u] \to K[u_i]$ onde $i \in \{1, 2, ..., n\}$ tal que $\sigma_i(u) = u_i$ e $\sigma(a) = a \ \forall\ a \in K$. Pelo Corolário 3.1.9 existe $\hat{\sigma}_i \in Aut_L K$ tal que $\hat{\sigma}_i|_{K[u]} = \sigma_i$, ou seja, existem pelo menos n automorfismos, donde temos $[L : K] \leq |Aut_K L|$, já que $[L : K] = n$, mas, do Corolário 2.1.25 segue que $[L : K] \geq |Aut_L K|$, logo, $[L : K] = n = |Aut_L K|$.

(b) Seja $\alpha \in L$, $\alpha \notin K$. Se $g(x) = irr(\alpha, K)$ segue que $\partial\ g(x) = r \geq 2$. Pela Proposição 2.1.14 todas as raízes de $g(x)$ são simples, assim, existe $\beta \neq \alpha$ tal que $g(\beta) = 0$. Pelo Corolário 3.1.10 L é normal. Agora, pela Proposição 3.1.6 existe

$\sigma : K[\alpha] \to K[\beta]$ isomorfismo tal que $\sigma(a) = a \; \forall \; a \in K$ e $\sigma(\alpha) = \beta$. Pelo Corolário 3.1.9 existe $\hat{\sigma} \in Aut_K L$, $\hat{\sigma}|_{K[\alpha]} = \sigma$, portanto, temos $\hat{\sigma}(\alpha) \neq \alpha$.

□

Exemplo 3.1.13. Sabemos que o grau da extensão $\mathbb{C}|\mathbb{R}$ é 2, pois, sendo i um elemento algébrico sobre $\mathbb{R}$, já que para $p(x) = x^2 + 1 \in R[x]$, $p(i) = 0$; pelo item *(b)* da Proposição 2.1.19 segue que $[\mathbb{R}[i] : \mathbb{R}] = 2$. Por outro lado, do Corolário 2.1.25, $|Aut_{\mathbb{R}}\mathbb{C}| \leq [\mathbb{C} : \mathbb{R}]$. Perceba que, $p(x) = (x + i)(x - i)$ e como $\mathbb{C} = Gal(p, \mathbb{R})$ e $\mathbb{C}|\mathbb{R}$ é finita, a extensão é galoisiana, logo, pelo item *(b)* do corolário anterior 3.1.12, se $\sigma : \mathbb{C} \to \mathbb{R}$, $\sigma(i) = \pm i$. Assim, só existem dois automorfismo para a extensão, portanto, $|Aut_{\mathbb{R}}\mathbb{C}| = [\mathbb{C} : \mathbb{R}]$.

Teorema 3.1.14. *Se $L|M|K$ são extensões finitas e $L|K$ é galoisiana, então as seguintes afirmações são equivalentes:*

(a) $M|K$ *galoisiana*

(b) $\sigma(M) \subseteq M \; \forall \; \sigma \in Aut_K L$

(c) $Aut_M L \trianglelefteq Aut_K L$

Demonstração:

$(a) \Rightarrow (b)$ Seja $u \in M$ tal que $M = K[u]$. Se $M|K$ é galoisiana segue do Corolário 3.1.10 que $M|K$ é normal. Se $h(x) = irr(u, K)$ e $\sigma \in Aut_K L$, sabemos que $v = \sigma(u)$ é também raiz de $h(x)$ e como $M|K$ é normal, temos $v = \sigma(u) \in M$, ou seja, $\sigma(K[u]) \subseteq K[u] = M$, como queríamos demonstrar.

$(b) \Rightarrow (a)$ Seja $u \in L$ tal que $M = K[u]$ e seja $h(x) = irr(u, K)$. Vamos mostrar que se $\sigma(M) \subseteq M$ para todo $\sigma \in Aut_K L$, então, $M = Gal(h, K)$.

Sejam v uma raiz de $h(x)$ e $M' = K[v]$. Pela Proposição 3.1.6, existe um isomorfismo, $\sigma_0 : M \to M'$ tal que $\sigma(u) = v$ e $\sigma(a) = a$, para todo $a \in K$. Assim, pelo Teorema 3.1.8, existe $\sigma \in Aut_K L$ tal que $\sigma|_M = \sigma_0$. Como $\sigma(M) \subseteq M$ e $u \in M$ temos $v = \sigma(u) \in M$ e isto prova a implicação.

$(b) \Rightarrow (c)$ Sejam $\sigma \in Aut_K L$ e $\gamma \in Aut_M L$. Vamos provar que se $\sigma(M) \subseteq M$ então, $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$. De fato, se $\sigma(M) \subseteq M$ e $m' = \sigma(m), m \in M$ temos: $\gamma(m') = m'$ e $(\sigma^{-1} \circ \gamma \circ \sigma)(m) = \sigma^{-1}(\gamma(m')) = \sigma^{-1}(m') = m$, isto é, $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$.

$(c) \Rightarrow (b)$ Suponha por absurdo que existe $\sigma \in Aut_K L$ e existe $u \in M$ tal que $\sigma(u) = v \notin M$. Como L|K é galoisiana, existe f tal que $L = Gal(f, K) \subset Gal(f, M) \subset L$, logo $L|M$ é galoisiana. Temos pelo Corolário 3.1.12 item (b) que existe $\gamma \in Aut_M L$ tal que $\gamma(v) \neq v$. Assim $(\sigma^{-1} \circ \gamma \circ \sigma)(u) = \sigma^{-1}(\gamma(v)) \neq \sigma^{-1}(v) = u$, ou seja, $(\sigma^{-1} \circ \gamma \circ \sigma) \notin Aut_M L$, o que contraria a hipótese $Aut_M L \trianglelefteq Aut_K L$. □

Teorema 3.1.15. *[5] Se $L|K$ uma extensão finita. Então as seguintes condições são equivalentes:*

(1) $L|K$ *galoisiana*

(2) $L|K$ *normal*

(3) $\forall\, \alpha \in L - K\ \exists\, \sigma \in Aut_K L$ *tal que* $\sigma(\alpha) \neq \alpha$.

(4) $[L : K] = |Aut_K L|$

Demonstração:

$(1) \Rightarrow (2)$ Segue imediatamente do Corolário 3.1.10.

$(2) \Rightarrow (3)$ Segue imediatamente dos Corolários 3.1.10 e 3.1.12.

$(3) \Rightarrow (4)$ Pelo Corolário 2.1.25, temos $[L : K] \geq |Aut_K L|$. Suponha por absurdo que $[L : K] > |Aut_K L|$. Seja $Aut_K L = \varphi_1, \varphi_2, ..., \varphi_n$ onde $\varphi_1 = id$ é o automorfismo identidade de L. Se $[L : K] > n$ então, existem $u_1, u_2, ..., u_n, u_{n+1} \in L$ linearmente independentes sobre o corpo K. Considere agora o sistema linear homogêneo com n equações e $(n + 1)$ incógnitas $x_1, x_2, ..., x_{n+1} \in L$:

$$\begin{cases} \varphi_1(u_1)x_1 + \varphi_1(u_2)x_2 + ... + \varphi_1(u_j)x_j + ... + \varphi_1(u_n)x_n + \varphi_1(u_{n+1})x_{n+1} = 0 \\ \varphi_2(u_1)x_1 + \varphi_2(u_2)x_2 + ... + \varphi_2(u_j)x_j + ... + \varphi_2(u_n)x_n + \varphi_2(u_{n+1})x_{n+1} = 0 \\ \quad \vdots \\ \varphi_i(u_1)x_1 + \varphi_i(u_2)x_2 + ... + \varphi_i(u_j)x_j + ... + \varphi_i(u_n)x_n + \varphi_i(u_{n+1})x_{n+1} = 0 \\ \quad \vdots \\ \varphi_n(u_1)x_1 + \varphi_n(u_2)x_2 + ... + \varphi_n(u_j)x_j + ... + \varphi_n(u_n)x_n + \varphi_n(u_{n+1})x_{n+1} = 0 \end{cases} \tag{2}$$

Como o número de equações de (2) é menor que o número de incógnitas então, (2) admite solução não trivial.

Seja agora $(x_1, x_2, ..., x_{n+1}) = (a_1, a_2, ..., a_{n+1})$ uma solução não trivial de (2) com o maior número de incógnitas iguais a zero. Reordenando se necessário, denotaremos por $a_1, a_2, ..., a_r$ os $a_i's$ não nulos dessa solução.

Multiplicando por a_1^{-1} se necessário, podemos assumir que $a_1 = 1$. Assim $1, a_2, ..., a_r$ não nulos são tais que $(1, a_2, ..., a_r, 0, ..., 0)$ é uma solução de (2) com um número máximo de zeros. Então temos $\varphi_i(u_1) + \varphi_i(u_2)a_2 + ... + \varphi_i(u_r)a_r = 0$ para todo $i \in \{1, 2, ..., n\}$.

Como $\varphi_1 = id_L$ e $u_1, u_2, ..., u_r, ..., u_n$ são linearmente independentes sobre K então, segue que existe $a_i \in L$ tal que $a_i \notin K$. Seja $a_r \notin K$. Assim por (c) existe $\sigma \in Aut_K L$ tal que $\sigma(a_r) \neq a_r$.

Daí segue que $(\sigma \circ \varphi_i)(u_1) + (\sigma \circ \varphi_i)(u_2)\sigma(a_2) + ... + (\sigma \circ \varphi_i)(u_r)\sigma(a_r) = 0$ para todo $i \in \{1, 2, ..., n\}$.

Como $Aut_K L$ é um grupo e $\sigma \in Aut_K L$ segue que

$$Aut_K L = \{\varphi_1, \varphi_2, ..., \varphi_n\} = \{\sigma\varphi_1, \sigma\varphi_2, ..., \sigma\varphi_n\}.$$

Portanto $\sigma\varphi_1 = \varphi_k$ para algum k e temos

$$\varphi_k(u_1) + \varphi_k(u_2)\sigma(a_2) + ... + \varphi_k(u_r)\sigma(a_r) = 0, \forall\ k \in \{1, 2, ..., n\}$$

por outro lado

$$\varphi_k(u_1) + \varphi_k(u_2)a_2 + ... + \varphi_k(u_r)a_r = 0, \forall\ k \in \{1, 2, ..., n\}.$$

Daí segue que:

$$\varphi_k(u_2)(\sigma(a_2) - a_2) + ... + \varphi_k(u_r)(\sigma(a_r) - a_r) = 0, \forall\ k \in \{1, 2, ..., n\}.$$

Como $\sigma(a_r) - a_r \neq 0$ temos uma solução $(0, \sigma(a_2) - a_2, ..., \sigma(a_r) - a_r, ...)$ que contradiz a maximalidade de zeros da solução $(0, a_2, ..., a_r, ..., 0, ..., 0)$.

$(4) \Rightarrow (1)$ Suponhamos $L|K$ uma extensão finita e $[L : K] = |Aut_K L|$. Vamos provar que $L|K$ é galoisiana. Sejam $L = K[u]$ e $h(x)$ definido por $h(x) = irr(u, K)$ então, para todo $\sigma \in Aut_K L$ temos $\sigma(u)$ é raiz de $h(x)$ e por outro lado para cada raiz $\beta \in L$ de $h(x)$, existe um único $\sigma \in Aut_K L$ tal que $\sigma(u) = \beta$.

Logo, $|Aut_K L| = n$, com n o número de raízes de $h(x)$ em L. Agora se $[L : K] = |Aut_K L|$ então, $\partial\ h(x) = [L : K] = |Aut_K L| = n$. Daí segue que L contém todas as raízes de $h(x)$, ou seja, $L = Gal(h, K)$. □

Proposição 3.1.16. *Se $L|K$ é uma extensão galoisiana de grau n, então $G = Aut_K L$ é isomorfo a um subgrupo de S_n.*

Demonstração: Seja $\Omega = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ o conjunto de todas as raízes distintas de $f = irr(\alpha, K)$. Sabemos pela proposição 1.2.22 que se $\sigma \in Aut_K L$, então, $\sigma(\alpha_j)$, $j = 1, ..., n$ também é uma raiz de $f(x)$, logo, $\sigma(\alpha_j) \in \Omega$. E como σ é injetiva e Ω infinito, segue que $\sigma(\Omega) = \Omega$, ou seja, σ permuta as distintas raízes de $f(x)$. Considere

$$\begin{array}{rccc} \Psi & : & G & \to & S_\Omega \\ & & \sigma & \mapsto & \sigma_0 \end{array}$$

Verificamos que essa função é um homomorfismo. Seja σ,$\tau \in G$. Vamos mostrar que $(\sigma \circ \tau)|_\Omega = \sigma|_\Omega \circ \tau|_\Omega$. Tome $\gamma = \sigma \circ \tau$. Então, temos que $\Psi(\gamma) = \sigma \circ \tau|_\Omega = \sigma\tau|_\Omega = \sigma|_\Omega\, \tau|_\Omega$. Logo, é um homomorfismo. Como $L = K[\alpha_1, ..., \alpha_n]$ então, $\sigma \in G$ está completamente determinada por seus valores em Ω. Logo, se $\sigma, \Psi \in G$ são tais que $\sigma|_\Omega = \Psi|_\Omega$, então, $\sigma = \Psi$, o que denota que Ψ é injetora. Portanto, G é isomorfo a um subgrupo de $S_\Omega \simeq S_n$. □

Observação 3.1.17. O automorfismo σ fica completamente descrito pelas imagens das raízes α_j onde $j = \{1, 2, ..., n\}$, ou seja, para todo $\sigma \in Aut_K L$ temos sua caracterização pela rescpectiva permutação $\sigma_0 \in S_n$.

Exemplo 3.1.18. Considere a extensão finita (como visto em 2.1.23) $L|\mathbb{Q}$ onde $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Sendo $p(x) = x^4 - 2x^2 - 3x^2 + 6$ o polinômio irredutível sobre $\mathbb{Q}$, fica claro que a extensão é galoisiana, já que, é possível uma decomposição de $p(x)$ em $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ com todas as suas raízes pertencentes ao $\mathbb{C}$, sendo $p(x) = (x - \sqrt{3})^2(x - \sqrt{2})^2$. Já sabemos que o grau da extensão é 4, então, $Aut_\mathbb{Q} L$ é isomorfo a um subgrupo de S_4.

Proposição 3.1.19. *Seja $a \in K$ e $L = Gal(x^n - a, K)$ onde K contém uma raiz ζ primitiva, n-ésima da unidade, então, $Aut_K L$ é um grupo abeliano.*

Demonstração: Seja $\alpha = \sqrt[n]{a} \in \mathbb{C}$ e ζ uma raiz primitiva n-ésima da unidade tal que $\zeta \in K$, então, $\alpha, \alpha\zeta, \alpha\zeta^2, ..., \alpha\zeta^{n-1}$ são as n raízes distintas de $x^n - a \in \mathbb{C}$. Sabemos que $L = K[\zeta, \alpha] = K[\alpha]$, pois $\zeta \in K$. Assim, pela Proposição 1.2.22, se $\sigma, \tau \in Aut_K L$ então, $\sigma(\alpha) = \alpha\zeta^i$ para algum i e $\tau(\alpha) = \alpha\zeta^j$ para algum j. Daí, segue que $(\sigma \circ \tau)(\alpha) = \sigma(\alpha\zeta^j) = \sigma(\alpha)\zeta^j = \alpha\zeta^i\zeta^j = \alpha\zeta^{i+j}$ e, $(\tau \circ \sigma)(\alpha) = \tau(\alpha\zeta^i) = \tau(\alpha)\zeta^i = \alpha\zeta^j\zeta^i = \alpha\zeta^{j+i}$. Assim, $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha) \forall \sigma, \tau \in Aut_K L$. Como $L = K[\alpha]$ então, $\sigma \circ \tau = \tau \circ \sigma$ para todo $\sigma, \tau \in Aut_K L$. □

Proposição 3.1.20. *Seja p um número primo e $f(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau p. Se $f(x)$ possui exatamente duas raízes não reais então $Aut_\mathbb{Q} L \simeq S_p$ onde $L = Gal(f, \mathbb{Q})$.*

Demonstração: [5], página 175. □

3.2 A CORRESPONDÊNCIA DE GALOIS

Adentraremos agora a uma das mais importantes ideias da *teoria de Galois*. Diante da existência de um autormorfismo de L que fixa K, e alguns conceitos de *grupos*, podemos estabelecer fortes relações entre extensões intermediárias e subgrupos do grupo de Galois.

Definição 3.2.1. Seja $M|K$ uma extensão finita. Se L é um subcorpo de M contendo K, ou seja, $M \supset L \supset K$, L é um *corpo intermediário* de $M|K$.

Denotaremos o conjunto dos *corpos intermediários* por $\vartheta(M,K) = \{L : \textit{corpo intermediário de } M|K\}$. E a partir de agora, adotaremos $G = Aut_K M$ sendo $\iota(G) = \{H : H \textit{subgrupo de } G\}$

Proposição 3.2.2. *Seja H um subgrupo de G, então $L = \{a \in M : \gamma(a) = a, \forall\, \gamma \in H\}$.*

A proposição anterior nos garante que L é um corpo intermediário, mas isso já era de imediato, contudo, observe que L deixa fixo todo elemento de H, e dessa razão chamamos L de *corpo fixo* de H.

Podemos estabelecer uma conexão entre os subgrupos de G e os corpos intermediários da extensão $M|K$, bem como, entre L e o $Aut_L M$, vejamos:

$$\begin{array}{ccccc} \theta & : & \iota(G) & \to & \vartheta(M,K) \\ & & H & \mapsto & \theta(H) \end{array} \qquad \begin{array}{ccccc} \psi & : & \vartheta(M,K) & \to & \iota(G) \\ & & L & \mapsto & \psi(L) \end{array}$$

Dessas relações, decorrem as seguintes propriedades, imediatas, logo, omitiremos as demonstrações:

(1) $\psi(K) = Aut_K M = G$

(2) $\psi(M) = Aut_M M = \{I_M\}$

(3) $\theta(\{I_M\}) = \{a \in M : I_M(a) = a\} = M$

(4) $\theta(G) = \{a \in M : \gamma(a) = a, \forall \gamma \in G\} \supseteq K$

(5) $\theta(G) = K \Leftrightarrow M|K$ galoisiana.

Proposição 3.2.3. *(a) se* $L_1, L_2 \in \vartheta(M,K)$ *e* $L_1 \subseteq L_2$*, então* $\psi(L_1) \geq \psi(L_2)$

(b) se $H_1, H_2 \in \iota(G)$ *e* $H_1 \leq H_2$*, então* $\theta(H_1) \supseteq \theta(H_2)$

(c) $\forall\ L \in \vartheta(M,K)$ *tem-se* $(\theta \circ \psi)(L) \supseteq L$

(d) $\forall\ H \in \iota(G)$ *tem-se* $(\psi \circ \theta)(H) \geq H$*.*

Demonstração:

(a) Sejam $L_1, L_2 \in \vartheta(M,K)$. Temos que $\psi(L_1) = Aut_{L_1}M$ e $\psi(L_2) = Aut_{L_2}M$ e como $L_1 \subseteq L_2$, então, $Aut_{L_1}M \geq Aut_{L_2}M$.

(b) Sejam $H_1, H_2 \in \iota(G)$ e $H_1 \leq H_2$. Sabemos que $\theta(H_1) = \{a \in M : \gamma(a) = a, \forall\ \gamma \in H_1\}$ e $\theta(H_2) = \{a \in M : \gamma(a) = a, \forall\ \gamma \in H_2\}$, logo, $\theta(H_2) \subseteq \theta(H_1)$.

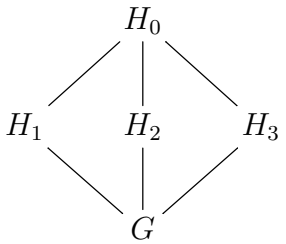
(c) Seja $L \in \vartheta(M,K)$. Temos que $(\theta \circ \psi)(L) = \theta(\psi(L)) = \theta(Aut_L M)$, e das definições, $\theta(Aut_L M) \supseteq L$.

(d) Seja $H \in \iota(G)$. Como $\theta(H) = \{a \in M : \gamma(a) = a, \forall\ \gamma \in H\} = N$, se $(\psi \circ \theta)(H) = \psi(\theta(H)) = \psi(N) = Aut_N M$, e sendo H subgrupo de $Aut_N M$ segue que $H \leq (\psi \circ \theta)(H)$.

□

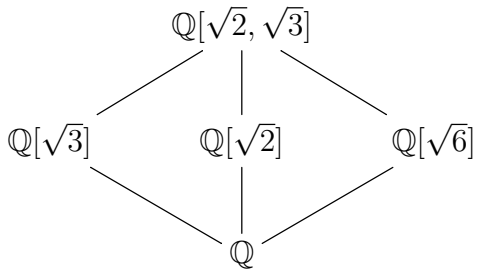
Exemplo 3.2.4. Considere a extensão $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ de $K = \mathbb{Q}$. Como vimos em 3.1.18, a extensão é isomorfa a S_4, portanto, o $Aut_K M = \{id, \sigma_1, \sigma_2, \sigma_3\}$. Para esse grupo de automorfismos, temos os seguintes subgrupos: $H_0 = \{id\}$, $H_1 = \{id, \sigma_1\}$, $H_2 = \{id, \sigma_2\}$ e $H_3 = \{id, \sigma_3\}$. Deste modo, temos o seguinte diagrama do reticulado desses subgrupos, sendo $G = Aut_K M$:

(3)



Veja que o corpo fixo do grupo de Galois G é $\theta(G) = \mathbb{Q}$, sendo $\theta(H_1) = \mathbb{Q}\sqrt{3}$, $\theta(H_2) = \mathbb{Q}\sqrt{2}$ e $\theta(H_3) = \mathbb{Q}\sqrt{6}$.

Assim, temos o seguinte diagrama do reticulado das extensões intermediárias:



(4)

Em síntese, o que interessa são as extensões com automorfismos que fazem com que os itens (c) e (d) da proposição 3.2.3, possam ser enunciados como igualdades em vez de inclusões.

Teorema 3.2.5. *[5] (Teorema Fundamental de Galois) Se $M|K$ é uma extensão galoisiana, então:*

(a) $\forall\ L \in \vartheta(M,K)$ *tem-se* $[M:L] = |\psi(L)|$ *e* $[L:K] = [G:\psi(L)]$ *(o índice de* $\psi(L)$ *em* G*)*

(b) $\forall\ H \in \iota(G)$ *tem-se* $[M:\theta(H)] = |H|$ *e* $[\theta(H):K] = [G:H]$ *(o índice de* H *em* G*)*

(c) $\psi \circ \theta = I_{\iota(G)}$ *e* $\theta \circ \psi = I_{\vartheta(M,K)}$

(d) $\forall\ L \in \vartheta(M,K), L|K$ *galoisiana* $\Leftrightarrow \psi(L) = Aut_L M \trianglelefteq G$

(e) Seja $L \in \vartheta(M,K)$*. Se* $L|K$ *galoisiana, então* $[L:K] = |Aut_K L|$ *e* $G/\psi(L) \simeq Aut_K L$*.*

Demonstração:

(a) Seja $L \in \vartheta(M,K)$. Por hipótese $M|K$ é galoisiana, então, $M|L$ também. Pelo Teorema 3.1.15, segue que, $[M:L] = |Aut_L M| = |\psi(L)|$ e como $[M:K] = |Aut_K M| = [M:L]\cdot[L:K]$, temos $[L:K] = |G|/|Aut_L M| = |\psi(L)|\cdot[L:K]$ donde $[L:K] = [G:\psi(L)]$.

(b) Seja $H \in \iota(G)$ e $L = \theta(H)$. Sabemos pelo item (a) que: $[M:L] = |Aut_L M|$ e $[L:K] = [G:\psi(L)]$. Por outro lado, pela Proposição 3.2.3 item (d), temos $H \subset Aut_L M$, então, $[M:L] = |Aut_L M| \geq |H|$.

Utilizaremos agora um argumento semelhante a demonstração do Teorema 3.1.15. Suponha $H = \{\gamma_1 = id_L, \gamma_2, ..., \gamma_n\}$ e por absurdo suponha $|Aut_L M| > |H|$. Logo, $[M : L] > n$.

Assim, existem $n + 1$ vetores $u_1, u_2, ..., u_n, u_{n+1} \in M$ linearmente independentes sobre o corpo L. Considere agora o sistema linear homogêneo com n equações e $n + 1$ incógnitas $a_1, a_2, ..., a_{n+1} \in L$:

$$\begin{cases} \gamma_1(u_1)a_1 + \gamma_1(u_2)a_2 + ... + \gamma_1(u_{n+1})a_{n+1} = 0 \\ \gamma_2(u_1)a_1 + \gamma_2(u_2)a_2 + ... + \gamma_2(u_{n+1})a_{n+1} = 0 \\ \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \gamma_n(u_1)a_1 + \gamma_n(u_2)a_2 + ... + \gamma_n(u_{n+1})a_{n+1} = 0 \end{cases} \tag{5}$$

Então existe uma solução não nula $(a_1, a_2, ..., a_{n+1}) \in L_{n+1}$. Considere uma solução não trivial de (5) com o maior número de zeros possível nas coordenadas $(a_1, a_2, ..., a_{n+1})$, assim denotaremos por $a_1, a_2, ..., a_r$ os $a_i s$ não nulos dessa solução, isto é, reorganizando podemos supor

$$a_1 \neq 0, a_2 \neq 0, ..., a_r \neq 0, a_{r+1} \neq 0, ..., a_{n+1} \neq 0.$$

Multiplicando o sistema por a_1^{-1} se necessário, podemos assumir $a_1 = 1$. Temos que a solução $(1, a_2, ..., a_r, 0, ..., 0) \in L_{n+1}$, com $1, a_2, ..., a_r$ não nulos, é uma solução de (5) com um número máximo de zeros. A primeira equação é:

$$u_1 + u_2 a_2 + ... + u_r a_r = 0, \text{ pois } \gamma_1 = id.$$

Como $u_1, u_2, ..., u_r$ é linearmente independente sobre L, então nem todos os a_j são elementos de L. Logo reorganizando novamente os valores, podemos supor $a_2 \notin L = \theta(H)$. Assim, existe $\gamma \in H$ tal que $\gamma(a_2) \notin a_2$. Aplicando ao sistema (6) temos:

$$\begin{cases} \gamma(\gamma_1(u_1)a_1) + \gamma(\gamma_1(u_2)a_2) + ... + \gamma(\gamma_1(u_r)a_r) = 0 \\ \gamma(\gamma_2(u_1)a_1) + \gamma(\gamma_2(u_2)a_2) + ... + \gamma(\gamma_2(u_r)a_r) = 0 \\ \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \gamma(\gamma_n(u_1)a_1) + \gamma(\gamma_n(u_2)a_2) + ... + \gamma(\gamma_n(u_r)a_r) = 0 \end{cases} \tag{6}$$

Mas como $\gamma \in H$ e $K = \{\gamma_1, ..., \gamma_n\}$ então, $H = \{\gamma\gamma_1, ..., \gamma\gamma_n\}$, ou seja, o sistema 7 é uma permutação do sistema (6):

$$\begin{cases} \gamma_1(u_1)a_1 + \gamma_1(u_2)\gamma(a_2) + ... + \gamma_1(u_r)\gamma(a_r) = 0 \\ \gamma_2(u_1)a_1 + \gamma_2(u_2)\gamma(a_2) + ... + \gamma_2(u_r)\gamma(a_r) = 0 \\ \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \gamma_n(u_1)a_1 + \gamma_n(u_2)\gamma(a_2) + ... + \gamma_n(u_r)\gamma(a_r) = 0 \end{cases} \tag{7}$$

Subtraindo o sistema (5) de (7), temos:

$$\begin{cases} 0 + \gamma_1(u_2)(a_2 - \gamma(a_2)) + ... + \gamma_1(u_r)(a_r - \gamma(a_r)) = 0 \\ 0 + \gamma_2(u_2)(a_2 - \gamma(a_2)) + ... + \gamma_2(u_r)(a_r - \gamma(a_r)) = 0 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ 0 + \gamma_n(u_2)(a_2 - \gamma(a_2)) + ... + \gamma_n(u_r)(a_r - \gamma(a_r)) = 0 \end{cases} \tag{8}$$

Como $a_2 \neq \gamma(a_2)$ implica que $a_2 - \gamma(a_2) \neq 0$ e

$$(0, a_2 - \gamma(a_2), a_3 - \gamma(a_3), ..., a_r - \gamma(a_r), 0, ..., 0).$$

é uma solução de (5) com no máximo $r - 1$ coeficientes não nulos. Logo, temos uma contradição com a minimalidade de r de coeficientes não nulos. Portanto $|Aut_L M| = |H|$, ou seja, $H = Aut_L M$.

(c) Seja $H \in \iota(G)$ e $L \in \vartheta(M, K)$. Sabemos da Proposição 3.2.3 que $H \leq \psi(\theta(H))$ e $L \leq \theta(\psi(L))$. Pelo item (a) temos $[G : \psi(\theta(H)] = [\theta(H) : K]$ e pelo item (b), temos que $[\theta(H) : K] = [G : H]$. Daí segue que $\psi(\theta(H) = H$. Analogamente, pelo item (b) temos $[M : \theta(\psi(L)] = |\psi(L)|$ e pelo item (a) temos $|\psi(L)| = [M : L]$. Daí segue imediatamente que: $\theta \circ \psi(L) = L$.

(d) Consequência imediata do Teorema 3.1.14 sendo $L|K$ galoisiana, se e somente se, $Aut_L M \trianglelefteq Aut_K M$.

(e) Sabemos do item (a) que $[G : \psi(L)] = [L : K]$, resta provar que para todo corpo intermediário L da extensão $M|K$, tal que $M|L$ seja galoisiana, temos que $G/\psi(L) \simeq Aut_K L$.

De fato, como $L|K$ é galoisiana, pelo Teorema 3.1.14, temos que para todo $\sigma \in G = Aut_K M$ ocorre $\sigma_0 = \sigma|_L \in Aut_K L$, portanto, podemos definir:

$$\begin{array}{rccc} \Phi & : & G & \to & Aut_K L \\ & & \sigma & \mapsto & \sigma_0 \end{array}$$

Vemos que Φ é homomorfismo de grupos. De fato, sejam $\sigma, \tau \in G$, então,

$$\Phi(\sigma \circ \tau) = (\sigma \circ \tau)|_L = \sigma|_L \circ \tau|_L = \Phi(\sigma) \circ \Phi(\tau).$$

Observe também que: $\sigma \in N(\Phi) \Leftrightarrow \Phi(\sigma) = id_L \Leftrightarrow \sigma|_L = id_L \Leftrightarrow \sigma \in Aut_L M$.

Por outro lado, como $M|L$ é uma extensão galoisiana, então pelo Teorema 3.1.8, para todo $\sigma_0 \in Aut_K L$, existe $\sigma \in Aut_K M$, tal que $\sigma|_L = \sigma_0$, logo, Φ é sobrejetor. Pelo Teorema de homomorfismo temos: $G/Aut_L M \simeq Aut_K M$.

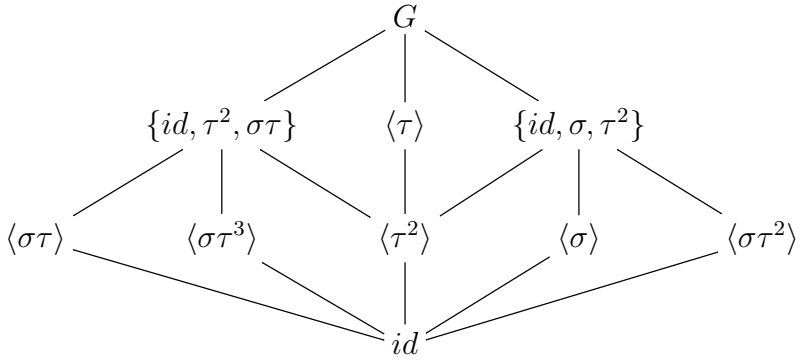
□

Assim, podemos estabelecer o seguinte diagrama:

$$\begin{array}{ccc}
\theta(I_M) = M & \longleftrightarrow & \{I_M\} = \quad \psi(M) \\
| & & | \\
\theta(H_2) = L_2 & \longleftrightarrow & H_2 = Aut_{L_2} M = \psi(L_2) \\
| & & | \\
\theta(H_1) = L_1 & \longleftrightarrow & H_1 = Aut_{L_1} M = \psi(L_1) \\
| & & | \\
\theta(G) = K & \longleftrightarrow & G = \ Aut_K M = \psi(K)
\end{array} \tag{9}$$

Exemplo 3.2.6. Seja $p(x) = x^4 - 2 \in \mathbb{Q}[x]$. Claramente, a extensão $\mathbb{Q}[i, \sqrt[4]{2}]|\mathbb{Q}$ é galoisiana, já que $p(x)$ pode ser decomposto em $(x^2 - \sqrt{2})(x^2 + \sqrt{2})$. O grupo de Galois da extensão é $Aut_{\mathbb{Q}}\mathbb{Q}[i, \sqrt[4]{2}] = \{id, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\} = G$; onde σ e τ são $\mathbb{Q}$-automorfismos de $\mathbb{Q}[i, \sqrt[4]{2}]$, sendo que os elementos de G ficam determinados sobre i e $\sqrt[4]{2}$ do seguinte modo: $\sigma(i) = -i$, $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$ e $\tau(i) = i$, $\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$.

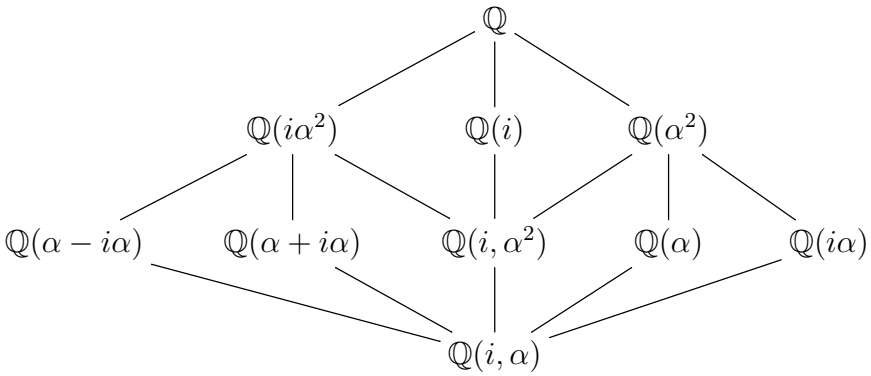
Veja o reticulado do grupo em questão:



(10)

Analogamente, estabelecemos o reticulado das extensões de corpos inter-

mediários, com base na correspondência de Galois:



(11)

onde $\alpha = \sqrt[4]{2}$.

Observe que os subgrupos $\mathbb{Q}(i\alpha^2), \mathbb{Q}(\alpha), \mathbb{Q}(\alpha + i\alpha), \mathbb{Q}(\alpha - i\alpha)$ de G possuem ordem 2, já os subgrupos $\mathbb{Q}(i\alpha^2), \mathbb{Q}(i), \mathbb{Q}(\alpha^2)$ possuem ordem 4 e esses são todos corpos normais sobre $\mathbb{Q}$, além de $\mathbb{Q}(i\alpha^2), \mathbb{Q}, \mathbb{Q}(i, \alpha)$, que também o são.

3.3 O PROBLEMA INVERSO DE GALOIS

Nas seções anteriores, apresentamos a Teoria de Galois, exemplificando o Teorema Fundamental de Galois 3.2.5. Com bases nestes conceitos podemos adentrar ao *Problema Inverso de Galois*, o qual consiste em descobrir em que condições podemos determinar um polinômio que tenha G como grupo de Galois.

Desse modo, dado G um grupo finito e K um corpo, a questão é: será que existe uma extensão de Galois $L|K$, finita, tal que o grupo de Galois da extensão é isomorfo ao grupo G? A indagação quanto a existência desta extensão é atribuída a Emmy Noether e David Hilbert, contudo, tal problema ainda está em aberto, pois somente para alguns grupos obteve-se resultado.

Dada essa relevância do Problema Inverso de Galois, o presente trabalho pode servir de base à continuação dos questionamentos que envolvem esse problema.

REFERÊNCIAS

[1] BOLDRINI, J. L., COSTA, S. I. R., FIGUEIREDO, V. L., AND WETZLER, H. G. *Álgebra Linear*, 3 ed. Harbra, 1980.

[2] DOMINGUES, H. H., AND IEZZI, G. *Álgebra Moderna*. Atual, 2003.

[3] ENDLER, O. *Teoria dos Corpos*, 1243 ed. IMPA, 2005.

[4] GARCIA, A., AND LEQUAIN, Y. *Elementos de Álgebra*, 4 ed. IMPA, 2006.

[5] GONCALVES, A. *Introdução à Álgebra*, 5 ed. IMPA, 2012.

[6] LANG, S. *Álgebra para Graduação*, 2 ed. Ciência Moderna, 2008.

[7] STEWART, I. *Galois Theory*, 3 ed. CRC Press, 1945.

APÊNDICE A - ALGUMAS NOÇÕES BÁSICAS DE ÁLGEBRA LINEAR

Nesta seção, relembremos alguns conceitos de *Álgebra Linear* utilizados no presente trabalho.

Definição A.0.1. Um *espaço vetorial* sobre um corpo K é um conjunto V, não vazio, com duas operações: uma soma e uma com elementos do corpo K com V:

$$\begin{array}{rcccccccc} + & : & V \times V & \to & V & \qquad & K \times V & \to & V \\ & & (u,v) & \mapsto & u+v & & (\lambda, v) & \mapsto & \lambda v \end{array}$$

tais que, para quaisquer, $u, v, w \in V$ e $\lambda, \mu \in K$, as seguintes propriedades sejam satisfeitas:

i) $(u+v)+w = u+(v+w)$

ii) $u+v = v+u$

iii) Existe $0 \in V$ tal que $u+0 = u$

iv) Existe $-u \in V$ tal que $u+(-u) = 0$

v) $\lambda(u+v) = \lambda u + \lambda v$

vi) $(\lambda+\mu)v = \lambda v + \mu v$

vii) $(\lambda\mu)v = \lambda(\mu v)$

viii) $1u = u$

Exemplo A.0.2. Seja $L \supset K$ e $\alpha \in L$. É possível definir operações sobre $K[x]$ (ou $K[\alpha]$), de modo que, $K[x]$ (ou $K[\alpha]$) torne-se um *espaço vetorial* sobre K. Segue imediatamente,

$$\begin{array}{rcccccccc} + & : & K[x] \times K[x] & \to & K[x] & \qquad & K \times K[x] & \to & K[x] \\ & & (f(x), g(x)) & \mapsto & f(x)+g(x) & & (\lambda, f(x)) & \mapsto & \lambda f(x) \end{array}$$

tais que, para quaisquer, $f(x), g(x), h(x) \in K[x]$ e $\lambda, \mu \in K$, as seguintes propriedades sejam satisfeitas:

i) $(f(x)+g(x))+h(x) = f(x)+(g(x)+h(x))$

ii) $f(x)+g(x) = g(x)+f(x)$

iii) Existe $0 \in K[x]$ tal que $f(x) + 0 = f(x) + 0 = f(x)$

iv) Existe $-f(x) \in K[x]$ tal que $f(x) + (-f(x)) = -f(x) + f(x) = 0$

v) $\lambda(f(x) + g(x)) = \lambda f(x) + \lambda g(x)$

vi) $(\lambda + \mu)g(x) = \lambda g(x) + \mu g(x)$

vii) $(\lambda\mu)g(x) = \lambda(\mu g(x))$

viii) $1f(x) = f(x)$

Portanto, $K[x]$ com é um espaço vetorial sobre K.

De modo análogo, naturalmente, temos que a extensão L sobre K também é um espaço vetorial sobre K.

Definição A.0.3. Sejam V um espaço vetorial, $v_1, v_2, ..., v_n \in V$ e $a_1, a_2, ..., a_n \in K$. Então, o vetor $v = a_1v_1, a_2v_2, ..., a_nv_n$ é um elemento de V ao que chamamos de *combinação linear* de $v_1, ..., v_n$.

A seguir, dois teoremas, os quais o leitor pode encontrar a demonstração em [1]. Os mesmos cooroboram à acepção de dimensão de uma extensão, bem como, sobre a obtenção de um elemento desta extensão.

Teorema A.0.4. *[1] Sejam $v_1, ..., v_n$ vetores não nulos que geram um espaço vetorial V. Então, dentre esses vetores, podemos extrair uma base de V.*

Teorema A.0.5. *[1] Seja um espaço vetorial V gerado por um conjunto finito de vetores $v_1, ..., v_n$. Então, qualquer conjunto com mais de n vetores é necessariamente linearmente dependente (e, portanto, qualquer conjunto linearmente independente tem no máximo n vetores).*

Se $v_1, ..., v_n \in V$ denominamos de *linearmente independentes* (LI) se a equação vetorial $\sum_{i=1}^{n} \alpha_i v_i = 0$ com $\alpha_i \in K$ é satisfeita apenas para os escalares $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$. Caso contrário, $v_1, ..., v_n$ são *linearmente dependentes* (LD) [5].

ÍNDICE REMISSIVO