Marcio Antonio de Souza

INTRODUÇÃO A TEORIA DE GALOIS

Rio Grande, Rio Grande do Sul, Brasil

Dezembro, 2017

Marcio Antonio de Souza

INTRODUÇÃO A TEORIA DE GALOIS

Trabalho de Conclusão de Curso submetido pelo aluno Marcio Antonio de Souza como requisito parcial para obtenção do grau de Licenciado em Matemática, pelo Curso de Matemática Licenciatura junto ao Instituto de Matemática, Estatística e Física da Universidade Federal do Rio Grande.

Universidade Federal do Rio Grande - FURG

Instituto de Matemática, Estatística e Física - IMEF

Curso de Licenciatura em Matemática

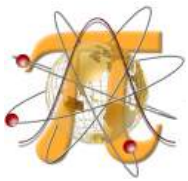
Orientador: Dra. Daiane Silva de Freitas

Rio Grande, Rio Grande do Sul, Brasil

Dezembro, 2017

Colaboradores

Universidade Federal do Rio Grande
http://www.furg.br



Instituto de Matemática, Estatística e Física
http://www.imef.furg.br

Marcio Antonio de Souza

INTRODUÇÃO A TEORIA DE GALOIS

Trabalho de Conclusão de Curso submetido pelo aluno Marcio Antonio de Souza como requisito parcial para obtenção do grau de Licenciado em Matemática, pelo Curso de Matemática Licenciatura junto ao Instituto de Matemática, Estatística e Física da Universidade Federal do Rio Grande.

Dra. Daiane Silva de Freitas
(Orientador - FURG)

Dr. Rafael Cavalheiro
(Avaliador - FURG)

Dra. Gasiela Martini
(Avaliador - FURG)

Rio Grande, Rio Grande do Sul, Brasil
Dezembro, 2017

Este trabalho é dedicado àqueles que amo e àqueles que respeito,
pois amo alguns, mas respeito a todos.

Agradecimentos

A gradeço a Deus pela vida, pela saúde e pela força que permitiu superar as dificuldades durante toda a trajetória acadêmica. A Fundação Universidade Federal do Rio Grande - Furg, pela oportunidade de fazer o curso de Matemática Licenciatura e ao seu corpo docente pela convivência e pelos sentimentos fraternais. A minha orientadora, Profª. Drª. Daiane Freitas pela paciência e carinho desprendidos deste as aulas de Álgebra Abstrata até a elaboração deste trabalho. A banca avaliadora, formada pelos professores, Profª. Drª. Grasiela Martini e Prof. Dr. Rafael Cavalheiro pelas correções, sugestões e incentivo. As minhas queridas filhas pelo amor e pelas palavras de incentivo, aos amigos pelo carinho e pelas vibrações de afeto. A todos que direta ou indiretamente contribuíram e fizeram parte da minha formação acadêmica e pessoal, o meu muito obrigado.

Resumo

Este trabalho tem como objetivo estudar o conteúdo introdutório da Teoria de Galois. O trabalho foi feito devido à motivação durante o curso regular de álgebra abstrata, onde estruturas algébricas como grupos, anéis, ideais e corpos foram introduzidas e estudadas durante a graduação. A elaboração do trabalho baseou-se na pesquisa em bibliografias e artigos publicados sobre o assunto. Foram mostrados em alguns capítulos os conteúdos que são pré-requisitos, conceitos e definições que tornam possível a compreensão da Teoria de Galois. No presente trabalho realizou-se um estudo simples das Extensões de Corpos e a Correspondência de Galois.

Palavras-chaves: Polinômios, Extensão de corpos, Teoria de Galois

Abstract

This work aims to study the introductory content of Galois Theory. The work was done due to the motivation during the regular course of Abstract Algebra, where algebraic structures such as groups, rings, ideals and fields were introduced and studied during graduation. The elaboration of the work was based on the research in bibliographies and articles published on the subject. It was shown in some chapters the contents that are prerequisites, concepts and definitions that make understanding of Galois Theory possible. In the present work it was carried out a simple study of the Extensions of fields and the Correspondence of Galois.

Key-words: Polynomials, Field extensions, Galois teory.

Sumário

Introdução

Entre 1500 e 1515, o matemático italiano Scipione de Ferro (1456-1526) descobriu um procedimento para resolver a equação cúbica $x^3 + px + q = 0$ (em notação atual) Esse procedimento se traduz, modernamente na seguinte fórmula:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

Conforme (DOMINGUES; IEZZI, 2011) Del Ferro mostrou, com isso, que é possível expressar as raízes da cúbica considerada em termos de seus coeficientes, usando apenas adições, subtrações, multiplicações, divisões e radiciações. Ou, como se diz modernamente, que a equação dada é resolúvel por radicais. Como já se sabia há muitos séculos que as equações de grau um e dois também são resolúveis por radicais (no caso destas últimas, lembrar a chamada fórmula de Bhaskara), a solução de del Ferro colocou o seguinte desafio para os algebristas: será que toda equação algébrica é resolúvel por radicais? As pesquisas visando responder a essa questão se arrastaram por mais de dois séculos e meio, frustraram alguns dos grandes matemáticos desse período e contribuíram decisivamente para a criação do conceito de "grupos". Na verdade a questão da solubilidade das equações algébricas só começou a ser esclarecida genericamente na segunda metade do século XVIII. Na obra Réflexions sur la révolution algébrique des équations (Reflexões sobre a resolução algébrica de equações) (1770-1771), o ítalo-francês Joseph-Louis Lagrange (1736-1813), possivelmente o primeiro matemático a perceber com lucidez maior o caminho a ser seguido para abordar o problema, observou que a "teoria das permutações" era de grande importância para a resolução de equações. Lagrange referia-se a permutações envolvendo as raízes da equação. Em 1824, o matemático norueguês Niels Henrik Abel (1802-1829) provaria aquilo de que Lagrange suspeitara fortemente que não há nenhuma fórmula geral por radicais para resolver as equações de grau 5. Ainda assim uma questão permanecia em pé: já que as equações de grau 5 não são, de modo geral, solúveis por radicais, mas alguns tipos o são, como já se sabia bem antes de Abel, o que caracteriza matematicamente estas últimas? A resposta a essa pergunta seria dada pelo matemático francês Evariste Galois (1811-1832), em cuja obra aparece delineado pela primeira vez o conceito de grupo, inclusive com esse nome. Resumidamente, a ideia de Galois para responder a essa pergunta foi associar a cada equação um grupo formado por permutações de suas raízes e condicionar a solubilidade por radicais a uma propriedade desse grupo. E, como para toda equação de grau 4 o grupo de permutações que lhe é associado goza dessa propriedade e para n $>$ 4 sempre há equações cujo grupo não se sujeita a essa propriedade, a questão da resolubilidade por radicais estava por fim esclarecida.

Com o objetivo de continuar o estudo da Álgebra Abstrata, estudada durante a graduação, iniciaremos um trabalho de leitura e compreensão de introdução à Teoria de Galois. Este trabalho está dividido em quatro capítulos. No primeiro capítulo são apresentados recursos mínimos necessários ao bom desenvolvimento do trabalho, os quais são: as estruturas algébricas anéis e ideais, homomorfismo de anéis. Aqui também apresentamos algumas noções de álgebra linear. No segundo capítulo é feito um estudo dos polinômios em uma variável, devido a sua importância na construção das extensões de corpos. Os polinômios têm várias aplicações dentro da Matemática e em áreas da atividade científica como a Física entre outras. No terceiro capítulo, apresentamos a teoria relacionada aos corpos e extensões de corpos através do processo de adjunção de raízes de um polinômio. Provamos também, alguns resultados que são úteis no desenvolvimento da Teoria de Galois. Grande parte destes conceitos foram retirados de (GONÇALVES, 2002), (SILVA, 2013) e (OLIVEIRA; NEUMAN, 2014). No quarto capítulo, são apresentados exemplos de Extensões Galoisianas e Normais, fazendo uso de exemplos previamente discutidos nos capítulos anteriores, apresentação da Correspondência de Galois e demonstração do Teorema Fundamental da Teoria de Galois. A discussão teórica é necessária para a construção da Teoria Elementar de Galois.

1 Pré-requisitos

Neste capítulo apresentaremos os recursos mínimos necessários ao bom desenvolvimento do trabalho.

1.1 Anéis e ideais

Definição 1.1.1. *Seja A um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de adição e multiplicação em A e denotaremos por $+$ e $\cdot$:*

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

$$\begin{aligned} \cdot : A \times A &\to A \\ (a, b) &\mapsto a \cdot b. \end{aligned}$$

Diremos que $(A, +, \cdot)$ é um ***anel*** *se as seguintes propriedades são verificadas para quaisquer que sejam a, b, $c \in A$:*

(i) $(a + b) + c = a + (b + c)$;

(ii) *Existe* $0 \in A$ *tal que* $a + 0 = 0 + a = a$;

(iii) *Para qualquer* $a \in A$ *existe um único* $b \in A$, *denotado por* $b = -a$, *tal que* $a + b = b + a = 0$;

(iv) $a + b = b + a$;

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(vi) $a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(a + b) \cdot c = a \cdot c + b \cdot c$.

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

(vii) *Existe* $1 \in A - \{0\}$, *tal que* $a \cdot 1 = 1 \cdot a = a, \forall a \in A$, *diremos que* $(A, +, \cdot)$ *é um* ***anel com unidade*** 1.

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

(viii) Para qualquer $a, b \in A$, se $a \cdot b = b \cdot a$, diremos que $(A, +, \cdot)$ é um ***anel comutativo****.*

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

(ix) Dados a,b $\in$A, $a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$, diremos que (A,+,·) é um ***anel sem divisores de zero****.*

Se (A,+, ·) é um anel comutativo, com unidade e sem divisores de zero, dizemos que (A,+,·) é um ***domínio de integridade****.*

E finalmente, se um domínio de integridade (A,+,·) satisfaz a propriedade:

(x) Para qualquer $a \in A$ - $\{0\}$, existe b $\in$A tal que $a \cdot b = b \cdot a = 1$, diremos que (A,+,·) é um ***corpo****.*

Observação 1.1.1. *Por questão de simplicidade vamos denotar um anel $(A, +, \cdot)$, simplesmente por A, ficando subentendido as operações de adição e multiplicação.*

Exemplo 1.1.1. *Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ e $n \cdot \mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ munidos da soma e produto usuais são anéis. Já o conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$ é um anel munido das operações:*

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z}_n \\ (\overline{m}, \overline{n}) &\mapsto \overline{m+m} \ , \end{aligned}$$

e

$$\begin{aligned} \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\to \mathbb{Z}_n \\ (\overline{m}, \overline{n}) &\mapsto \overline{m \cdot m} \ . \end{aligned}$$

O conjunto $\mathbb{Z}[\sqrt{p}] = \left\{a + b\sqrt{p} : a, b \in \mathbb{Z}\right\}$ com p primo, são anéis com as operações abaixo:

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$$

e

$$(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pbd) + (bc + ad)\sqrt{p},$$

com $a, b, c, d \in \mathbb{Z}$.

O conjunto $\mathbb{Q}[\sqrt{p}] = \left\{a + b\sqrt{p} : a, b \in \mathbb{Q}\right\}$ também é um anel com às operações análogas as operações em $\mathbb{Z}[\sqrt{p}]$.

Entre esses anéis, são exemplos de corpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[\sqrt{p}]$ e $\mathbb{Z}_p$, com p primo.

Definição 1.1.2. *Seja A um anel e B um subconjunto não vazio de A. Dizemos que B é um* ***subanel*** *de A, se valem as condições:*

(i) $x, y \in B \Rightarrow x - y \in B$;

(ii) $x, y \in B \Rightarrow x \cdot y \in B$.

Exemplo 1.1.2. *Temos que $n\mathbb{Z}$ é subanel de $\mathbb{Z}$, por sua vez $\mathbb{Z}$ é subanel de $\mathbb{Q}$, este que é subanel de $\mathbb{R}$, já $\mathbb{R}$ é subanel de $\mathbb{C}$. Ademais, $\mathbb{Z}[\sqrt{p}]$ é subanel de $\mathbb{Q}[\sqrt{p}]$ e este é subanel de $\mathbb{R}$.*

Definição 1.1.3. *Um subanel B de um corpo K é chamado um* ***subcorpo*** *de K, se dado $a \in B - \{0\}$ existe $b \in B$ tal que $a \cdot b = 1$.*

Exemplo 1.1.3. *Observe que $\mathbb{Q}$ é subcorpo de $\mathbb{R}$, já $\mathbb{R}$ é subcorpo de $\mathbb{C}$. Ademais, $\mathbb{Q}[\sqrt{p}]$ é um subcorpo de $\mathbb{R}$.*

Definição 1.1.4. *Seja A um anel e seja I um subanel de A. Diremos que I é um* ***ideal*** *A se, $a \cdot x \in I, \forall a \in A, \forall x \in I$ e $n \cdot a \in I, \forall a \in A, \forall n \in I$.*

Os subanéis $\{0\}$ e A são ideais de A e são chamados de ideais triviais de A.

Exemplo 1.1.4. *Seja A um anel comutativo e $x_1, x_2, ..., x_n \in A$. É de direta verificação que o conjunto definido por*

$$A \cdot x_1 + A \cdot x_2 + ... + A \cdot x_n = \{a_1 \cdot x_1 + a_2 \cdot x_2 + ... + a_n \cdot x_n : a_i \in A\}$$

é um ideal de A, o qual é chamado de ideal gerado por $x_1, x_2, ..., x_n \in A$. Os ideais do tipo $I = A \cdot x_1$ são chamados ideais principais.

Observação 1.1.2. *Um anel em que todos os ideais são principais é chamado anel principal. O anel $\mathbb{Z}$ é um anel principal.*

Observação 1.1.3. *Se A é um anel com unidade 1 e J é um ideal de A tal que $1 \in J$, então $J = A$. De fato, primeiro note que $J \subset A$, pois J é ideal de A. Por outro lado, mostremos que $A \subset J$. Seja $x \in A$, como J é ideal e $1 \in J$, então $x = x \cdot 1 \in J$. Logo, $A \subset J$. Portanto $A = J$.*

Definição 1.1.5. *Seja A um anel e seja M um ideal de A. Dizemos que M é um ideal maximal de A se, $M \neq A$ e se J é ideal de A tal que $M \subset J \subset A$, então $J = M$ ou $J = A$.*

Exemplo 1.1.5. *O ideal $p\mathbb{Z}$ em $\mathbb{Z}$ com p primo é maximal. De fato, seja p primo e $J = p \cdot \mathbb{Z}$. Vamos provar que J é um ideal maximal em $\mathbb{Z}$. Considere I um ideal de $\mathbb{Z}$ tal que,*

$$J \subset I \subset \mathbb{Z}.$$

Como todo ideal de $\mathbb{Z}$ é principal, temos que existe um inteiro n tal que $I = n \cdot \mathbb{Z}$. Assim, $p \in p \cdot \mathbb{Z} \subset n \cdot \mathbb{Z}$, e daí segue $p = n \cdot k$ para algum $k \in \mathbb{Z}$, e portanto $n \mid p$ e teremos $n = \pm 1$ ou $n = \pm p$. Se $n = \pm 1$ temos que $I = \mathbb{Z}$ e se $n = \pm p$ temos que $I = J$.

Teorema 1.1.1. *Seja K um anel comutativo com unidade $1 \in K$. Então as seguintes condições são equivalentes:*

(i) K é um corpo;

(ii) $\{0\}$ é um ideal maximal em K;

(iii) Os únicos ideais de K são os triviais.

Demonstração: $(i) \Rightarrow (ii)$. Sejam K um corpo e J um ideal de K tal que $\{0\} \subset$ J $\subset$ K. Suponhamos $J \neq 0$. Assim existe a $\in J$, a $\neq 0$. Como K é um corpo, existe $b \in K$ tal que b $\cdot$ a = 1 e portanto $1 \in J$ e daí segue imediatamente que J = K.
$(ii) \Rightarrow (iii)$. Segue imediatamente das definições.
$(iii) \Rightarrow (i)$. Seja $0 \neq a \in K$ e $I = K \cdot a$ o ideal principal de K gerado por a. Como $1 \in K$, temos $a = 1 \cdot a \in I$, logo $I \neq 0$ e assim pela nossa hipótese, teremos I = K.
Portanto,

$$1 \in K = K \cdot a$$

donde existe $b \in K$ tal que $1 = b \cdot a$. Logo a é inversível em K.

□

Definição 1.1.6. *Um domínio de integridade D é dito de característica 0 se $m = 0$ sempre que $ma = 0$ com $a \in D, a \neq 0$ e $m \in \mathbb{N}$. Por outro lado, D diz-se de característica finita se existe $a \in D, a \neq 0$, tal que $ma = 0$ para algum inteiro $m \neq 0$. Nesse caso definimos como a característica de D o menor inteiro positivo m tal que $ma = 0$ para algum $a \in D, a \neq 0$*

Exemplo 1.1.6. *Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ tem característica 0, pois se $m \neq 0$, então $m \cdot 1 = m$ e, portanto, $m \cdot 1 \neq 0$.*

Exemplo 1.1.7. *Observemos primeiro que em $\mathbb{Z}_m$, $m \cdot \overline{1} = \overline{1} + \overline{1} + ... + \overline{1} = \overline{m} = \overline{0}$. Suponhamos, por outro lado, que para algum inteiro r, $0 < r < m$, tivéssemos $r \cdot \overline{1} = \overline{0}$. Como $r \cdot \overline{1} = \overline{r}$, então $\overline{r} = \overline{0}$, ou seja, $r \equiv 0 \pmod{m}$. Então $m \mid r$, o que é impossível, uma vez que $0 < r < m$. Logo, característica de $\mathbb{Z}_m = m$.*

Vamos agora definir a seguinte relação em A. Dados

$$x, y \in A, x \equiv y (mod J) \Leftrightarrow x - y \in J.$$

Primeiramente vamos provar que $\equiv (modJ)$ *define uma relação de equivalência em* A. *De fato, quaisquer que sejam* $x, y, z \in A$, *temos:*
(i) $x \equiv x(mod\ \ J)$ *pois* $0 = x - x \in J$.
(ii) $x \equiv y(mod\ \ J) \Rightarrow y \equiv x(mod\ \ J)$ *pois se* $x - y \in J$ *então* $y - x = -(x - y) \in J$.
(iii) $x \equiv y(mod\ \ J)$ *e* $y \equiv z(modJ) \Rightarrow x \equiv z(mod\ \ J)$ *pois,* $x - y \in J$ *e* $y - z \in J \Rightarrow$ $x - z = (x - y) + (y - z) \in J$.

Denotaremos por $\overline{x}$ *a classe de equivalência de* $x \in A$ *segundo a relação* $\equiv (mod\ \ J)$. *Assim,*

$$\overline{x} = \{y \in A : y \equiv x(mod\ \ J)\}.$$

Agora observe que $y \in \overline{x} \Leftrightarrow y - x \in J$, *e por isso também denotaremos essa classe* $\overline{x}$ *por* $\overline{x} = x + J = \{x + z : z \in J\}$. *Chamaremos de conjunto quociente de* A *pelo ideal* J, *ao conjunto* $A/J = \{\overline{x} = x + J : x \in A\}$.

Definiremos as seguintes operações em A/J:

$$\begin{aligned} + : A/J \times A/J &\to A/J \\ (\overline{a}, \overline{b}) &\mapsto \overline{a + b} \end{aligned}$$

e

$$\begin{aligned} \cdot : A/J \times A/J &\to A/J \\ (\overline{a}, \overline{b}) &\mapsto \overline{a \cdot b}\ . \end{aligned}$$

Munido destas operações temos que A/J *é um anel, chamado anel quociente.*

Observação 1.1.4. *Se* A *tem unidade, então* A/J *também tem. De fato, considere 1 a unidade de* A *e* $x \in A$. *Temos que,*

$$1 \cdot x = x \cdot 1 = x, \forall x \in A.$$

Agora seja $\overline{x} \in A/J$, *daí,* $\overline{x} = x + J = x \cdot 1 + J = \overline{x} \cdot \overline{1} \in A/J$.

Exemplo 1.1.8. *O anel quociente* $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ *com as operações induzidas pela soma e multiplicação de inteiros. Observe que*

$$\overline{0} = 0 + 4\mathbb{Z} = \{..., -12, -8, -4, 0, 4, 8, 12, ...\}$$

$$\overline{1} = 1 + 4\mathbb{Z} = \{..., -11, -7, -3, 1, 5, 9, 13, ...\}$$

$$\overline{2} = 2 + 4\mathbb{Z} = \{..., -10, -6, -2, 2, 6, 10, 14, ...\}$$

$$\overline{3} = 3 + 4\mathbb{Z} = \{..., -9, -5, -1, 3, 7, 11, 15, ...\}$$

Ademais, ao unirmos todas estas classes obtemos o próprio $\mathbb{Z}$. Ademais, a interseção de quaisquer duas classes é vazia.

Teorema 1.1.2. *Sejam A um anel comutativo com unidade 1 e J um ideal de A. Então J é um ideal maximal de A se, e somente se, A/J é um corpo.*

Demonstração: ($\Rightarrow$) Suponhamos J ideal maximal de A, e seja $\overline{0} \neq \overline{a} \in \overline{A} = A/J$. Temos que provar que existe $\overline{b} \in \overline{A}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. De fato, se $L = A \cdot a$ ideal principal de A gerado por a, temos que: J+L = $\{x + y : x \in J, y \in L\}$ é um ideal contendo J, e mais $\overline{a} \neq 0$ se e somente se, $a \notin J$. Como $a = 1 \cdot a \in L \subset J + L$ temos que $J + L$ é um ideal que contém J e mais $J + L \neq J$. Pela maximalidade de J segue que $A = J + L$ e daí vem, $1 \in J + L$ implica que existe $u \in J, v \in L$ tais que $1 = u + v$.
Assim, existe $u \in J, v \in L = A \cdot a$ e temos que $v = b \cdot a$ para algum $b \in A$, ou seja, existe $b \in A$ e $u \in J$ tais que $1 = u + b \cdot a$. Passando as classes de equivalência em ambos os membros, segue que, $\overline{1} = \overline{u + b \cdot a} = \overline{u} + \overline{b \cdot a} = \overline{0} + \overline{b} \cdot \overline{a}$, isto é, $\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b} = \overline{1}$, como queríamos demonstrar.
($\Leftarrow$) Por outro lado, suponhamos que $\overline{A} = A/J$ seja um corpo. Assim, $\overline{0}, \overline{1} \in \overline{A}$ implica que, $J \neq A$.
Se $M \neq J$ é um ideal de A e $J \subset M \subset A$, então teremos que existe $a \in M, a \notin J$, ou seja, $\overline{a} \neq \overline{0}$, com $\overline{a} \in \overline{A}$. Como $\overline{A}$ é corpo existe $\overline{b} \in \overline{A}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, ou ainda,

$$ab \equiv 1(mod\ \ J) \Leftrightarrow ab - 1 \in J \Leftrightarrow \exists\ \ u \in J$$

tal que $ab - 1 = u$, e isto nos diz que, $1 = ab - u$. Como $a \in M$ segue que $ab \in M$ e como $u \in J \subset M$ temos também $u \in M$. Logo concluímos que $1 = ab - u \in M$ e imediatamente temos $M = A$.

□

1.2 Homomorfismo de anéis

Podemos descobrir informações sobre um anel examinando sua interação com outros anéis. Fazemos isto através do homomorfismo que, é uma aplicação que preserva as operações dos anéis.

Sejam A e B dois anéis e sejam 0 o elemento neutro de A e $0'$ o elemento neutro de B. Se ambos anéis A e B possuem unidade, denotaremos por 1 a unidade de A e por $1'$ a unidade de B.

Definição 1.2.1. *Uma função $f : A \to B$ diz-se um homomorfismo de A em B se satisfaz as seguintes condições:*

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

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

Exemplo 1.2.1. *Sejam A e B dois anéis quaisquer. Então $f : A \to B$, dada por $f(a) = 0$, para todo $a \in A$, é claramente um homomorfismo de anéis. Vejamos, sejam a, $b \in A$. Têm-se:*

$$f(a+b) = 0 = 0 + 0 = f(a) + f(b),$$
$$f(a \cdot b) = 0 = 0 \cdot 0 = f(a) \cdot f(b).$$

Proposição 1.2.1. *Sejam A e B anéis e $f : A \to B$ um homomorfismo.*

Então,

(i) $f(0) = 0'$
(ii) $f(-a) = -f(a)$ *para todo e qualquer* $a \in A$
(iii) Se A e B são domínios de integridade então ou f é a função constante zero ou $f(1) = 1'$.
(iv) Se A e B são corpos então ou f é a função constante zero ou f é injetiva.

Demonstração: (i) Em um anel a equação $X + X = X$ tem o elemento neutro como única solução e assim temos,

$$0 + 0 = 0 \Rightarrow f(0+0) = f(0) + f(0) = f0)$$

e portanto $f(0) = 0'$ que é elemento neutro de B.
(ii) Seja $a \in A$. De $a + (-a) = 0$ segue pelo intem (i) que:

$$f(a) + f(-a) = 0'$$

ou seja,

$$f(-a) = -f(a)$$

(iii) De $1 \cdot 1' = 1$ segue que $f(1)^2 = f(1)$, isto é, $f(1) \cdot (f(1) - 1') = 0'$. Agora, B é domínio de integridade nos diz que ou $f(1) = 0'$ ou $f(1) = 1'$.

Se $f(1) = 0'$ então segue que $f(x) = f(x \cdot 1) = f(x) \cdot f(1) = f(x) \cdot 0' = 0'$ para todo e qualquer $x \in A$, ou seja, f é a função constante zero.
(iv) Sejam A e B corpos. Suponhamos que f não é uma função constante zero. Pelo item (iii) sabemos que $f(1) = 1'$. Provaremos que f é injetiva. De fato. Se x, $y \in A$ e $f(x) = f(y)$ teremos, $f(x - y) = 0'$. Suponhamos por absurdo que $x \neq y$, então $x - y \neq 0$ e A é corpo, nos diz que existe $b \in A$ tal que $b \cdot (x - y) = 1$ e daí segue que $f(b) \cdot f(x - y) = f(b) \cdot 0' = 1'$ que é uma contradição.

□

Teorema 1.2.1. *Sejam A e B anéis e $f : A \to B$ um homomorfismo. Então:*

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

(ii) *$ker(f) = \{a \in A : f(a) = 0'\}$ é um ideal de A e f é injetiva se, e somente se, $ker(f) = 0$;*

(iii) *Os anéis $\frac{A}{ker(f)}$ e $Im\ f$ são isomorfos.*

Demonstração: (i) De fato temos:

(a) $0' = f(0) \in Imf$.

(b) $f(a), f(b) \in Imf \to f(a) - f(b) = f(a - b) \in Imf$.

(c) $f(a), f(b) \in Imf \Rightarrow f(a) \cdot f(b) = f(a \cdot b) \in Imf$.

(ii) Vamos mostrar que $ker(f) = \{a \in A : f(a) = 0'\}$ é um ideal de A. De fato,

(a) $0 \in ker(f)$ pois $f(0) = 0'$.

(b) $a, b \in ker(f) \Rightarrow f(a - b) = f(a) - f(b) = 0' - 0' = 0$, ou seja $a - b \in ker(f)$.

(c) Seja $x \in A$ e $a \in ker(f)$ então

$$f(a \cdot x) = f(a) \cdot f(x) = 0' \cdot f(x) = 0'$$

e

$$f(x \cdot a) = f(x) \cdot f(a) = f(x) \cdot 0' = 0',$$

ou seja, $a \cdot x \in ker(f)$ e $x \cdot a \in ker(f)$. Assim $ker(f)$ é um ideal de A.

Agora, se f é injetiva, segue imediatamente que $ker(f) = \{0\}$ pois $f(0) = 0'$.

Se $f(x) = f(y), x, y \in A$ e $ker(f) = \{0\}$ segue, $f(x) - f(y) = 0' \Rightarrow f(x - y) = 0' \Rightarrow x - y \in ker(f) = \{0\} \Rightarrow x = y$ como queríamos mostrar.

Vamos demonstrar o item (iii), para isso definiremos uma função

$$\begin{aligned} F : \frac{A}{ker(f)} &\to Imf \\ \overline{a} &\mapsto f(a). \end{aligned}$$

Primeiramente, devemos verificar que F é uma função bem definida, isto é, se $a_1, a_2 \in A$ são tais que $\overline{a_1} = \overline{a_2}$, então $f(a_1) = f(a_2)$. De fato, se $\overline{a_1} = \overline{a_2}$, então $a_1 - a_2 \in ker(f)$,

logo $f(a_1 - a_2) = 0$; ademais $f(a_1 - a_2) = f(a_1) - f(a_2)$, pois f é um homomorfismo; portanto, $f(a_1) = f(a_2)$.

Agora, F é uma aplicação sobrejetiva e é um homomorfismo pois, para elementos a_1, $a_2 \in A$, temos:
(a) $F(\overline{a_1} + \overline{a_2}) = F(\overline{a_1 + a_2}) = f(a_1 + a_2)$ pela definição de F.
Por f ser um homomorfismo $f(a_1 + a_2) = f(a_1) + f(a_2) = F(\overline{a_1}) + F(\overline{a_2})$.
(b) Analogamente ao item a) têm-se;

$$\begin{aligned} F(\overline{a_1} \cdot \overline{a_2}) &= F(\overline{a_1 \cdot a_2}) = f(a_1 \cdot a_2) \\ &= f(a_1) \cdot f(a_2) = F(\overline{a_1}) \cdot F(\overline{a_2}). \end{aligned}$$

Por fim, temos que $ker(F) = \left\{\overline{a} \in \frac{A}{ker(f)} : f(a) = 0\right\} = \left\{\overline{a} \in \frac{A}{ker(f)} : a \in ker(f)\right\} = \{\overline{0}\}$.
Logo F é injetiva.

□

1.3 Noçoes básicas de álgebra linear

Nesta seção relembraremos algumas noções básicas de álgebra linear, como espaço vetorial e base. Grande parte destes conceitos foram retirados de (COELHO; LOURENÇO, 2007).

Definição 1.3.1. *Seja K um corpo qualquer e seja V um conjunto não vazio onde está definida uma operação de adição. Suponhamos também que esteja definida, uma operação de elementos de K por elementos de V. Assim, estão definidas:*

$$\begin{aligned} + : V \times V &\to V \\ (u, v) &\mapsto u + v \end{aligned}$$

e

$$\begin{aligned} \cdot : K \times V &\to V \\ (\lambda, v) &\mapsto \lambda \cdot v. \end{aligned}$$

Dizemos que V munido dessas operações é um espaço vetorial sobre o corpo K se as seguintes proposições são verificadas quaisquer que sejam $u, v, w \in V$ e $\lambda, \mu \in K$:

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

(ii) Existe 0 *que pertence a* V *tal que* $u + 0 = 0 + u = u$.

(iii) *Para todo x que pertence a V, existe y que pertence a V tal que $x + y = y + x = 0$.*

(iv) $u + v = v + u$.

(v) $1v = v$ *onde* 1 *é a unidade do corpo* K.

(vi) $\lambda(u + v) = \lambda u + \lambda v$ *e* $(\mu + \lambda)u = \mu u + \lambda u$.

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

Observação 1.3.1. *Até o fim desta seção K representa um corpo e V um espaço vetorial sobre K. Um subconjunto não vazio $W \subset V$ diz-se um subespaço vetorial de V se as seguintes condições são satisfeitas:*

(i) $0 \in W$

(ii) $w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$;

(iii) $\lambda \in K, w \in W \Rightarrow \lambda w \in W$.

Observe que pelas condições acima as operações do espaço vetorial V induzem operações em W e o próprio W é um espaço vetorial com as operações induzidas.

Se $v_1, ..., v_n \in V$ dizemos que $v_1, ..., v_n$ são linearmente independentes se a equação vetorial $\sum_{i=1}^{n} \alpha_i v_i = 0, \alpha_i \in K$ é satisfeita apenas para os escalares $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$. Caso contrário dizemos que $v_1, ..., v_n$ são linearmente dependentes. Usamos simbolicamente L.I para linearmente independentes e L.D para linearmente dependentes. Por exemplo, $e_1 = (1, 0, ..., 0), e_2 = (0, 1, ..., 0), ..., e_n = (0, 0, ..., 1)$ são L.I em K^n.

Se $u_1, u_2, ..., u_r \in V$ então é fácil vericar que

$$W = \left\{ \sum_{i=1}^{r} \alpha_i u_i : \alpha_i \in K, i = 1, ..., r \right\}$$

é um subespaço vetorial de V, o qual chamaremos de subespaço gerado por $u_1, ..., u_r$. Denotaremos esse espaço por,

$$W = \langle u_1, ..., u_r \rangle .$$

Se um conjunto (ordenado) $v_1, ..., v_n \in V$ for L.I. e tal que $\langle v_1, ..., v_n \rangle = V$ dizemos que $v_1, ..., v_n$ é uma base de V. Por exemplo, $e_1, ..., e_n$ é uma base de K^n.

Definição 1.3.2. *Dizemos que um espaço vetorial V sobre K é finitamente gerado se possuir um conjunto gerador finito.*

Proposição 1.3.1. *Seja V um K-espaço vetorial finitamente gerado não nulo e assuma que $\{v_1, ..., v_m\}$ seja um conjunto gerador de V. Então todo conjunto L.I de vetores de V tem no máximo m elementos.*

Demonstração Vamos mostrar que todo conjunto de elementos de V que contenha mais do que m vetores é L.D. Para tanto, seja $A = \{u_1, ..., u_n\} \subseteq V$ com $n > m$. Observe que, como $\{v_1, ..., v_m\}$ é um conjunto gerador de V, então existem escalares $\alpha_{ij} \in K$ tais que para cada $j = 1, ..., n$,

$$u_j = \alpha_{ij}v_1 + ... + \alpha_{mj}v_m = \sum_{i=1}^{m} \alpha_{ij}v_i.$$

Assim, se $\lambda_1, ..., \lambda_n$ são escalares quaisquer em K, teremos

$$\lambda_1 u_1 + ... + \lambda_n u_n = \sum_{j=1}^{n} \lambda_j u_j = \sum_{j=1}^{n} \lambda_j \left(\sum_{i=1}^{m} \alpha_{ij} v_i \right) =$$

$$= \sum_{j=1}^{n} \sum_{i=1}^{m} \lambda_j \alpha_{ij} v_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \lambda_j \alpha_{ij} \right) v_i.$$

Vamos analisar a situação em que $\sum_{j=1}^{n} \lambda_j \alpha_{ij} = 0$, para cada $i = 1, ..., m$.

Para tanto, consideremos o sistema

$$\begin{cases} \alpha_{11}\lambda_1 + ... + \alpha_{1n}\lambda_n = 0 \\ \vdots \\ \alpha_{m1}\lambda_1 + ... + \alpha_{mn}\lambda_n = 0 \end{cases} \tag{1.1}$$

nas incógnitas $\lambda_1, ..., \lambda_n$ e com coeficientes $\alpha_{ij} \in K$. Como o número de equações de (1.1) é estritamente menor do que o número de incógnitas, segue que (1.1) tem uma solução não nula, isto é, existem $\gamma_1, ..., \gamma_n \in K$, não todos nulos, tais que

$$\sum_{j=1}^{n} \gamma_j \alpha_{ij} = 0$$

para $i = 1, ..., m$. Portanto, $\gamma_1 u_1 + ... + \gamma_n u_n = 0$ com $\gamma_1, ..., \gamma_n$ não todos nulos, o que implica que $\{u_1, ..., u_n\}$ é L.I.

□

Corolário 1.3.1. *Seja V um K-espaço vetorial finitamente gerado não nulo. Então duas bases quaisquer de V têm o mesmo número de elementos.*

Demonstração: Sejam B e B' duas bases de V. Como é finitamente gerado, decorre da Proposição 1.3.1 que B e B' são finitas com, m e m' elementos respectivamente. Considerando B como conjunto gerador de V e B' L.I segue da Proposição 1.3.1 que $m' \leq m$. Por outro lado, considerando B' como conjunto gerador e B L.I, teremos $m \leq m'$. Daí segue que $m = m'$.

□

2 Polinômio em uma variável

2.1 Definição e exemplos

Definição 2.1.1. *Seja K um corpo qualquer. Chamaremos de um polinômio sobre K em uma indeterminada x a uma expressão formal*

$$p(x) = a_0 + a_1x + ... + a_mx^m + ... \ ,$$

onde $a_i \in K, \forall i \in \mathbb{N}$ e $\exists n \in \mathbb{N}$ tal que $a_j = 0, \forall j \geq n$.

Dizemos que dois polinômios

$$p(x) = a_0 + a_1x + ... + a_mx^m + ...$$

e

$$q(x) = b_0 + b_1x + ... + b_kx^k + ...$$

sobre K são iguais se, e somente se $a_i = b_i$ em $K, \forall i \in \mathbb{N}$.

Se $p(x) = 0+0x+...+0x^m+...$, indicaremos $p(x)$ por 0 e o chamaremos de polinômio identicamente nulo sobre K. Assim um polinômio $p(x) = a_0 + a_1x + ... + a_mx^m + ...$ sobre K é identicamente nulo se, e somente se $a_i = 0 \in K, \forall i \in \mathbb{N}$.
Se $a \in K$ indicaremos por a ao polinômio $p(x) = a_0 + a_1x + ... + a_nx^n + ...$ onde $a_0 = a$, e $a_i = 0, \forall i \geq 1$. Chamaremos ao polinômio $p(x) = a, a \in K$ de polinômio constante a.

Exemplo 2.1.1. *São exemplos de polinômios constantes no corpo dos reais,*

$$p(x) = 7, \quad f(x) = \sqrt{2}, \quad g(x) = \frac{3}{5},$$

de modo geral, $p(x) = k$, com $k \in \mathbb{R}$.

Se $p(x) = a_0 + a_1x + ... + a_nx^n + ...$ é tal que $a_n \neq 0$ e $a_j = 0, \forall j > n$ dizemos que n é o grau do polinômio $p(x)$ e nesse caso indicaremos $p(x) = a_0 + a_1x + ... + a_nx^n$, e o grau de $p(x)$ por $\partial p(x) = n$.

Exemplo 2.1.2. *No polinômio $p(x) = x^4 - 10x^3 + 24x^2 + 10x - 24$, note que o termo que possui um maior expoente é x^4. Portanto o grau deste polinômio é 4.*

Vamos denotar por $K[x]$ o conjunto de todos os polinômios sobre K, em uma indeterminada x. Observe que não está definido o grau do polinômio 0, e ∂ pode ser interpretada como uma função do conjunto de todos os polinômios não nulos no conjunto $\mathbb{N}$. Assim,

$$\begin{aligned} \partial : K[x] - \{0\} &\rightarrow \mathbb{N} \\ p(x) &\mapsto \partial p(x) = grau \ \ de \ \ p(x) \end{aligned}$$

Agora vamos definir duas operações no conjunto $K[x]$. Sejam

$$p(x) = a_0 + a_1x + ... + a_mx^m$$

e

$$q(x) = b_0 + b_1x + ... + b_rx^r$$

dois elementos do conjunto $K[x]$. Definimos

$$p(x) + q(x) = c_1x + ... + c_kx^k,$$

onde $c_i = (a_i + b_i) \in K$, e

$$p(x) \cdot q(x) = c_0 + ... + c_kx^k,$$

onde $c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0, c_2 = a_0b_2 + a_1b_1 + a_2b_0, ..., c_k = a_0b_k + a_1b_{k-1} + ... + a_{k-1}b_1 + a_kb_0$ com $k \in \mathbb{N}$.

Observe que a definição acima de produto provém da regra $x^m \cdot x^n = x^{m+n}$ e da propriedade distributiva. Convencionam-se também as regras $x^0 = 1$ e $x^1 = x$. Note que $K[x]$ é um domínio de integridade, onde o polinômio 0 é o elemento neutro de $K[x]$ e o polinômio constante 1 é a unidade de $K[x]$. Observe que se identificarmos os elementos $a \in K$ com os polinômios constantes $p(x) = a$ podemos pensar em $K[x]$ contendo o corpo K.

2.2 O algoritmo da divisão

Teorema 2.2.1. *(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 $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Demonstração: Seja $f(x) = a_0 + a_1x + ... + a_nx^n$ e $g(x) = b_0 + b_1x + ... + b_mx^m$, com $(\partial g(x) = m)$.
Existência:
Se $f(x) = 0$ basta tomar $q(x) = r(x) = 0$. Suponhamos $f(x) \neq 0$. Assim $\partial f = n$. Se $n < m$ basta tomar $q(x) = 0$ e $r(x) = f(x)$. Assim podemos assumir $n \geq m$. Agora seja $f_1(x)$ o polinômio definido por

$$f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + f_1(x).$$

Observe que $\partial f_1(x) < \partial f(x)$. Vamos demonstrar o Teorema por indução sobre $\partial f = n$. Se $n = 0, n \geq m \Rightarrow m = 0$ e portanto $f(x) = a_0 \neq 0, g(x) = b_0 \neq 0$ e teremos,

$$f(x) = a_0 b_0^{-1} g(x)$$

e basta tomar $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$. Pela igualdade $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ e $\partial f_1(x) < \partial f(x) = n$. Temos pela hipótese de indução que: existem $q_1(x), r_1(x)$ tais que:

$$f_1(x) = q_1(x) \cdot g(x) + r_1(x),$$

onde $r_1(x) = 0$ ou $\partial r_1(x) < \partial g(x)$. Daí segue imediatamente que:

$$f(x) = (q_1(x) + a_n b_m^{-1} x^{n-m}) g(x) + r_1(x)$$

e portanto tomando $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r_1(x) = r(x)$ provamos a existência dos polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$, e $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Agora vamos provar a unicidade. Sejam $q_1(x), q_2(x), r_1(x)$ e $r_2(x)$ tais que:

$$f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x),$$

onde $r_1(x) = 0$ ou $\partial r_i(x) < \partial g(x), i = 1, 2$. Daí segue:

$$(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x).$$

Mas se $q_1(x) \neq q_2(x)$ o grau do polinômio do lado esquerdo da igualdade acima é maior ou igual ao $\partial g(x)$ enquanto que o $\partial(r_2(x) - r_1(x)) < \partial g(x)$ o que é uma contradição. Logo $q_1(x) = q_2(x)$ e daí segue

$$r_1(x) = f(x) - q_1(x)g(x) = f(x) - q_2(x)g(x) = r_2(x).$$

□

Exemplo 2.2.1. *Determine $q(x)$ e $r(x)$ tais que:*

$$f(x) = q(x) \cdot g(x) + r(x)$$

onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$ e $f(x)$, $g(x) \in \mathbb{R}[x]$.

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

$$\begin{array}{r} \Big(\quad x^3 + 3x^2 \quad - x - 3 \Big) : \Big(x - 1 \Big) = x^2 + 4x + 3 \\ \underline{- x^3 \quad + x^2} \\ \qquad\qquad 4x^2 \quad - x \\ \qquad\quad \underline{- 4x^2 + 4x} \\ \qquad\qquad\qquad 3x - 3 \\ \qquad\qquad\quad \underline{- 3x + 3} \\ \qquad\qquad\qquad\quad 0 \end{array}$$

$q(x) = x^2 + 4x + 3$

$r(x) = 0x$

$$f(x) = q(x) \cdot g(x) + r(x)$$
$$(x^3 + 3x^2 - x - 3) = (x^2 + 4x + 3) \cdot (x - 1) + 0x.$$

2.3 Ideais principais e máximo divisor comum

Teorema 2.3.1. *Todo ideal de $K[x]$ é principal.*

Demonstração: Seja J um ideal de $K[x]$. Se $J = \{0\}$ então J é gerado por 0. Suponhamos que $J \neq \{0\}$ e escolhemos $0 \neq p(x) \in J$ tal que $\partial p(x)$ seja o menor possível. Se $p(x) = a \neq 0$ então $1 = a^{-1} \cdot a \in J$ e assim segue imediatamente que $J = K[x]$ é gerado por $1 \in K[x]$. Suponhamos então $\partial p(x) > 0$. Como $p(x) \in J$, claramente temos $K[x] \cdot p(x) \subset J$. Agora vamos provar que $J \subset K[x] \cdot p(x)$. De fato, seja $f(x) \in J$. Pelo algoritmo da divisão temos que existem $q(x), r(x) \in K[x]$ tais que $f(x) = q(x) \cdot p(x) + r(x)$ onde ou $r(x) = 0$ ou $\partial r(x) < \partial p(x)$. Agora, como $f(x), p(x) \in J$ segue imediatamente que $r(x) = f(x) - q(x) \cdot p(x) \in J$ e pela minimalidade de nossa escolha do polinômio $p(x) \in J$ segue que $r(x) = 0$ e portanto temos $f(x) = q(x) \cdot p(x) \in K[x] \cdot p(x)$.

□

Definição 2.3.1. *Sejam $f(x)$, $g(x) \in K[x]$, com $g(x) = 0$. Dizemos que $g(x)$ divide $f(x)$ em $K(x)$ se existe $h(x) \in K[x]$ tal que,*

$$f(x) = h(x) \cdot g(x).$$

Se $g(x)$ é um divisor de $f(x)$ em $K[x]$ escrevemos $g(x) \mid f(x)$ em $K[x]$.

Definição 2.3.2. *Se $f(x) = a_0 + a_1x + ... + a_nx^n$ é um polinômio não nulo de $K[x]$ tal que $a_n = 1$ dizemos que $f(x)$ é um polinômio* ***mônico*** *em $K[x]$.*

Definição 2.3.3. *Sejam $f(x), g(x)$ polinômios não nulos em $K[x]$ e seja $d(x) \in K[x]$ um polinômio mônico tal que $d(x)$ divide $f(x)$ e $g(x)$ e se $h(x) \in K[x]$ é tal que $h(x)$ divide $f(x)$ e $g(x)$, então $h(x)$ divide $d(x)$. A este polinômio $d(x)$ chamamos de máximo divisor comum de $f(x)$ e $g(x)$. Se $d(x) = 1$, então $f(x)$ e $g(x)$ são primos entre si.*

Teorema 2.3.2. *(Existência de M.D.C). Sejam $p_1(x), ..., p_m(x) \in K[x] - \{0\}$ e seja o ideal $J = K[x] \cdot p_1(x) + ... + K[x] \cdot p_m(x)$ de $K[x]$ gerado pelos polinômios não nulos $p_1(x), ..., p_m(x)$. Se $d(x) \in K[x]$ é tal que $J = K[x] \cdot d(x)$ então são válidas as seguintes propriedades:*

(i) existem $r_1(x), ..., r_m(x) \in K[x]$ tais que

$$d(x) = r_1(x) \cdot p_1(x) + ... + r_m(x) \cdot p_m(x);$$

(ii) $d(x)$ é um divisor comum de $p_1(x), ..., p_m(x)$;

(iii) Se $h(x)$ é um divisor comum qualquer de $p_1(x), ..., p_m(x)$, então $h(x)$ é também um divisor de $d(x)$.

Demonstração:(i) Decorre da igualdade

$$K[x] \cdot d(x) = K[x] \cdot p_1(x) + ... + K[x] \cdot p_m(x).$$

(ii) Seja $i \in 1, ..., m$ e $K[x] \cdot d(x) = K[x] \cdot p_1(x) + ... + K[x] \cdot p_m(x)$ temos que,

$$p_i(x) \in K[x] \cdot p_i(x) \subset K[x] \cdot p_1(x) + ... + K[x] \cdot p_m(x) = K[x] \cdot d(x)$$

e portanto existe $r_i(x) \in K[x]$ tal que $p_i(x) = r_i(x) \cdot d(x)$, isto é, $d(x)$ é um divisor de cada $p_i(x)$, com $i = 1, ..., m$.
(iii) Seja $h(x)$ um divisor comum em $K[x]$, de $p_1(x), ..., p_m(x)$, isto é, existe $r_i(x) \in K[x]$ tal que $p_i(x) = r_i(x) \cdot h(x)$, com $i = 1, ..., m$.
Assim,

$$K[x] \cdot p_i(x) \subset K[x] \cdot h(x), \forall i \in 1, ..., m$$

e daí segue que,

$$K[x] \cdot d(x) = K[x] \cdot p_1(x) + ... + K[x] \cdot p_m(x) \subset K[x] \cdot h(x),$$

ou seja, existe $r(x) \in K[x]$ tal que $d(x) = r(x) \cdot h(x)$.

□

2.4 Polinômios irredutíveis e ideais maximais

Definição 2.4.1. *Seja $f(x) \in K[x]$ tal que $\partial f(x) \geq 1$. Dizemos que $f(x)$ é um polinômio irredutível sore K se toda vez que $f(x) = g(x) \cdot h(x)$, com $g(x), h(x) \in K[x]$ então temos $g(x) = a$ constante em K ou $h(x) = b$ constante em K. Se $f(x)$ for não irredutível sobre K dizemos que f é redutível sobre K.*

Exemplo 2.4.1. *O polinômio $p(x) = x^2 - 3 \in \mathbb{Q}[x]$ é irredutível em $\mathbb{Q}[x]$, porém $p(x) = x^2 - 3$ é redutível em $\mathbb{R}[x]$, pois,*

$$x^2 - 3 = (x + \sqrt{3})(x - \sqrt{3}), \text{ com } \sqrt{3} \in \mathbb{R}.$$

Exemplo 2.4.2. *O polinômio $p(x) = x^2 + 3$ é irredutível em $\mathbb{R}[x]$, mas é redutível em $\mathbb{C}[x]$, pois,*

$$x^2 + 3 = (x + \sqrt{3}i)(x - \sqrt{3}i), \text{com } i = \sqrt{-1} \text{ e } \sqrt{3}i \in \mathbb{C}.$$

Teorema 2.4.1. *Sejam K um corpo e $p(x) \in K[x]$. As seguintes condições são equivalentes:*

(i) $p(x)$ é irredutível sobre K.

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

(iii) $\dfrac{K[x]}{J}$ é um corpo, onde $J = K[x] \cdot p(x)$.

Demonstração: Vamos mostrar que $(i) \Leftrightarrow (ii)$.
$(i) \Rightarrow (ii)$: Suponhamos $p(x) \in K[x]$, com $p(x)$ irredutível sobre K e seja $J = K[x] \cdot p(x) = \{g(x) \cdot p(x); g(x) \in K[x]\}$. Como grau $p(x) \geq 1$ temos imediatamente que $J \neq K[x]$. Se $I = K[x] \cdot h(x)$ é um ideal de $K[x]$ tal que $I \supset J$ vamos provar que $I = J$ ou $I = K[x]$. Assim, $p(x) \in K[x] \cdot p(x) \subset K[x] \cdot h(x)$ nos diz que, $p(x) = g(x) \cdot h(x)$ para algum $g(x) \in K[x]$. Como $p(x)$ é irredutível temos que $g(x) = a \in K - \{0\}$ constante ou $h(x) = b \in K - \{0\}$ constante. Se $g(x) = a \neq 0$ constante temos que $h(x) = a^{-1} \cdot p(x)$ e portanto $I = K[x] \cdot h(x) \subset K[x] \cdot p(x) = J$ e isto nos dá $I = J$. Se $h(x) = b \neq 0$ constante temos $I = K[x] \cdot h(x) = K[x]$ e isto termina a implicação $(i) \Rightarrow (ii)$.
$(ii) \Rightarrow (i)$: Seja $J = K[x] \cdot p(x)$ um ideal maximal em $K[x]$. Assim $J \neq K[x]$ nos diz que $\partial p(x) \geq 1$. Suponhamos $g(x), h(x) \in K[x]$ e $p(x) = g(x) \cdot h(x)$. Assim segue imediatamente que $J \subset I = K[x] \cdot h(x)$ e como J é maximal temos que $J = I$ ou $I = K[x]$. Se $J = I$ segue que $h(x) \in J = K[x] \cdot p(x)$ e isto nos diz que $h(x) = f(x) \cdot p(x)$ para

algum $f(x) \in K[x]$. Daí segue que $p(x) = g(x) \cdot f(x) \cdot p(x)$. Como $p(x) \neq 0$ e $K[x]$ é um domínio de integridade teremos $1 = g(x) \cdot f(x)$, isto é, $g(x) \in K[x]$ é um polinômio invertível em $K[x]$. Portanto temos imediatamente que $g(x) = a \neq 0$ é um polinômio constante. Se $I = K[x]$ segue imediatamente que $h(x) = b \neq 0$ constante ou seja $p(x)$ é irredutível sobre K.
$(ii) \Rightarrow (iii)$ Sai imediatamente do Teorema 1.1.2.

□

2.5 Fatorização única

Teorema 2.5.1. *Seja K um corpo então todo polinômio $f(x) \in K[x] - \{0\}$ pode ser escrito na forma,*

$$f(x) = u \cdot p_1(x)...p_m(x),$$

onde $u \in K - \{0\}$ e $p_1(x), p_2(x), ..., p_m(x)$ são polinômios irredutíveis sobre K (não necessariamente distintos). Mais ainda, essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), ..., p_m(x)$.

Demonstração: Seja $f(x) \in K[x] - \{0\}$. Vamos provar por indução sobre o $\partial f(x) = n$. Se $n = 0, f(x) = u$ constante não nula. Assim podemos assumir $\partial f(x) = n \geq 1$. Vamos supor pela hipótese de indução que todo polinômio não nulo de grau menor que n pode ser escrito na expressão desejada e vamos demonstrar que $f(x)$ também pode ser escrito naquela expressão.

Suponhamos, por absurdo, que $f(x)$ não possa ser escrito como produto de irredutíveis. Então $f(x)$ é um polinômio irredutível sobre K. Assim, existem

$$g(x),\ h(x) \in K[x],\ 1 \leq \partial g(x) < n,\ 1 \leq \partial h(x) < n$$

tais que

$$f(x) = g(x)h(x).$$

Agora, por indução temos,

$$g(x) = a \cdot p_1(x)...p_r(x), a \in K - \{0\} \text{ e } p_1(x), ..., p_r(x)$$

polinômios irredutíveis sobre K. Analogamente,

$$h(x) = b \cdot p_{r+1}(x)...p_m(x), b \in K - \{0\} \text{ e } p_{r+1}(x), ..., p_m(x)$$

polinômios irredutíveis sobre K. Assim

$$f(x) = u \cdot p_1(x)...p_m(x) = u' \cdot q_1(x)...q_s(x),$$

onde $u, u' \in k - \{0\}$ e $p_1(x), ..., p_m(x), q_1(x)...q_s(x)$ são polinômios irredutíveis sobre K. Assim temos,

$$p_1(x) \mid q_1(x)...q_s(x)$$

e daí segue que existe $u'_i \in K - \{0\}$ tal que $q_i(x) = u'_i \cdot p_1(x)$ (nesse caso dizemos que $q_i(x)$ e $p_1(x)$ são associados em $K[x]$). Agora o Teorema segue por indução sobre m. Se $m = 1$ e $p_1(x)$ irredutível temos que necessariamente $s = 1$ e $p_1(x)$ e $q_i(x)$ são associados em $K[x]$.

Suponhamos $m > 1$. De $q_i(x) = u'_i \cdot p_1(x)$ e sendo $K[x]$ um domínio temos que:

$$u \cdot p_2(x)...p_m(x) = u' \cdot u_i \cdot q_1(x)...p_{i-1}(x) \cdot p_{i+1}(x)...p_s(x)$$

e daí segue pela hipótese de indução que $m - 1 = s - 1$ (isto é, $m = s$) e mais, cada $q_j(x)$ está associado com algum $p_i(x)$ através de uma constante, e isto termina a demonstração.

□

2.6 O critério de Eisenstein

Proposição 2.6.1. *(Gauss). Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$ então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: Suponhamos que $f(x)$ seja irredutível sobre $\mathbb{Z}$, mas $f(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in \mathbb{Q}[x]$ e $1 \leq \partial g(x), \partial h(x) < \partial f(x)$. Claramente existe inteiro positivo m tal que $m \cdot f(x) = g_1(x) \cdot h_1(x)$ onde $g_1(x), h_1(x) \in \mathbb{Z}[x]$.
Assim temos,

$$g_1(x) = a_0 + a_1x + ... + a_rx^r, a_i \in \mathbb{Z}$$

e

$$h_1(x) = b_0 + b_1x + ... + b_sx^s, b_j \in \mathbb{Z}.$$

Suponhamos agora que $p \mid m$, com p primo. Vamos provar que $p \mid a_i$, $\forall i \in \{1, ..., r\}$ ou $p \mid b_j$, $\forall j \in \{1, ..., s\}$.
De fato, se existe $i \in \{1, ..., r\}$ e existe $j \in \{1, ..., s\}$ tais que $p \nmid a_i$ e $p \nmid b_j$ consideremos

i e j menores possíveis com esta propriedade. Ora, como $p \mid m$ temos que p divide o coeficiente de x^{i+j} do polinômio $m \cdot f(x) = g_1(x) \cdot h_1(x)$, isto é,

$$p \mid (b_0a_{i+j} + b_1a_{i+j-1} + ... + b_ja_i + ... + b_{i+j-1}a_1 + b_{i+j}a_0).$$

Pela nossa escolha de i e j temos que p divide cada parcela, exceto b_ja_i, do coeficiente de x^{i+j} de $g_1(x) \cdot h_1(x)$. Como p divide toda a expressão segue também que $p \mid b_ja_i$ e como p é um número primo temos que $p \mid b_j$ ou $p \mid a_i$ que é uma contradição.
Assim, se p primo, $p \mid m \Rightarrow p \mid a_i$, $\forall i \in \{1, ..., r\}$ ou $p \mid b_j$, $\forall j \in \{1, ..., s\}$. Sem perda de generalidade, suponhamos que $p \mid a_i$, $\forall i \in \{1, ..., r\}$. Assim, $g_1(x) = p \cdot g_2(x)$ onde $g_2(x) \in \mathbb{Z}[x]$, e se $m = p \cdot m_1$ temos

$$p \cdot m_1 f(x) = p \cdot g_2(x) \cdot h_1(x)$$
$$\Downarrow$$
$$m_1 f(x) = g_2(x) \cdot h_1(x).$$

Como o número de fatores primo de m é finito, prosseguindo no argumento acima (ou por indução sobre o número de fatores primos de m) chegamos que:

$$f(x) = g'(x) \cdot h'(x)$$

onde,

$$g'(x) \cdot h'(x) \in \mathbb{Z}[x]$$

e $g(x)$ e $h(x)$ são múltiplos racionais de $g(x)$ e $h(x)$, respectivamente, contradizendo a irredutibilidade de $f(x)$ sobre $\mathbb{Z}$.

□

Teorema 2.6.1. *(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:*

(i) $p \nmid a_n$;

(ii) $p \mid a_0, a_1, a_{n-1}$;

(iii) $p^2 \nmid a_0$.

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

Demonstração: Pela Proposição anterior é suficiente provar que $f(x)$ é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que,

$$f(x) = g(x) \cdot h(x), g(x), h(x) \in \mathbb{Z}[x]$$

e

$$1 \leq \partial g(x), \partial h(x) < \partial f(x) = n.$$

Sejam,

$$g(x) = b_0 + b_1 x + ... + b_r x^r \in \mathbb{Z}[x],\ \partial g(x) = r \text{ e}$$

$$h(x) = c_0 + c_1 x + ... + c_s x^s \in \mathbb{Z}[x],\ \partial h(x) = s.$$

Assim $n = r + s$.

Agora $b_0 \cdot c_0 = a_0$ e assim $p \mid b_0$ ou $p \mid c_0$ e como $p^2 \nmid a_0$ segue que p divide apenas um dos inteiros b_0, c_0. Vamos admitir, sem perda de generalidade, que $p \mid b_0$ e $p \nmid c_0$. Agora $a_n = b_r \cdot c_s$ é o coeficiente de $x^n = x^{r+s}$ e portanto $p \nmid b_r$ e $p \mid b_0$. Seja b_i o primeiro coeficiente de $g(x)$ tal que $p \nmid b_i$.

Agora $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + ... + b_i \cdot c_0$ e portanto como $p \mid b_0, ..., b_{i-1}, p \nmid b_i$ e $p \nmid c_0 \Rightarrow p \nmid a_i \Rightarrow i = n$ o que é um absurdo pois $1 \leq i \leq r < n$.

□

3 Extensão algébrica dos racionais

O objetivo deste capítulo é construir corpos K, tais que $\mathbb{Q} \subset K \subset \mathbb{C}$. Para isso vamos usar o processo chamado adjunção de raízes de um polinômio. Ademais, vamos apresentar alguns resultados que são muito importantes no desenvolvimento da Teoria de Galois.

3.1 Adjunção de raízes

Definição 3.1.1. *Um corpo L é dito uma extensão de um corpo K, se K for subcorpo de L e denotamos por $L \supset K$.*

Exemplo 3.1.1. *O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$, por sua vez $\mathbb{C}$ é extensão de $\mathbb{R}$ e de $\mathbb{Q}$.*

Definição 3.1.2. *Sejam L uma extensão de K e $\alpha \in L$. Dizemos que α é algébrico sobre K se existe $f(x) \in K[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso o contrário dizemos que α é transcendente sobre K.*

Definição 3.1.3. *Sejam L uma extensão de K. Dizemos que L é uma extensão algébrica de K se todo $\alpha \in L$ é algébrico sobre K:*

Exemplo 3.1.2. *O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$. Desde que $\sqrt{2}$ é uma raiz do polinômio $f(x) = x^2 - 2$, temos que $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$. Note que $i \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$ pois é raíz de $p(x) = x^2 + 1$.*

Exemplo 3.1.3. *O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$. O número real π é transcendente sobre $\mathbb{Q}$, uma vez que, π não é raíz de nenhum polinômio em $\mathbb{Q}[x]$. Por outro lado, π é algébrico em $\mathbb{R}$ pois é raiz do polinômio $f(x) = x - \pi \in \mathbb{R}[x]$.*

Proposição 3.1.1. *Se $\alpha \in K$, então α é algébrico sobre K.*

Demonstração: Basta tomar $f(x) = x - \alpha \in K[x]$ e temos que $f(\alpha) = \alpha - \alpha = 0$. Logo α é algébrico sobre K.

□

Observação 3.1.1. *Se $\alpha \in L \supset K$ definimos $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$. Ademais, $K[\alpha]$ é um subdomínio de L que contém K.*

Seja $\alpha \in L$ algébrico sobre K e seja $p(x) \in K[x]$, mônico e de menor grau tal que $p(\alpha) = 0$. Pela minimalidade do grau de $p(x)$ segue que $p(x)$ é o único polinômio mônico irredutível em $K[x]$ tal que $p(\alpha) = 0$, o qual será denotado aqui por $p(x) = irr(\alpha, K)$.

De fato, seja $p(x) \in K[x]$, pelo algorítimo da divisão existem $g(x), r(x) \in K[x]$, tais que,

$$p(x) = f(x)g(x) + r(x),$$

com $r(x) = 0$ ou $\partial r(x) \leq \partial g(x)$, como α é raiz de $p(x)$ temos,

$$\begin{aligned} 0 = p(\alpha) &= f(\alpha)g(\alpha) + r(\alpha) \\ \Rightarrow r(\alpha) &= p(\alpha) - f(\alpha)g(\alpha) \\ \Rightarrow r(\alpha) &= 0. \end{aligned}$$

Mas $p(x)$ é o menor polinômio tal que aplicando α resulta em 0, assim, $r(x) = 0$, daí,

$$p(x) = f(x)g(x).$$

Como $p(x)$ é mônico, isto significa que o coeficiente do termo de maior grau é 1, logo $f(x) = 1$ ou $g(x) = 1$, constante. E portanto $p(x)$ é irredutível em $K[x]$. E $p(x)$ é único, pois suponha que exista $q(x) \in K[x]$ tal que,

$$q(\alpha) = 0,$$

note que,

$$q(\alpha) = 0 = p(\alpha), \text{ então } q(\alpha) = p(\alpha),$$

como $q(x)$ e $p(x)$ são mônicos e de menor grau, segue que,

$$q(x) = p(x).$$

□

Exemplo 3.1.4. *Sejam* $\mathbb{R} \supset \mathbb{Q}$ *e* $\alpha = \sqrt{2} \in \mathbb{R}$ *vamos mostrar que*

$$\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}.$$

De fato, por definição temos que,

$$Q[\sqrt{2}] = \left\{f(\sqrt{2}) : f(x) \in \mathbb{Q}[x]\right\}.$$

Agora, se $f(x) \in \mathbb{Q}[x]$*, segue pelo algoritmo da divisão que existem* $q(x)$ *e* $r(x) \in \mathbb{Q}[x]$ *tais que,*

$$f(x) = q(x)(x^2 - 2) + r(x), \text{ onde } r(x) = a + bx.$$

Para $x = \sqrt{2}$ *temos que,*

$$\begin{aligned} f(\sqrt{2}) &= q(\sqrt{2})(2-2) + r(\sqrt{2}), \\ f(\sqrt{2}) &= q(\sqrt{2})0 + r(\sqrt{2}), \\ f(\sqrt{2}) &= 0 + r(\sqrt{2}), \\ f(\sqrt{2}) &= r(\sqrt{2}). \end{aligned}$$

Como $r(x)$ *é da forma,* $r(x) = a + bx$*, temos*

$$f(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2},$$

com $a, b \in \mathbb{Q}$*, Logo,* $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$.

Exemplo 3.1.5. *Sejam* $\mathbb{R} \supset \mathbb{Q}$ *e* $\alpha = \sqrt[3]{2} \in \mathbb{R}$*. vamos mostrar que*

$$K[\alpha] = Q[\sqrt[3]{2}] = \left\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\right\}.$$

Por definição,

$$\mathbb{Q}[\sqrt[3]{2}] = \left\{f(\sqrt[3]{2}) : f(x) \in \mathbb{Q}[x]\right\}.$$

Pelo algoritmo da divisão temos que existem $q(x)$ *e* $r(x) \in \mathbb{Q}[x]$ *tais que,*

$$f(x) = q(x)(x^3 - 2) + r(x), r(x) = a + bx + cx^2$$

para $x = \sqrt[3]{2}$*, temos:*

$$f(\sqrt[3]{2}) = r(\sqrt[3]{2});$$

como $r(x)$ *é da forma* $r(x) = a + bx + cx^2$*, temos*

$$f(\sqrt[3]{2}) = r(\sqrt[3]{2}) = a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2,$$

com $a, b, c \in \mathbb{Q}$.

Observação 3.1.2. *De modo geral, seja* $\alpha = \sqrt[n]{p} \in \mathbb{R}$, n *inteiro maior ou igual a* 2 *e* p *maior ou igual a* 2 *um número primo. Então* α *é uma raiz real do polinômio* $x^n - p$ *que é, pelo critério de Eisenstein, irredutível sobre* $\mathbb{Q}$. *Assim* $x^n - p = irr(\alpha, \mathbb{Q})$ *e temos,* $\mathbb{Q}[\alpha]$ *é um subcorpo de* $\mathbb{R}$ *contendo* $\mathbb{Q}$ *e mais ainda,*

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

Teorema 3.1.1. *Se* $\alpha \in L \supset K$ *e se* $\Psi : K[x] \to L$ *é definida por* $\Psi(f(x)) = f(\alpha)$, *então* Ψ *é um homomorfismo de corpos tal que:*

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

(ii) α *é transcendente sobre* K *se, e somente se,* $ker(\Psi) = 0$;

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

(iv) $K[x]/ker(\Psi) \simeq K[\alpha]$.

Demonstração: Primeiro mostraremos que Ψ é um homomorfismo, para isso, considere $f(x), g(x) \in K[x]$. Logo:

$$\Psi(f(x) + g(x)) = \Psi((f+g)(x)) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \Psi(f(x)) + \Psi(g(x)),$$

$$\Psi(f(x) \cdot g(x)) = \Psi((f \cdot g)(x)) = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha) = \Psi(f(x)) \cdot \Psi(g(x)).$$

Portanto Ψ é homomorfismo.

Agora mostraremos os itens de (i) à (iv).

(i) Temos que

$$Im\Psi = \{f(\alpha) : f(\alpha) = \Psi(f(x))\}$$

mas Ψ está definida em $K[x]$, de modo que todo $f(x) \in K[x]$. Daí,

$$Im\Psi = \{f(\alpha) : f(x) \in K[x]\},$$

e por definição, isto é $K[\alpha]$. Logo, $Im\Psi = K[\alpha]$. Para vericar que $K[\alpha]$ contém K basta tomar a função $g(\alpha) = a_i, a_i \in K, i = 1, 2, \ldots$.

(ii) Seja

$$ker(\Psi) = \{f(x) \in K[x] : \Psi(f(x)) = 0\}.$$

Como α é transcendente sobre K, seja $f(x) \in K[x] - \{0\}$ com $f(\alpha) \neq 0$. Mas $\Psi(f(x)) = f(\alpha) \Rightarrow \Psi(f(x)) \neq 0$. Portanto, somente o polinômio nulo anula α. Logo $Ker(\Psi) = 0$. Reciprocamente, suponha $Ker(\Psi) = 0$ (onde 0 é o polinômio nulo), vem que, para todo $f(x) \neq 0 \in K[x]$ têm-se,

$$\Psi(f(x)) \neq 0.$$

Como $\Psi(f(x)) = f(\alpha)$, temos que,

$$0 \neq \Psi(f(x)) = f(\alpha).$$

Deste modo, α é transcendente sobre K.

(iii) Como α é algébrico sobre K ,então $ker(\Psi) \neq \{0\}$. Considere então $ker(\Psi) = K[x] \cdot p(x)$ um ideal em $K[x]$. Como $p(x)$ é irredutível sobre K, pelo Teorema 2.4.1 temos que $ker(\Psi) = K[x] \cdot p(x)$ é um ideal maximal em $K[x]$.

(iv) Segue pelo item (i) deste Teorema que $Im\Psi = K[\alpha]$ e agora é imediato do Teorema 1.2.1 item (iii) que

$$K[x]/ker(\Psi) \simeq K[\alpha].$$

□

Corolário 3.1.1. *Sejam L uma extensão de K e $\alpha \in L$. Então:*

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

(ii) 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: (i) Tomemos um homomorfismo nas condições do Teorema 3.1.1, ou seja, $\Psi : K[x] \to L$ definido por $\Psi(f(x)) = f(\alpha)$. Suponha que é algébrico sobre K e seja $p(x) = irr(\alpha, K) \in K[x]$. Pelo item (iii) do Teorema 3.1.1 temos que $ker(\Psi) = K[x] \cdot p(x)$ é um ideal maximal e portanto,

$$\frac{K[x]}{ker(\Psi)},$$

é um corpo. Agora pelo item (iv) do Teorema 3.1.1 temos

$$\frac{K[x]}{ker(\Psi)} \simeq K[\alpha],$$

donde segue que $K[\alpha]$ também é um corpo.
(ii) Para provar que $K[\alpha]$ é um subdomínio de L precisamos mostrar que $K[\alpha]$ é subanel e que não possui divisores de zero.

Vamos primeiro mostrar que $K[\alpha]$ é subanel, para isto, considere $f(\alpha), g(\alpha) \in K[\alpha]$.
Note que,
1)$f(\alpha)g(\alpha) = (fg)(\alpha) \in K[\alpha]$.
2)$f(\alpha) \cdot g(\alpha) = (f \cdot g)(\alpha) \in K[\alpha]$.

Agora, observe que $K[\alpha]$ não possui divisores de zero, pois

$$f(\alpha) \cdot g(\alpha) = 0 \Rightarrow f(\alpha) = 0 \ \ ou \ \ g(\alpha) = 0,$$

como α é transcendente sobre $K[\alpha]$, vem que

$$f(\alpha) = 0(\alpha) \ \ ou \ \ g(\alpha) = 0(\alpha).$$

□

Corolário 3.1.2. *Se L é uma extensão de K e se α, $\beta \in L$ são raízes de um mesmo polinômio irredutível sobre K, então $K[\alpha]$ e $K[\beta]$ são corpos isomorfos.*

Demonstração: Por hipótese, $p(x) = irr(\alpha, K) = irr(\beta, K)$. Agora, pelo item (iii) do Teorema 3.1.1, obtemos

$$J = K[x] \cdot p(x),$$

e por (iv) temos $K[\alpha] \simeq \frac{K[x]}{J}$ e da mesma forma $\frac{K[x]}{J} \simeq K[\beta]$. Logo

$$K[\alpha] \simeq K[\beta].$$

□

Proposição 3.1.2. *Seja L uma extensão de K e $\alpha \in L$ algébrico sobre K. Se o grau do polinômio $irr(\alpha, K)$ é n, então:*

(i) Qualquer $f(x) \in K[x], f(\alpha)$ *pode ser expresso de modo único na forma,* $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$*, onde* $a_i \in K$*.*

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

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

Demonstração: Seja $p(x) = irr(\alpha, K)$. Por hipótese, $\partial p(x) = n$.
(i) Se $f(x) \in K[x]$ então pelo algorítimo da divisão existem $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x) \cdot p(x) + r(x), \quad onde \quad r(x) = 0 \quad ou \quad \partial r(x) < \partial p(x).$$

Assim $r(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ onde $a_i \in K, i = 0, 1, ..., n-1$.
Agora temos,

$$f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha),$$

e como $p(\alpha) = 0$ segue que $f(\alpha) = r(\alpha)$ ou seja, $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$.

Para demonstrar a unicidade da expressão temos que:
se $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}, a_i, b_i \in K, \forall i \in 1, ..., n-1$.

Então segue que o polinômio $q(x) \in K[x]$, onde

$$q(x) = (a_0 - b_0) + (a_1 - b_1)x + ... + (a_{n-1} - b_{n-1})x^{n-1}$$

é tal que $q(\alpha) = 0$ e $\partial q(x) < n = \partial irr(\alpha, K)$. Assim $q(x) = 0$ e daí segue

$$a_i = b_i, \forall i \in 1, ..., n-1.$$

(ii) Primeiro vamos mostrar que $K[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in K\}$. Por definição $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$, agora pelo item (i) desta proposição $f(\alpha)$ pode ser expresso de modo único na forma $f(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$, onde $a_i \in K$, daí temos

$$K[\alpha] = \{f(\alpha) : f(x) \in K[x]\} = \left\{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in K\right\}.$$

O fato de $K[\alpha]$ ser um subcorpo de L que contém K segue diretamente do item (i) do Corolário 3.1.1.
(iii) Para demonstrar este item basta observar que pelos itens anteriores temos:

$$\mathbb{Z}_p[\alpha] = \left\{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Z}_p\right\}.$$

Assim existe uma correspondência bijetiva entre $\mathbb{Z}_p[\alpha]$ e o conjunto de todas as n-uplas $(a_0, a_1, ..., a_{n-1})$ onde cada $a_i \in \mathbb{Z}_p = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$.

□

Exemplo 3.1.6. *Considerando a Observação 3.1.2 por exemplo,*

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] = \left\{a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q}\right\} \subset \mathbb{R},$$

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] = \left\{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 : a_0, a_1, a_2 \in \mathbb{Q}\right\} \subset \mathbb{R},$$

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{3}] = \left\{a_0 + a_1\sqrt[4]{3} + a_2(\sqrt[4]{3})^2 + a_3(\sqrt[4]{3})^3 : a_0, a_1, a_2, a_3 \in \mathbb{Q}\right\} \subset \mathbb{R},$$

são extensões do corpo $\mathbb{Q}$.

Agora se β é uma raiz cúbica complexa de 2 e $\beta \neq \mathbb{R}$, temos que,

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}, \mathbb{Q} \subset \mathbb{Q}[\beta] \subset \mathbb{C}$$

Mais ainda, pelo Corolário 3.1.2, $\mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\beta]$ pois $\sqrt[3]{2} \in \mathbb{R}$ e $\beta \in \mathbb{C}$ são raízes do mesmo polinômio irredutível $x^3 - 2$ sobre $\mathbb{Q}$.

3.2 Corpo de decomposição de um polinômio

Considere K um subcorpo de $\mathbb{C}$. Como $\mathbb{C}$ é um corpo algebricamente fechado, ou seja, para qualquer$f(x) \in \mathbb{C}[x]$ existe $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$. Assim, se $f(x) \in K[x]$ 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,

$$f(x) = c \cdot (x - \alpha_1)^{m_1}...(x - \alpha_r)^{m_r}$$

em $\mathbb{C}[x]$ onde $c \in K$ e r, $m_1, ..., m_r$ são inteiros positivos.

O inteiro m_i chama-se multiplicidade da raiz α_i. Se $m_i = 1$ dizemos que α_i é uma raiz simples de $f(x)$. Se $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$ definimos $f'(x) = a_1 + 2a_2x + ... + na_nx^{n-1} \in K[x]$ o qual chamamos de derivada de $f(x)$. Observe que se $\partial f(x) = n \geq 1$ então $f'(x) \neq 0$ e $\partial f'(x) = n - 1$.

Se $f(x), g(x) \in K[x]$ e $a \in K$ segue as seguintes regras:

$$(f(x) + g(x))' = f'(x) + g'(x),$$

$$(a \cdot f(x))' = a \cdot f'(x),$$

$$(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x).$$

Proposição 3.2.1. *Sejam $f(x) \in K[x], \partial f(x) = n \geq 1$ e $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$. Então:*

(i) α é raiz simples de $f(x)$ se, somente se, $f(\alpha) = 0$ e $f'(\alpha) \neq 0$.

(ii) Se $f(x)$ é irredutível sobre K então todas as raízes de $f(x)$ são simples.

Demonstração: (i) Se $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$, com multiplicidade $m \geq 1$ temos que $f(x)$ pode ser fatorado em $\mathbb{C}[x]$ como, $f(x) = (x-\alpha)^m \cdot g(x)$, onde $g(x) \in \mathbb{C}[x]$ e $g(\alpha) \neq 0$. Sendo assim:

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

Para $m = 1$, temos que

$$f(x) = (x-\alpha)g(x) \Rightarrow f(\alpha) = (\alpha-\alpha)g(\alpha) \Rightarrow f(\alpha) = 0 \cdot g(\alpha) = 0.$$

$$f'(x) = g(x) + (x-\alpha)g'(x).$$

$$\Downarrow$$

$$f'(\alpha) = g(\alpha) + (\alpha-\alpha)g'(\alpha) = g(\alpha) \neq 0.$$

Reciprocamente, sendo $f(x) = (x-\alpha)^m \cdot g(x)$ e $f'(x) = m(x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m g'(x)$. Observe que $f'(\alpha) = 0 \Leftrightarrow m \geq 2$, logo

$$f'(x) = m(x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m g'(x)$$
$$\Rightarrow f'(\alpha) = m \cdot 0 \cdot g(x) + (\alpha-\alpha)^m g'(\alpha) = 0$$

Mas por hipótese $f'(\alpha) \neq 0$. Logo, $m = 1$. Donde α é raiz simples.
(ii) Se $f(x) \in K[x]$ é um polinômio irredutível em K e $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$, de multiplicidade m, queremos provar que $m = 1$. Seja $p(x) = irr(\alpha, K)$, então pelo algoritmo da divisão existem polinômios $q(x), r(x) \in K[x]$ tais que, $f(x) = q(x) \cdot p(x) + r(x)$ com $r(x) = 0$ ou $\partial r(x) < \partial p(x)$. Como α é uma raiz de $f(x)$ vem que,

$$0 = f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha)$$

e assim,

$$r(\alpha) = f(\alpha) - q(\alpha) \cdot p(\alpha) = 0 \Rightarrow r(\alpha) = 0.$$

Como $p(x)$ é o polinômio de menor grau que aplicando α resulta em zero, temos que $r(x) = 0$. Daí,

$$f(x) = q(x) \cdot p(x).$$

Mas, $f(x)$ é irredutível, assim, $q(x) = a \in K$ e

$$f(x) = a \cdot p(x).$$

Se $m > 1$ pelo $item(i)$ desta Proposição têm-se,

$$f'(\alpha) = a \cdot p'(\alpha) = 0 \Rightarrow p'(\alpha) = 0$$

Mas isso contradiz a minimalidade do grau de $p(x)$, já que

$$\partial p'(x) < \partial p(x).$$

Assim, $m = 1$ e por definição α é raiz simples de $f(x)$.

□

Definição 3.2.1. *Chamamos* ***corpo de decomposição*** *de um polinômio $f(x) \in K[x]$ sobre K, que denotaremos por $L = Gal(f, K)$ ao menor subcorpo de $\mathbb{C}$ que contém K e todas as raízes de $f(x)$ em $\mathbb{C}$.*

Observe que tal menor subcorpo existe e é igual a interseção de todos os subcorpos de $\mathbb{C}$ contendo K e todas as raízes de $f(x)$ em $\mathbb{C}$. Sejam $f(x) \in K[x]$ e $\alpha_1, ..., \alpha_r$ as distintas raízes de $f(x)$ em $\mathbb{C}$. Vejamos como definir de um modo construtivo o $Gal(f, K)$.

Consideremos,

$$K_0 = K \subset K_1 = K[\alpha_1] \subset K_2 = K_1[\alpha_2] \subset ... \subset K_r = K_{r-1}[\alpha_r].$$

K_r é o menor subcorpo de $\mathbb{C}$ contendo K e $\alpha_1, ..., \alpha_r$ e portanto $K_r = Gal(f, K)$. Denotando $K_r = K[\alpha_1, ..., \alpha_r]$ temos $Gal(f, K) = K[\alpha_1, ..., \alpha_r]$. É imediato que qualquer que seja a ordem em que pegamos as raízes $\alpha_1, ..., \alpha_r$ ainda assim esse processo nos levaria ao $Gal(f, K)$. A esse processo chamamos de **adjunção de raízes**.

Exemplo 3.2.1. *Vamos construir o corpo de decomposição de $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Primeiramente note que $\alpha = \sqrt[3]{2} \in \mathbb{R}$ é raíz de $f(x)$, pois*

$$f(\sqrt[3]{2}) = (\sqrt[3]{2})^3 - 2 = 2 - 2 = 0.$$

Agora observe que

$$\beta = \sqrt[3]{2} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i \right) \in \mathbb{C}$$

é raiz complexa de $f(x)$, onde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ é uma raiz cúbica complexa da unidade. De fato,

$$\beta = -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2} i$$

daí,

$$f\left(-\tfrac{\sqrt[3]{2}}{2} + \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right) = \left(-\tfrac{\sqrt[3]{2}}{2} + \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right)^3 - 2$$

$$= \left(-\tfrac{\sqrt[3]{2}}{2} + \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right)\left(-\tfrac{\sqrt[3]{2}}{2} + \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right)^2 - 2$$

$$= \left(-\tfrac{\sqrt[3]{2}}{2} + \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right)\left(\tfrac{(\sqrt[3]{2})^2}{4} + 2\left(-\tfrac{\sqrt[3]{2}}{2} \cdot \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right) + \left(-\tfrac{(\sqrt[3]{2})^2(\sqrt{3})^2}{4}\right)\right) - 2$$

$$= \left(-\tfrac{\sqrt[3]{2}}{2} + \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right)\left(\tfrac{\sqrt[3]{4}}{4} - \tfrac{\sqrt[3]{4}\cdot 3}{4} - \tfrac{\sqrt[3]{4}\cdot\sqrt{3}i}{2}\right) - 2$$

$$= \left(-\tfrac{\sqrt[3]{2}}{2} + \tfrac{\sqrt[3]{2}\cdot\sqrt{3}}{2} i\right)\left(-\tfrac{\sqrt[3]{4}}{2} - \tfrac{\sqrt[3]{4}\sqrt{3}i}{2}\right) - 2$$

$$= \left(\tfrac{\sqrt[3]{8}}{4} + \tfrac{\sqrt[3]{8}\cdot\sqrt{3}i}{4} - \tfrac{\sqrt[3]{8}\cdot\sqrt{3}i}{4} - \tfrac{\sqrt[3]{8}\cdot 3i^2}{4} - 2\right)$$

$$= \left(\tfrac{\sqrt[3]{8}}{4} - \tfrac{\sqrt[3]{8}\cdot 3i^2}{4} - 2\right)$$

$$= \left(\tfrac{1}{2} + \tfrac{6}{4} - 2\right)$$

$$= \frac{2 + 6 - 8}{4} = 0.$$

E mais $\overline{\beta} = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)$ é raiz de f.

Logo, as três raízes distintas de $f(x) = x^3 - 2$ *em* $\mathbb{C}$ *são* $\alpha = \sqrt[3]{2},\ \beta = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)$ *e* $\overline{\beta} = \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)$. *Então*

$$Gal(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta, \overline{\beta}] = \mathbb{Q}[\alpha, \beta].$$

Exemplo 3.2.2. *Consideremos o polinômio* $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. *As suas quatro raízes em* $\mathbb{C}$ *são*

$$\theta_1 = \sqrt[4]{2}, \quad \theta_2 = \sqrt[4]{2}i, \quad \theta_3 = -\sqrt[4]{2}, \quad \theta_4 = -\sqrt[4]{2}i,$$

e $Q(\sqrt[4]{2}, i)$ *é o seu corpo de decomposição.*

Definição 3.2.2. *Seja* K *um corpo. Um automorfismo de* K *é um isomorfismo* $f : K \to K$. *O conjunto dos automorfismos de* K *será denotado por* $AutK$.

Proposição 3.2.2. *Seja* $L \supset K$ *é uma extensão de* K, *onde* K *é um subconjunto de* $\mathbb{C}$. *Considere o seguinte conjunto:*

$$Aut_K L = \{\sigma \in AutL : \sigma(a) = a, \forall a \in K\}.$$

Seja $f(x) \in K[x]$ *e* $\alpha \in L$ *uma raiz de* $f(x)$ *em* L, *então* $\sigma(\alpha)$ *é também uma raiz de* $f(x)$ *em* L, $\forall \sigma \in Aut_K L$.

Demonstração: Seja $\alpha \in L$ é uma raiz de $f(x)$, tem-se que $f(\alpha) = 0$. Note que,

$$\sigma(\alpha) = \alpha, \quad pois \quad \sigma(\alpha) \in AutL$$

e mais ainda,

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

Isto nos diz que $\sigma(\alpha)$ é uma raiz de $f(x) \in K[x]$.

□

3.3 Grau de uma extensão

Sendo L uma extensão de K, considere a adição em L e o produto por escalar

$$\begin{aligned} + : L \times L &\to L \\ (\alpha, \beta) &\mapsto \alpha + \beta \end{aligned}$$

e

$$\cdot : K \times L \to L$$
$$(\alpha, x) \mapsto \alpha x.$$

Temos que L munido dessa adição e desse produto por escalar é um K-espaço vetorial. A dimensão de L visto como K-espaço vetorial é chamada de grau da extensão L sobre K e denotamos por $[L : K]$.

Uma extensão L de K é dita extensão finita se tem grau finito. Caso contrário, dizemos $L \supset K$ é extensão infinita.

Exemplo 3.3.1. *O corpo $\mathbb{C}$ visto como espaço vetorial sobre $\mathbb{R}$ tem dimensão 2, pois $\{1, i\}$ é base desse espaço vetorial. Assim, $\mathbb{C}$ é uma extensão de grau 2 sobre $\mathbb{R}$, ou seja, $[\mathbb{C} : \mathbb{R}] = 2$.*

Proposição 3.3.1. *Seja K um corpo e $L \supset K$ uma extensão de K. Então:*

(a) Se $L \supset K$ é finita, então $L \supset K$ é algébrica;

(b) Se $\alpha \in L \supset K$ é um elemento algébrico sobre K e o grau de $irr(\alpha, K)$ 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 $\alpha \in L \supset K$ é um elemento transcendente sobre K, então $K[\alpha] \supset K$ é uma extensão infinita.

Exemplo 3.3.2. *$\mathbb{R}$ é uma extensão de $\mathbb{Q}$ de grau infinito.(π é transcendente).*

Demonstração: (a) Suponha $[L : K] = m < \infty$ e $\alpha \in L \supset K$, como $K[\alpha]$ um subespaço de L segue que $[K[\alpha] : K] \leq m < \infty$. Se $[K[\alpha] : K] = n$ então o conjunto $\{1, \alpha, ..., \alpha^n\}$ é L.D., pois n é o número máximo de elementos L.I., e portanto existem escalares $a_0, a_1, ..., a_n \in K$ não nulos tais que

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0,$$

e isso signica que α é algébrico sobre K, pois anula o polinômio $p(x) = a_0+a_1x+...+a_nx^n \in K[x]$.
(b) Seja $\alpha \in L \supset K$ um elemento algébrico sobre K tal que grau de $irr(\alpha, K) = n$. Mas pela Proposição 3.1.2, todo elemento de $K[\alpha]$ pode ser escrito de modo único como combinação linear sobre K de $1, \alpha, ..., \alpha^{n-1}$. Assim, $\{1, \alpha, ..., \alpha^{n-1}\}$ é uma base de $K[\alpha]$ sobre K. Logo, $[K[\alpha] : K] = n$.
(c) Segue de imediato do item (a)

□

Vejamos um corolário que decorre desta proposição.

Corolário 3.3.1. *Seja $\alpha \in L \supset K$. Então, as seguintes afirmações são equivalentes:*

(i) *α é algébrico sobre K;*

(ii) *$[K[\alpha] : K] < \infty$;*

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

Demonstração: $(i) \Rightarrow (ii)$ Note que se $\alpha \in L \supset K$ é algébrico sobre K, então existe $p(x) \in K[x]$ tal que $p(\alpha) = 0$. Seja $f(x) = irr(\alpha, K)$, com $\partial f(x) = n$, pela minimalidade do grau de $f(x)$ e por resultado da Proposição 3.3.1, item (b) 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 3.3.1, 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.

□

Proposição 3.3.2. *Sejam $M \supset L \supset K$ corpos tais que $[M : L]$ e $[L : K]$ são finitos então $[M : K]$ é finito e $[M : K] = [M : L] \cdot [L : K]$.*

Demonstração: Suponha M sobre K finita. Temos que L é um subespaço do K-espaço vetorial M. Logo, $[L : K]$ é finita. Considere β uma base de M sobre K. Temos que β é finita e que β gera M também como L-espaço vetorial. Logo, $[M : L]$ é finita. Suponha agora $[M : L]$ e $[L : K]$ finitas. Sendo $[M : L] = m$ e $[L : K] = n$, $\alpha = \{\alpha_1, ..., \alpha_m\}$ é base de M sobre L e $\gamma = \{\beta_1, ..., \beta_n\}$ é base de L sobre K. Tomemos

$$\delta = \{\beta_i \alpha_j : i = 1, ..., n; j = 1, ..., m\}.$$

Note que δ é base de M sobre K. De fato, suponha $x \in M$, então

$$x = a_1\alpha_1 + ... + a_m\alpha_m, \text{ com } a_j \in L,$$

como γ é base de L sobre K, temos $\alpha j = \lambda_{ij}\beta_1 + ... + \lambda_{nj}\beta_n$ com $\lambda_{ij} \in K$ para $i = 1, ..., n$ e $j = 1, ..., m$. Logo, x é combinação linear dos elementos de δ com coeficientes em K. Assim, δ gera o K-espaço vetorial M. Suponha agora, $\lambda_{ij} \in K, i = 1, ..., n$ e $j = 1, ..., m$ tais que

$$\sum_{j=1}^{m}\sum_{i=1}^{n}\lambda_{ij}\beta_i\alpha_j = 0.$$

Temos que

$$(\lambda_{11}\beta_1 + ... + \lambda_{n1}\beta_n)\alpha_1 + ... + (\lambda_{1m}\beta_1 + ... + \lambda_{nm}\beta_n)\alpha_m = 0,$$

como α é L.I sobre L, devemos ter $(\lambda_{1j}\beta_1 + ... + \lambda_{nj}\beta_n) = 0$ para todo $j = 1, ..., m$. Como γ é L.I sobre K, devemos ter $\lambda_{ij} = 0$. Assim,

$$[M : K] = m \cdot n = [M : L][L : K].$$

□

Corolário 3.3.2. *(a) Se* $\overline{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C} : \alpha$ *algébrico sobre* $\mathbb{Q}\}$ *então* $\overline{\mathbb{Q}}$ *é subcorpo de* $\mathbb{C}$ *e é uma extensão algébrica infinita de* $\mathbb{Q}$*;*
(b) Se $\overline{\mathbb{Q}}_{\mathbb{R}} = \{\alpha \in \mathbb{R} : \alpha$ *algébrico sobre* $\mathbb{Q}\}$ *então é um subcorpo de* $\mathbb{R}$ *e é uma extensão algébrica infinita de* $\mathbb{Q}$*.*

Demonstração: (a) Por definição $\overline{\mathbb{Q}}$ é um subconjunto de $\mathbb{C}$ e contém $\mathbb{Q}$. Mostremos que $\overline{\mathbb{Q}}_{\mathbb{C}}$ é um subcorpo de $\mathbb{C}$. Para isso é suficiente provarmos as seguintes três propriedades:

(i) $\alpha, \beta \in \overline{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha - \beta \in \overline{\mathbb{Q}}_{\mathbb{C}}$;

(ii) $\alpha, \beta \in \overline{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \alpha \cdot \beta \in \overline{\mathbb{Q}}_{\mathbb{C}}$;

(iii) $0 \neq \alpha \in \overline{\mathbb{Q}}_{\mathbb{C}} \Rightarrow \frac{1}{\alpha} \in \overline{\mathbb{Q}}_{\mathbb{C}}$.

Vamos demonstrar simultaneamente (i), (ii), e (iii). De fato, seja $K = \mathbb{Q}[\alpha]$ e $L = K[\beta]$. Como α é algébrico sobre $\mathbb{Q}$ segue pelo Corolário 3.3.1 que $[K : \mathbb{Q}] < \infty$. Agora sendo β algébrico sobre $\mathbb{Q}$, β também é algébrico sobre K e daí pelo mesmo Corolário segue que $[L : K] < \infty$. Pela Proposição 3.3.2, temos que

$$[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}],$$

segue que $[L : \mathbb{Q}] < \infty$ e pela Proposição 3.3.1 temos que $L \supset \mathbb{Q}$ é uma extensão algébrica. Agora o resultado segue $\alpha \pm \beta \in L$, $\alpha \cdot \beta \in L$ e $\frac{1}{\alpha} \in L$ se $\alpha \neq 0$. Logo $\overline{\mathbb{Q}}_{\mathbb{C}}$ é uma extensão algébrica sobre $\mathbb{Q}$. Agora se $\alpha_i = \sqrt[2^i]{2}$ e $K_0 = \mathbb{Q}, K_1 = \mathbb{Q}[\alpha_1], ..., K_i = K_{i-1}[\alpha_i]$ temos que $M = \bigcup_{i=0}^{\infty} K_i$ é uma extensão algébrica infinita de $\mathbb{Q}$ e $M \subset \overline{\mathbb{Q}}_{\mathbb{R}} \subset \overline{\mathbb{Q}}_{\mathbb{C}}$.
(b) Basta observar que $\overline{\mathbb{Q}}_{\mathbb{R}} = \overline{\mathbb{Q}}_{\mathbb{C}} \bigcap \mathbb{R}$. De fato $\overline{\mathbb{Q}}_{\mathbb{R}} = \{\alpha \in \mathbb{R} : \alpha$ algébrico sobre $\mathbb{Q}\}$ temos $\beta \in \overline{\mathbb{Q}}_{\mathbb{C}} \bigcap \mathbb{R} \Rightarrow \beta \in \overline{\mathbb{Q}}_{\mathbb{C}} = \{\beta \in \mathbb{C} : \beta$ é algébrico sobre $\mathbb{Q}\}$ e $\beta \in \mathbb{R}$ implica que $\beta \in \mathbb{R}$ e β

é algébrico sobre $\mathbb{Q}$, assim, $\beta \in \overline{\mathbb{Q}}_{\mathbb{R}}$, ou seja, $\beta \in \mathbb{R}$ e β é algébrico sobre $\mathbb{Q}$. Como $\mathbb{R} \subset \mathbb{C}$, podemos tomar $\beta \in \overline{\mathbb{Q}}_{\mathbb{C}}$ e daí segue $\beta \in \overline{\mathbb{Q}}_{\mathbb{C}} \bigcap \mathbb{R}$ e também $M = \bigcup_{i=0}^{\infty} K_i \subset \overline{\mathbb{Q}}_{\mathbb{R}}$.

□

Corolário 3.3.3. *Seja $K \supset \mathbb{Q}$ tal que $[K : \mathbb{Q}] = m$ e $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ tal que $\partial p(x) = n$. Se $M.D.C.(m, n) = 1$ então $p(x)$ é um polinômio irredutível sobre K.*

Demonstração: Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Considere agora os corpos $\mathbb{Q}[\alpha] \subset K[\alpha]$ e suponhamos que $[K[\alpha] : K] = r$ e $[K[\alpha] : Q[\alpha]] = s$. Como $\partial p(x) = n$ e $p(x)$ é irredutível e $p(x) \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$ segue que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ e $[K[\alpha] : K] = r = n$. De fato, pela Proposição 3.3.2 segue que $n \cdot s = m \cdot r$ e como $M.D.C.(n, m) = 1$ vem que $n \mid r$. Mas $r \leq n$ nos diz que $n = r$ e assim $p(x)$ é também irredutível sobre K.

□

Corolário 3.3.4. *Seja $L = Gal(x^p - 2, \mathbb{Q})$. Então $[L : \mathbb{Q}] = p \cdot (p - 1)$.*

Demonstração: De fato, sabemos que $L = Gal(x^p - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u]$ onde

$$\alpha = \sqrt[p]{2} \in \mathbb{R} \;\; e \;\; u = \left(\cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p} \right) \in \mathbb{C}$$

é uma raiz $p - ésima$ da unidade tal que $1, u, u^2, ..., u^{p-1}$ nos dão todas as distintas raízes $p - ésimas$ da unidade em $\mathbb{C}$ (por isso u diz-se uma raiz primitiva da unidade). Agora pela Proposição 3.3.2,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}].$$

Pelo critério de Eisenstein temos $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$. Agora se $K = \mathbb{Q}[\alpha]$ temos $L = K[u] \supset K \supset Q$. Ainda por Eisenstein temos que u é a raiz de $x^{p-1} + x^{p-2} + ... + x + 1$ que é polinômio irredutível de grau $p-1$ sobre $\mathbb{Q}$. Como $[K : \mathbb{Q}] = p$ e $M.D.C.(p, p-1) = 1$ temos pelo Corolário anterior que $x^{p-1} + x^{p-2} + ... + x + 1$ é ainda irredutível sobre K, tendo u como raiz. Portanto $[K[u] : K] = p - 1$ e isto demonstra o Corolário pois

$$L = K[u] \text{ e } K = \mathbb{Q}[\alpha].$$

□

Teorema 3.3.1. *Seja $L \supset K \supset \mathbb{Q}$ tal que $[L : K] < \infty$. Então, existe $u \in L$ tal que $L = K[u]$.*

Demonstração: A demonstração será por indução sobre o grau $[L : K] < \infty$. Se $[L : K] = 1$ segue que $L = K$ e o teorema é válido trivialmente.

Suponhamos $[L : K] > 1$. Assim, existe $\alpha_1 \in L, \alpha_1 \notin K$. Seja $K_1 = K[\alpha_1]$. Se $K_1 = L$ o teorema está demonstrado. Caso contrário, existe $\alpha_2 \in L, \alpha_2 \notin K_1$.

Seja $K_2 = K_1[\alpha_2] = K[\alpha_1, \alpha_2]$. Como $[L : K] < \infty$ conseguimos $\alpha_1, \alpha_2, ..., \alpha_r, r \geq 2$, elementos de L tais que, $L = K[\alpha_1, \alpha_2, ..., \alpha_r]$ e $\alpha_i \notin K[\alpha_1, \alpha_2, ..., \alpha_{i-1}] = K_{i-1}, K_r = L \supseteq K_{r-1} = K[\alpha_1, \alpha_2, ..., \alpha_{r-1}] \supset ... \supset K_1 = K[\alpha_1] \supset K_0 = K$. Como $[K_{r-1} : K] < \infty$ temos pela hipótese de indução que existe $\alpha \in K_{r-1} = K[\alpha]$ e daí segue imediatamente que $L = K_r = K[\alpha, \alpha_r]$. Chamando $\alpha_r = \beta \in L$ temos $L = K[\alpha, \beta]$. Agora vamos mostrar que existe $u \in L$ tal que $L = K[u]$.

Sejam $p(x) = irr(\alpha, K)$ e $q(x) = irr(\beta, K)$ tais que $\partial p(x) = m$ e $\partial q(x) = n$. Pela Proposição 3.2.1 item (ii) segue que todas as raízes de $p(x)$ (respectivamente $q(x)$) são distintas em $\mathbb{C}$.

Sejam $\alpha_1 = \alpha, \alpha_2, ..., \alpha_m$ as raízes de $p(x)$ em $\mathbb{C}$ e sejam $\beta_1 = \beta, \beta_2, ..., \beta_n$ as raízes de $q(x)$ em $\mathbb{C}$. Vamos definir para $j \neq i$ os seguintes números complexos,

$$j \neq i, \lambda_{ij} = \frac{\alpha_i - \alpha}{\beta - \beta_j} \in \mathbb{C}$$

Como K é um corpo infinito então existe $\lambda \in K$ tal que $\lambda \notin \{\lambda_{ij} : 1 \leq i \leq m, \quad 2 \leq j \leq n\}$.

Agora seja $u = \alpha + \lambda\beta \in L$ e assim $K[u] \subset L$, vamos provar que de fato $L = K[u]$. Para isso vamos provar que $\alpha, \beta \in K[u]$.

Seja $F = K[u]$ e seja $h(x) = p(u - \lambda x) \in F[x]$, observe que

$$h(\beta) = p(u - \lambda\beta) = p(\alpha + \lambda\beta - \lambda\beta) = p(\alpha) = 0.$$

Mas β também é raiz de $q(x) \in K[x] \subset F[x]$. Portanto pelo Teorema 2.3.2 $(x - \beta)$ é um divisor de $d(x) = M.D.C(q(x), h(x))$ em $\mathbb{C}[x]$. Vamos de fato provar que $d(x) = (x - \beta)$, e para isso é suficiente provarmos que se $d(\beta_j) = 0$ então $j = 1$ já que $d(x) \mid q(x)$, e $q(x)$ só possui raízes simples.

Se $d(\beta_j) = 0$ e $j \neq 1$ teremos $h(\beta_j) = 0$, ou seja, $p(u - \lambda\beta_j) = 0$ o que nos diz que existe i, $1 \leq i \leq m$ tal que $\alpha_i - \alpha = \lambda(\beta - \beta_j) \Rightarrow \lambda = \dfrac{\alpha_i - \alpha}{\beta - \beta_j} \Rightarrow \lambda = \lambda_{ij}$ contradizendo a nossa escolha de λ. Portanto $x - \beta = d(x)$.

Agora se $d_1(x) = M.D.C(q(x), h(x))$ em $F[x]$, então temos por $F \subset \mathbb{C}$ que grau de $d_1(x)$ é menor ou igual ao grau $d(x)$. Portanto se $d_1(x) \neq d(x)$ teríamos que $1 = M.D.C(q(x), h(x))$ em $F[x]$ mas então sugeriria que $d(x) = 1$ o que é um absurdo. Logo $d(x) = x - \beta = M.D.C(q(x), h(x))$ em $F[x]$ e isto nos diz que $\beta \in F$. Agora, $\alpha = u - \lambda\beta \in F$ pois $u \in F = K[u], \beta \in F, \lambda \in K \subset F$.

□

Corolário 3.3.5. *Seja $L \supset K \supset \mathbb{Q}$ tal que $[L : K] < \infty$. Então, $[L : K] \geq |Aut_K L|$(onde $|Aut_K L|$ denota o número de elementos do conjunto $Aut_K L = \{f \in AutL; f(\lambda) = \lambda, \forall \lambda \in K\}$).*

Demonstração: Seja $L \supset K \supset \mathbb{Q}$ com $[L : K] < \infty$. Então pelo Teorema 3.3.1 existe, $u \in L$ tal que $L = K[u]$.

Sendo $\alpha \in Aut_K L$ e $p(x) = irr(\alpha, K)$ segue da Proposição 3.2.2 que $u' = \sigma(u)$ é também raiz de $p(x)$, com $u \in L$. Ora $K[u'] \subset L$ e $[K[u'] : K] = [L : K] = \partial p(x)$ nos diz que $L = K[u] = K[u']$. Como $\sigma(a) = a, \forall a \in K, \sigma$ fica completamente determinado pelo valor $u' = \sigma(u)$. Assim o número $|Aut_K L|$ é no máximo igual ao número de raízes u' de $p(x)$ que pertencem a L. Certamente esse número é no máximo o grau do polinômio $p(x) = irr(u, K)$, em que $\partial p(x) = [L : K]$

□

4 Teoria de Galois Elementar

Neste capítulo provaremos o teorema fundamental de Galois para extensões $L \supset K$ finitas tais que $\mathbb{C} \supset L \supset K \supset \mathbb{Q}$. Os resultados aqui apresentados se encontram no artigo (OLIVEIRA; NEUMAN, 2014)

4.1 Extensões galoisianas e extensões normais

Definição 4.1.1. *Seja L uma extensão de K. Se existe $f(x) \in K[x]$ tal que $L = Gal(f, K)$, dizemos que $L \supset K$ é uma extensão galoisiana.*

Definição 4.1.2. *Seja $L \supset K$ uma extensão algébrica. Dizemos que $L \supset K$ é normal se para todo $f(x) \in K[x]$, irredutível sobre K tal que possui uma raiz $\alpha \in L$, então $f(x)$ possui todas as suas raízes em L.*

Observação 4.1.1. *Mostraremos no Corolário* 4.1.2 *que se uma extensão $L \supset K$ é finita, então ser extensão galoisiana é equivalente a ser extensão normal.*

Exemplo 4.1.1. *As raízes do polinômio $x^3 - 2$ são $\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}$; onde ξ é raiz de $x^2 + x + 1$ (observe que $\xi^3 = 1$).*

Assim

$$\mathbb{Q}[\xi, \sqrt[3]{2}] = Gal(x^3 - 2, \mathbb{Q}), \quad isto \text{ é } \mathbb{Q}[\xi, \sqrt[3]{2}] \supset \mathbb{Q}$$

é uma extensão galoisiana, e pelo Corolário 4.1.2, também uma extensão normal.

Exemplo 4.1.2. *$\mathbb{C} \supset \mathbb{R}$ é uma extensão normal de $\mathbb{R}$ pois todo polinômio de $\mathbb{R}[x]$ se fatora em $\mathbb{C}$.*

Exemplo 4.1.3. *$\mathbb{Q}[\sqrt[3]{2}]$ não é uma extensão normal de $\mathbb{Q}$ pois não contém todos os conjugados, isto é, as raízes complexas de $\sqrt[3]{2}$.*

Definição 4.1.3. *Sejam K, K' corpos e $\sigma : K \to K'$ um isomorfismo de K sobre K'. Se $f(x) \in K[x]$, com $f(x) = a_0 + a_1x + ... + a_nx^n$, então definimos*

$$f^\sigma(x) = a'_0 + a'_1x + ... + a'_nx^n \in K'[x],$$

onde $a'_i = \sigma(a_i)$ para $i = 1, 2, ..., n$.

Proposição 4.1.1. *Sejam K, K' corpos, $\sigma : K \to K'$ um isomorfismo de corpos 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 raiz de $h^\sigma(x)$ em $\mathbb{C}$, então existe um único isomorfismo $\hat{\sigma} : K[\alpha] \to K'[\beta]$ tal que a função $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma} \mid_K = \sigma$.*

Demonstração: Sejam 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 e mais ainda se $\partial h(x) = \partial h^\sigma(x) = r$ sobre K, segue que:

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

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

Verifiquemos que $\hat{\sigma} : K[\alpha] \to K'[\beta]$ definido por

$$\hat{\sigma}(a_0 + a_1\alpha + ... + a_{r-1}\alpha^{r-1}) = \sigma(a_0) + \sigma(a_1)\beta + ... + \sigma(a_{r-1})\beta^{r-1}$$

é um isomorfismo de corpos, tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma} \mid_K = \sigma$.

Devemos provar então que:

a) $\hat{\sigma}$ é um homomorfismo;

Perceba que para $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in K[x]$. 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 $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ e $g(x) = b_0 + b_1x + ... + b_{n-1}x^{n-1}$ e seja $t(x) = f(x) + g(x)$.

Daí,

$$\hat{\sigma}(f(\alpha) + g(\alpha)) = \hat{\sigma}(t(\alpha)) = t^\sigma(\beta).$$

Por outro lado,

$$t^\sigma(x) = f^\sigma(x) + g^\sigma(x)$$

ou seja,

$$t^\sigma(\beta) = f^\sigma(\beta) + g^\sigma(\beta) = \hat{\sigma}(f(\alpha)) + \hat{\sigma}(g(\alpha)).$$

Devemos também mostrar que $\hat{\sigma}(f(\alpha)g(\alpha)) = \hat{\sigma}(f(\alpha))\hat{\sigma}(g(\alpha)) = f^\sigma(\beta)g^\sigma(\beta)$. De fato, sabemos que

$$f(x)g(x) = q(x)h(x) + R(x), \partial(R(x)) < r. \qquad (1)$$

Daí, $f(\alpha)g(\alpha) = R(\alpha)$, pois $h(\alpha) = 0$, assim $\hat{\sigma}(f(\alpha)g(\alpha)) = \hat{\sigma}(R(\alpha)) = R^\sigma(\beta)$.

Por outro lado, aplicando σ na equação (1) obtemos:

$$f^\sigma(x)g^\sigma(x) = q^\sigma(x)h^\sigma(x) + R^\sigma(x).$$

Daí, $f^\sigma(\beta)g^\sigma(\beta) = R^\sigma(\beta),$ pois $h^\sigma(\beta) = 0$. Logo, $\hat{\sigma}(f(\alpha)g(\alpha)) = f^\sigma(\beta)g^\sigma(\beta)$. Portanto, $\hat{\sigma}$ é um homomorfismo.

b) $\hat{\sigma}$ é injetor;

Como $K[\alpha]$ é um corpo e $\hat{\sigma} \neq 0$, segue que $Ker(\hat{\sigma}) = \{0\}$, logo $\hat{\sigma}$ é injetor.

c) $\hat{\sigma}$ é sobrejetor;

De fato, seja $b_0 + b_1\beta + ... + b_{r-1}\beta^{r-1} \in K'[\beta]$. Como σ é um isomorfismo então existem $a_0, a_1, ..., a_{r-1} \in K$ tais que $\sigma(a_j) = b_j, j = 0, ..., r-1$. 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.

Assim, $\hat{\sigma}$ é um isomorfismo.

d) $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma} \mid_K = \sigma$.

Como $\alpha \in K[\alpha]$, então $\alpha = 0 + 1\alpha$.

Assim, $\hat{\sigma}(\alpha) = \sigma(0) + \sigma(1)\beta = \beta$, logo $\hat{\sigma}(\alpha) = \beta$. E ainda, $\hat{\sigma}(a_0) = \sigma(a_0)$, logo $\hat{\sigma} \mid_K = \sigma$.

Agora mostremos a unicidade:
Seja $\varphi : K[\alpha] \to K'[\beta]$ tal que $\varphi(\alpha) = \beta$ e $\varphi \mid_K = \sigma$.
Então:

$\varphi(a_0 + a_1\alpha + ... + a_{r-1}\alpha^{r-1}) = \varphi(a_0) + \varphi(a_1)\varphi(\alpha) + ... + \varphi(a_{r-1})\varphi(\alpha^{r-1}) =$
$a'_0 + a'_1\beta + ... + a'_{r-1}\beta^{r-1} = \hat{\sigma}(a_0 + a_1\alpha + ... + a_{r-1}\alpha^{r-1})$.

□

Proposição 4.1.2. *Sejam K, K' corpos e $\sigma : K \to K'$ um isomorfismo e $\alpha \in \mathbb{C}$ uma raiz qualquer em $f(x) \in K[x]$. Então existe β 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 $\sigma_1 \mid_K = \sigma$.*

Demonstração: Seja $f(x) = f_1(x)^{m_1} f_2(x)^{m_1} ... f_k(x)^{m_k}$, onde $f_1(x), ..., f_k(x)$ são os distintos fatores irredutíveis de $f(x)$ em $K[x]$. Assim, $f^\sigma(x) = f_1^\sigma(x)^{m_1} f_2^\sigma(x)^{m_2} ... f_k^\sigma(x)^{m_k}$, onde $f_1^\sigma(x), ..., f_k^\sigma(x)$ são os distintos fatores irredutíveis de $f^\sigma(x)$ em $K'[x]$. Se α é raiz de $f(x)$ podemos assumir que α é raiz de $f_1(x)$, irredutível sobre K. Assim, se β é qualquer raiz do polinômio $f_1^\sigma(x)$, irredutível sobre K', considerando $h(x) = f_1(x)$, segue da Proposição 4.1.1 que existe um isomorfismo $\sigma_1 : K[\alpha] \to K'[\beta]$ tal que $\sigma_1(\alpha) = \beta$ e $\sigma_1 \mid_K = \sigma$.

□

Teorema 4.1.1. *Sejam K, K' corpos e $\sigma : K \to K'$ um isomorfismo, $f(x) \in K[x]$ e $\alpha_1, \alpha_2, ..., \alpha_r$ as distintas raízes de $f(x)$ em $\mathbb{C}$. Se $L = Gal(f, K)$ e $L' = Gal(f^\sigma, K')$ então existe $\hat{\sigma} : L \to L'$ um isomorfismo tal que $\hat{\sigma} \mid_K = \sigma$ e $\hat{\sigma}(\alpha_1), \hat{\alpha}(\alpha_2), ..., \hat{\sigma}(\alpha_r)$ são as raízes distintas 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 $\mathbb{C}[x]$, mas isto implica que $\alpha_1 \in K$ (ver o coeficiente de x^{m-1} em $f(x)$) e portanto $\sigma(\alpha_1) \in K'$ é a única raiz de $f^\sigma(x)$ em $\mathbb{C}$ e teremos $L = K, L' = K'$ e $\hat{\sigma} = \sigma : L \to L'$.

Agora se $f(x) = f_1(x)^{m_1} ... f_k(x)^{m_k}$ onde $f_i(x) \in K[x]$ são os 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 os distintos polinômios irredutíveis sobre K'.

Sabemos que o número r de raízes distintas de $f(x)$ em $\mathbb{C}$ é igual à soma dos graus dos polinômios $f_1(x), ..., f_k(x)$ e portanto temos como consequência que o número de raízes distintas de $f^\sigma(x)$ em $\mathbb{C}$ é também igual a r.

Sejam $\beta_1, \beta_2, ..., \beta_r$ as distintas raízes em $\mathbb{C}$ do polinômio $f^\sigma(x) \in K'[x]$, e sejam $K_1 = K[\alpha_1], K_2 = K_1[\alpha_2], ..., K_r = K_{r-1}[\alpha_r]$ e portanto $L = K[\alpha_1, ..., \alpha_r] = K_r$.

Pela Proposição 4.1.2, existe $\beta \in \beta_1, ..., \beta_r$ e existe um isomorfismo $\sigma_1 : K[\alpha_1] \to K'[\beta]$ tal que $\sigma_1(\alpha_1) = \beta$ e $\sigma_1 \mid_K = \sigma$. Notemos $\beta_1 = \beta, K_1 = K[\alpha_1]$ e $K'_1 = K'[\beta_1]$.

Como $f(x) \in K[x]$ e $\sigma_1 \mid_K = \sigma$, segue imediatamente que $f(x) \in K_1[x]$ e $f^{\sigma_1}(x) \in K_1'[x]$. Novamente pela Proposição 4.1.2, para os corpos K_1, K_1' e $\sigma_1 : K_1 \to K_1'$ existe $\beta \in \{\beta_2, ..., \beta_k\}$ (que chamaremos de β_2) e existe um isomorfismo $\sigma_2 : K_1[\alpha_2] \to K_1'[\beta_2]$ tal que $\sigma_2(\alpha_2) = \beta_2$ e $\sigma_2 \mid_{K_1} = \sigma_1 : K_1 \to K_1'$.

Observe que σ_2 é um isomorfismo e $\alpha_1 \neq \alpha_2$ implica que $\beta_1 = \sigma_2(\alpha_1) \neq \sigma_2(\alpha_2) = \beta_2$.

Como $\sigma_1 \mid_K = \sigma$ segue que $\sigma_2 \mid_K = \sigma$ e $\sigma_2(\alpha_1) = \beta_1, \sigma_2(\alpha_2) = \beta_2$ e $\sigma_2 : K[\alpha_1, \alpha_2] \to K'[\beta_1, \beta_2]$ é um isomorfismo.

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

Aplicando a Proposição 4.1.2 para os corpos $K_{k-1} = K[\alpha_1, ..., \alpha_{k-1}]$ 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 (que denotaremos por β_k) raiz de f^{σ} e um isomorfismo $\sigma_k : K_{k-1}[\alpha_k] \to K_{k-1}'[\beta_k]$ tal que $\sigma_k \mid_{K_{k-1}} = \sigma_{k-1}$ e $\sigma_k(\alpha_k) = \beta_k$.

Daí, segue que existe $\sigma_k : K[\alpha_1, ..., \alpha_k] \to K'[\beta_1, ..., \beta_k]$ isomorfismo tal que $\sigma_i(\alpha_i) = \beta_i$, para todo $i \in \{1, 2, ..., k\}$ e $\sigma_k \mid_K = \sigma$. Como $L = K_r = K[\alpha_1, ..., \alpha_r]$ o teorema segue imediatamente.

□

Corolário 4.1.1. *Seja $L \supset K$ 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 $\sigma' \in Aut_K L$ tal que $\sigma' \mid_M = \sigma$.*

Demonstração: Se $L = Gal(f, K)$ então a demonstração é consequência direta do teorema anterior pois $f^{\sigma}(x) = f(x)$ e $L = G(f, M) = L' = Gal(f^{\sigma}, M')$.

□

Corolário 4.1.2. *Seja $L \supset K$ uma extensão finita. Então esta extensão é galoisiana se, e somente se, esta extensão for normal.*

Demonstração: ($\Leftarrow$) Suponha que $L \supset K$ é normal. Como $L \supset K$ é finita, então pelo Teorema 3.3.1 existe $u \in L$ tal que $L = K[u]$. Como $L \supset K$ é normal segue que, se u é raiz de $h(x) = irr(u, K)$, então todas as raízes de $h(x)$ estão em L, o que implica que $L = Gal(h, K)$, ou seja, $L \supset K$ é galoisiana.
($\Rightarrow$) Suponhamos que $L \supset K$ é galoisiana com $L = Gal(f, K)$, seja $g(x) \in K[x]$ um polinômio irredutível tal que existe $\alpha \in L, g(\alpha) = 0$.

Mostremos que para todo $\beta \in \mathbb{C}$, se $g(\beta) = 0$ então $\beta \in L$.

Seja $\beta \neq \alpha$ uma raiz de $g(x)$ em $\mathbb{C}$. Sabemos pela Proposição 4.1.1 que existe um isomorfismo $\sigma : K[\alpha] \to K[\beta]$ tal que $\sigma(\alpha) = \beta$ e $\sigma(a) = a$, para todo $a \in K$.

Sejam $M = K[\alpha], M' = K[\beta], L' = Gal(f, M')$ e sejam $\gamma_1, ..., \gamma_n$ raízes de f. Então, $L = K[\gamma_1, ..., \gamma_n] \subset K[\beta][\gamma_1, ..., \gamma_n] = M'[\gamma_1, ..., \gamma_n] = L'$. Logo $L \subset L'$ e pelo Teorema 4.1.1 existe um isomorfismo $\hat{\sigma} : L \to L'$ que extende $\sigma : M \to M'$. Como $L \subset L'$, então $L = L'$.

□

Corolário 4.1.3. *Se $L \supset K$ é uma extensão galoisiana então:*

(i) $[L : K] =\mid Aut_K L \mid$.

(ii) Seja $\alpha \in L$, se $\alpha \notin K$ então existe $\sigma \in Aut_K L$ tal que $\sigma(\alpha) \neq \alpha$.

Demonstração: (i) Como $L \supset K$ é galoisiana, então L é gerado, sobre K, por um número finito de elementos algébricos sobre K, logo $L \supset K$ é uma extensão finita. Pelo Teorema 3.3.1, existe $\alpha \in L$ tal que $L = K[\alpha]$. Seja $h(x) = irr(\alpha, K)$, para cada raiz β de $h(x)$, temos que $\beta \in L$, pois $L \supset K$ é extensão normal. Como $[K[\beta] : K] = \partial(h(x))$, então $L = K[\beta]$. Pela Proposição 4.1.1, existem tantos automorfismos de L, quantas raízes do polinômio $h(x)$ (com $K = K$ e $\sigma = id$). Assim, $[L : K] = \partial(h(x)) \leq\mid Aut_K L \mid$ e pelo Corolário 3.3.5, temos $[L : K] =\mid Aut_K L \mid$.

(ii) Seja $\alpha \in L, \alpha \notin K$. Se $g(x) = irr(\alpha, K)$ segue que $\partial(g(x)) = r \geq 2$. Pela Proposição 3.2.2, existe $\beta \neq \alpha$ tal que $g(\beta) = 0$. Pelo Corolário 4.1.2, $\beta \in L$, pois L é normal. Agora pela Proposição 4.1.1, existe um isomorfismo $\sigma : K[\alpha] \to K[\beta]$ tal que $\sigma(a) = a$, para todo $a \in K$ e $\sigma(\alpha) = \beta \neq \alpha$. Pelo Corolário 4.1.1, existe $\hat{\sigma} \in Aut_K L, \hat{\sigma} \mid_{K[\alpha]} = \sigma$ finalizando assim a demonstração.

□

Teorema 4.1.2. *Se $K \subset M \subset L$ são extensões finitas e $L \supset K$ é galoisiana, então as seguintes afirmações são equivalentes:*

(i) $M \supset K$ é galoisiana.

(ii) $\sigma(M) \subset M$, para todo $\sigma \in Aut_K L$.

(iii) $Aut_M L \triangleleft Aut_K L$, onde $H \triangleleft G$ indica que H é subgrupo normal de G.

Demonstração: $(i) \Rightarrow (ii)$ Seja $u \in L$ tal que $M = K[u]$. Se $M \supset K$ é galoisiana segue do Corolário 4.1.2 que $M \supset K$ 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 $M \supset K$ é normal temos $v = \sigma(u) \in M$, ou seja, $\sigma(K[u]) \subset K[u] = M$.

$(ii) \Rightarrow (i)$ Seja $u \in L$ tal que $M = K[u]$ e seja $h(x) = irr(u, K)$. Vamos mostrar que se $\sigma(M) \subset M$ 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 4.1.1, existe um isomorfismo $\sigma_0 : M \to M$ tal que $\sigma_0(u) = v$ e $\sigma_0(a) = a$, para todo $a \in K$.

Assim pelo Teorema 4.1.1, existe $\sigma \in Aut_K L$ tal que $\sigma \mid_M = \sigma_0$. Como $\sigma(M) \subset M$ e $u \in M$ temos $v = \sigma(u) \in M$.

$(ii) \Rightarrow (iii)$ Sejam $\sigma \in Aut_K L$ e $\gamma \in Aut_M L$. Vamos mostrar que se $\sigma(M) \subset M$, então $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$. Seja $m \in M$, então $m' = \sigma(m) \in M$ e $\gamma(m') = m'$, logo $(\sigma^{-1} \circ \gamma \circ \sigma)(m) = \sigma^{-1}(\gamma(m')) = \sigma^{-1}(m') = m$, isto é $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$.

$(iii) \Rightarrow (ii)$ Suponha por absurdo que existe $\sigma \in Aut_K L$ e $u \in M$ tal que $\sigma(u) = v \notin M$. Como $L \supset K$ é galoisiana, existe f tal que $L = Gal(f, K) \subset Gal(f, M) \subset L$, logo $L \subset M$ é galoisiana. Temos pelo Corolário 4.1.3 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 $Aut_M L \triangleleft Aut_K L$.

□

Teorema 4.1.3. *Seja $L \supset K$ uma extensão finita. Então as seguintes afirmações são equivalentes:*

(i) $L \supset K$ *é galoisiana.*

(ii) $L \supset K$ *é normal.*

(iii) Para todo $\alpha \in L - K$ *existe* $\sigma \in Aut_K L$ *tal que* $\sigma(\alpha) \neq \alpha$.

(iv) $[L : K] = \mid Aut_K L \mid$.

Demonstração: $(i) \Leftrightarrow (ii)$ Segue do Corolário 4.1.2

$(i) \Rightarrow (iii)$ Segue do Corolário 4.1.3.

$(iii) \Rightarrow (iv)$ Pelo Corolário 3.3.5, temos $[L : K] \geq \mid Aut_K L \mid$. Suponha por absurdo que $[L : K] > \mid Aut_K L \mid$. Seja $Aut_K L = \{\varphi_1, \varphi_2, ..., \varphi_n\}$ onde $\varphi_1 = id_L$ 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 $x_1, x_2, ..., x_{n+1} \in L$:

$$\begin{cases} \varphi_1(u_1)x_1 + \varphi_1(u_2)x_2 + ... + \varphi_1(u_{n+1})x_{n+1} = 0 \\ \varphi_2(u_1)x_1 + \varphi_2(u_2)x_2 + ... + \varphi_2(u_{n+1})x_{n+1} = 0 \\ \qquad\qquad\qquad \vdots \\ \varphi_n(u_1)x_1 + \varphi_n(u_2)x_2 + ... + \varphi_n(u_{n+1})x_{n+1} = 0 \end{cases} \tag{4.1}$$

Como o número de equações de (4.1) é menor que o número de incógnitas então (4.1) 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 (4.1) 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 (4.1) 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 $\varphi \in Aut_K L$ 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 $\sigma\varphi_i = \varphi_k$ 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

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

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 $(1, a_2, ..., a_r, 0, ..., 0)$.

$(iv) \Rightarrow (i)$ Suponhamos $L \supset K$ extensão finita e $[L : K] =\mid Aut_K L \mid$. Vamos provar que $L \supset K$ é galoisiana. Sejam $L = K[u]$ e $h(x)$ definido por $h(x) = irr(u, K)$ então para todo $\sigma \in Aut_K L$ tem-se $\sigma(u)$ 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, $\mid Aut_K L \mid = n$, com n o número de raízes de $h(x)$ em L. Agora se $[L : K] =\mid Aut_K L \mid$ então $\partial(h(x)) = [L : K] =\mid Aut_K L \mid = n$.

Daí segue que L contém todas as raízes de $h(x)$, ou seja, $L = Gal(h, K)$.

□

Proposição 4.1.3. *Seja $L \supset K$ uma extensão galoisiana e seja $f(x) \in K[x]$ o polinômio de grau n, tal que $L = Gal(f, K)$. Então $G = Aut_K L$ é isomorfo a um subgrupo de S_n (grupo de permutações de n elementos).*

Demonstração: Seja $B = \{u_1, u_2, ..., u_n\}$ o conjunto de todas as raízes de $f(x)$. Como $L = Gal(f, K)$, temos $B \subset L = K[B]$. Sabemos, pela Proposição 3.2.2, que todo automorfismo $\sigma \in G = Aut_K L$ envia uma raiz de $f(x)$ em outra raiz de $f(x)$. Assim, como B é finito e σ injetivo, segue que $\sigma_0 = \sigma \mid_B : B \to B$ define uma permutação do conjunto B. Se S_B denota o grupo das permutações do conjunto B então basta mostrar que $Aut_K L$ é isomorfo a um subgrupo de S_B, pois $S_B \simeq S_n$.
Define-se da seguinte forma:

$$\begin{array}{rccc} \psi: & G & \to & S_B \\ & \sigma & \mapsto & \sigma_0 = \sigma \mid_B . \end{array}$$

A função ψ é um homomorfismo de grupos, pois $\psi(\sigma \circ \tau) = (\sigma \circ \tau) \mid_B = \sigma \mid_B \circ \tau \mid_B$. Obviamente ψ é injetiva, pois se todas as raízes de $f(x)$ são fixadas por $\sigma \in G$, então $\sigma = id_L$. Isto é, $G \simeq \psi(G)$ é subgrupo de $S_B \simeq S_n$.

□

Proposição 4.1.4. *Sejam K um corpo, $a \in K$ e $L = Gal(x^n - a, K)$. Suponha que K contém uma raiz ζ primitiva n-ésima da unidade, então $G = Aut_K L$ 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 $x^n - a$ em $\mathbb{C}$.

Sabemos que $L = K[\zeta, \alpha] = K[\alpha]$, pois $\zeta \in K$. Assim pela Proposição 3.2.2, 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 :

$$(\sigma \circ \tau)(\alpha) = \sigma(\alpha\zeta^j) = \sigma(\alpha)\zeta^j = \alpha\zeta^{i+j},$$

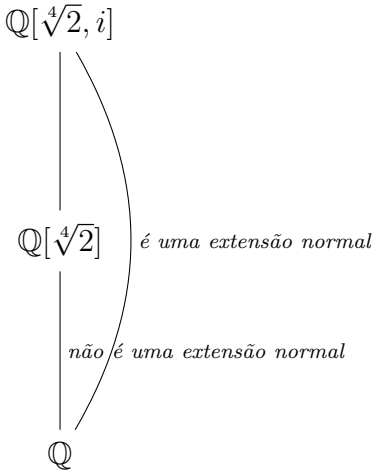
$$(\tau \circ \sigma)(\alpha) = \tau(\alpha\zeta^i) = \tau(\alpha)\zeta^i = \alpha\zeta^{j+i}.$$

Assim $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha)$, para todo $\sigma, \tau \in Aut_K L$. Como $L = K[\alpha]$, então $\sigma \circ \tau = \tau \circ \sigma$, para todo $\sigma, \tau \in Aut_K L$.

□

Exemplo 4.1.4. $\mathbb{Q}[\sqrt[4]{2}] \supset \mathbb{Q}$ *não é uma extensão normal, pois os* $\mathbb{Q}$*-conjugados de* $\mathbb{Q}[\sqrt[4]{2}]$ *são* $\pm[\sqrt[4]{2}]$, $\pm i[\sqrt[4]{2}]$. *Os dois últimos não são números reais e logo não pertencem ao corpo* $\mathbb{Q}[\sqrt[4]{2}]$.

O diagrama mostra a estrutura do corpo intermediário da extensão $\mathbb{Q}[\sqrt[4]{2}] \supset \mathbb{Q}$.



4.2 A correspondência de Galois

A partir desta seção denotaremos $G = Aut_K L$ o grupo de automorfismos de L que fixam K. Este grupo G é chamado de Grupo de Galois da extensão $L \supset K$.

Definição 4.2.1. *Seja* $L \supset K$ *uma extensão finita. Dizemos que* M *é um corpo intermediário de* $L \supset K$ *se* M *é um subcorpo de* L *contendo* K*, ou seja,* $K \subset M \subset L$.

Proposição 4.2.1. *Seja* H *subgrupo de* $G = Aut_K L$*, então o conjunto*

$$M = \{a \in L : \gamma(a) = a, \forall \gamma \in H\}$$

formado pelos elementos de L fixados pelos elementos de H é um corpo intermediário de $L \supset K$. Notaremos $M = L^H$.

Demonstração: De fato, $0, 1 \in K \subset L^H$.

Se $x, y \in L^H$, para todo $\gamma \in H$ temos $\gamma(x - y) = \gamma(x) - \gamma(y) = x - y$, então $x - y \in L^H$.

Se $x, y \in L^H$, para todo $\gamma \in H$ temos $\gamma(xy^{-1}) = \gamma(x) \cdot \gamma(y^{-1}) = \gamma(x) \cdot \gamma(y)^{-1} = xy^{-1}$ então $xy^{-1} \in L^H$.

Isto é, L^H é um corpo intermediário da extensão $L \supset K$. Esse corpo L^H é chamado de corpo fixo de H.

Assim temos uma correspondência entre subgrupos de $Aut_K L$ e os corpos intermediários da extensão $L \supset K$ da seguinte forma: Dado um subgrupo H de $G = Aut_K L$ obtemos um corpo intermediário L^H da extensão $L \supset K$.

Por outro lado, dado M um corpo, com $K \subset M \subset L$, obtemos o grupo $Aut_M L$. Temos uma inclusão natural $Aut_M L \subset Aut_K L$, pois se um automorfismo de L fixa M então ele fixará também $K \subset M$.

Para $G = Aut_K L$ temos as seguintes propriedades imediatas:

1. $Aut_L L = \{id_L\}$.
2. $L^{id_L} = \{a \in L : id_L(a) = a\} = L$.
3. $K \subset L^G = \{a \in L : \gamma(a) = a, \forall \gamma \in G\}$.
4. Pelo Teorema 4.1.3, temos:

$$L^G = K \Leftrightarrow L \supset K \text{ é uma extensão galoisiana.}$$

□

Proposição 4.2.2. *De acordo com as notações acima, temos:*

(a) Se M_1, M_2 são corpos tais que $K \subset M_1 \subset M_2 \subset L$ então $Aut_{M_2} L \subset Aut_{M_1} L$.

(b) Se $H_1 \subset H_2$ são subgrupos de $Aut_K L$ então $L^{H_2} \subset L^{H_1}$.

(c) Para todo corpo intermediário M com $K \subset M \subset L$, tem-se $M \subset L^{Aut_M L}$.

(d) Para todo subgrupo H de $Aut_K L$, tem-se $H \subset Aut_{L^H} L$.

Demonstração: (a) Considere os corpos $K \subset M_1 \subset M_2 \subset L$. Seja $\gamma \in Aut_{M_2}L$. Como $M_1 \subset M_2$, então γ fixa M_1 e daí $\gamma \in Aut_{M_1}L$.

(b) Sejam os grupos $H_1 \subset H_2 \subset G$, $\gamma \in H_1$ e a $\in L^{H_2}$. Como $\gamma \in H_1 \subset H_2$, então $\gamma(a) = a$. Logo $a \in L^{H_1}$.

(c) Seja M um corpo intermediário da extensão $L \supset K$. Por definição os elementos de $Aut_M L$ fixam M, logo $M \subset L^{Aut_M L}$.

(d) Seja H um subgrupo de G. Então um elemento $\gamma \in H \subset G$ é um automorfismo de L que fixa L^H, logo $H \subset Aut_{(L^H)}L$.

□

Considerando os corpos $K \subset M_1 \subset M_2 \subset L$ e os grupos $id_L \subset H_1 \subset H_2 \subset G = Aut_K L$, temos as correspondências abaixo:

$$\begin{array}{ccccccc} K & \subset & M_1 & \subset & M_2 & \subset & L \\ | & & | & & | & & | \\ Aut_K L & \supset & Aut_{M_1} L & \supset & Aut_{M_2} L & \supset & \{id_L\} \end{array}$$

e

$$\begin{array}{ccccccccc} & & G & \supset & H_1 & \supset & H_2 & \supset & \{id_L\} \\ & & | & & | & & | & & | \\ K & \subset & L^G & \subset & L^{H_1} & \subset & L^{H_2} & \subset & L. \end{array}$$

Agora vamos demonstrar o Teorema Fundamental de Galois:

Teorema 4.2.1. *(Teorema Fundamental de Galois) Se $L \supset K$ é uma extensão galoisiana, então:*

(a) Para todo corpo intermediário M, com $K \subset M \subset L$, tem-se $[L : M] =\mid Aut_M L \mid$ e $[M : K] = (G : Aut_M L)$ (o índice de $Aut_M L$ em G).

(b) Para todo subgrupo H de G, tem-se $[L : L^H] =\mid H \mid$ e $[L^H : K] = (G : H)$ (o índice de H em G).

(c) Para todo subgrupo $H \subset G$ e todo corpo M tal que $K \subset M \subset L$ temos que $Aut_{L^H} L = H$ e $L^{Aut_M L} = M$.

(d) Para todo corpo intermediário M, com $K \subset M \subset L$ temos que a extensão $M \supset K$ é galoisiana se, e somente se $Aut_M L$ é subgrupo normal de G.

(e) Para todo corpo intermediário M, com $K \subset M \subset L$, se $M \supset K$ é galoisiana então $[M : K] =\mid Aut_K M \mid$ e $G/Aut_M L \simeq Aut_K M$.

Demonstração: (a) Seja M um corpo intermediário da extensão $L \supset K$. Como $L \supset K$ é galoisiana, então $L \supset M$ também é galoisiana. Pelo Teorema 4.1.3, segue que: $[L : M] =\mid Aut_M L \mid$ e como $[L : K] =\mid Aut_K L \mid= [L : M][M : K]$, temos $[M : K] =\mid G \mid / \mid Aut_M L \mid= (G : Aut_M L)$.

(b) Seja H subgrupo de G e $M = L^H$. Sabemos pelo item (a) que:

$$[L : M] =\mid Aut_M L \mid e [M : K] = (G : Aut_M L).$$

Por outro lado, pela Proposição 4.2.2 item (d), tem-se: $H \subset Aut_M L$, então $[L : M] =\mid Aut_M L \mid\geq\mid H \mid$.

Utilizaremos um argumento semelhante ao usado na demonstração do Teorema 4.1.3. Suponha $H = \{\gamma_1 = id_M, \gamma_2, ..., \gamma_n\}$ e por absurdo suponha $\mid Aut_M L \mid>\mid H \mid$. Logo $[L : M] > n$.

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

$$\begin{cases} \gamma_1(u_1)a_1 + \gamma_1(u_2)a_2 + ... + \gamma_1(u_{n+1})a_{n+1} = 0 \\ \gamma_2(u_1)a_1 + \gamma_2(u_2)a_2 + ... + \gamma_2(u_{n+1})a_{n+1} = 0 \\ \vdots \\ \gamma_n(u_1)a_1 + \gamma_n(u_2)a_2 + ... + \gamma_n(u_{n+1})a_{n+1} = 0. \end{cases} \tag{4.2}$$

Então existe uma solução não nula $(a_1, a_2, ..., a_{n+1}) \in L^{n+1}$. Tomemos uma solução não trivial de (4.2) 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

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

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 (3) com um número máximo de zeros. A primeira equação é :

$$u_1 + u_2a_2 + ... + u_ra_r = 0, \text{ pois } \gamma_1 = id.$$

Como $\{u_1, u_2, ..., u_r\}$ é L.I sobre M, então nem todos os a_j são elementos de M.

Logo reorganizando novamente os valores, podemos supor $a_2 \notin M = L^H$. Assim, existe $\gamma \in H$ tal que $\gamma(a_2) \neq a_2$.

Aplicando γ ao sistema (4.2) temos:

$$\begin{cases} \gamma(\gamma_1(u_1)) + \gamma(\gamma_1(u_2)a_2) + ... + \gamma(\gamma_1(u_r)a_r) = 0 \\ \gamma(\gamma_2(u_1)) + \gamma(\gamma_2(u_2)a_2) + ... + \gamma(\gamma_2(u_r)a_r) = 0 \\ \vdots \\ \gamma(\gamma_n(u_1)) + \gamma(\gamma_n(u_2)a_2) + ... + \gamma(\gamma_n(u_r)a_r) = 0. \end{cases} \tag{4.3}$$

Mas como $\gamma \in H$ e $H = \{\gamma_1, ..., \gamma_n\}$ então $\{\gamma\gamma_1, ..., \gamma\gamma_n\} = H$, ou seja, o sistema (4.3) é uma permutação de (4.2):

$$\begin{cases} \gamma_1(u_1) + \gamma_1(u_2)\gamma(a_2) + ... + \gamma_1(u_r)\gamma(a_r) = 0 \\ \gamma_2(u_1) + \gamma_2(u_2)\gamma(a_2) + ... + \gamma_2(u_r)\gamma(a_r) = 0 \\ \vdots \\ \gamma_n(u_1) + \gamma_n(u_2)\gamma(a_2) + ... + \gamma_n(u_r)\gamma(a_r) = 0. \end{cases} \tag{4.4}$$

Subtraindo o sistema (4.2) de (4.4), temos:

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

Como $a_2 \neq \gamma(a_2) \Rightarrow a_2 - \gamma(a_2) \neq 0$ e

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

é uma solução de (4.2) com no máximo $r - 1$ coeficientes não nulos.

Logo, temos uma contradição com a minimalidade de r de coeficientes não nulos. Portanto $\mid Aut_M L \mid = \mid H \mid$, ou seja, $H = Aut_M L$ e obtemos o que queríamos.

c) Pelo item (b), já temos que $H = Aut_{L^H} L$. Resta provar que $L^{Aut_M L} = M$. Seja M um corpo intermediário da extensão $L \supset K$. Notemos $H = Aut_M L$. Como H fixa M, então $M \subseteq L^H \subseteq L$, ou seja, $[L : M] = [L : L^H][L^H : M]$. Pelo item (b), $[L : L^H] = \mid H \mid$ e pelo item (a), $[L : M] = \mid H \mid$.

Logo, $[L^H : M] = 1,$ isto é $\mathrm{L}^H = M$.

d) Segue imediatamente do Teorema 4.1.2, $M \supset K$ galoisiana se, e somente se, $Aut_M L \lhd Aut_K L = G$.

e) Sabemos do item (a) que $(G : Aut_M L) = [M : K]$, resta provar que para todo corpo intermediário M da extensão $L \supset K$, tal que $M \supset K$ seja galoisiana, temos que:

$$G/Aut_M L \simeq Aut_K M.$$

De fato, como$M \supset K$ é galoisiana, pelo Teorema 4.1.2, temos que para todo $\sigma \in G = Aut_K L$ tem-se $\sigma_0 = \sigma \mid_M \in Aut_K M$ portanto, podemos definir:

$$\begin{aligned} \phi : G &\to Aut_K M \\ \sigma &\mapsto \sigma_0 = \sigma \mid_M . \end{aligned}$$

Vemos que ϕ é homomorfismo de grupos. De fato, sejam $\sigma, \tau \in G$, então $\phi(\sigma \circ \tau) = (\sigma \circ \tau) \mid_M = \sigma \mid_M \circ \tau \mid_M = \phi(\sigma) \circ \phi(\tau)$.

Observe também que: $\sigma \in Ker(\Phi) \Leftrightarrow \Phi(\sigma) = id_M \Leftrightarrow \sigma \mid_M = id_M \Leftrightarrow \sigma \in Aut_M L$.

Por outro lado, como $L \supset M$ é uma extensão galoisiana, então pelo Corolário 4.1.1, para todo $\sigma_0 \in Aut_K M$, existe $\sigma \in Aut_K L$, tal que $\sigma \mid_M = \sigma_0$, logo ϕ é sobrejetor. Pelo Teorema de homomorfismo, temos:

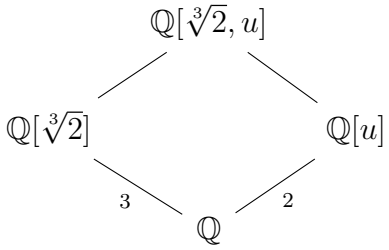
$$G/Aut_M L \simeq Aut_K M.$$

O seguinte diagrama ilustra a correspondência de Galois:

$$\begin{array}{ccccc} L^{id} & = & L & - & \{id_L\} & = & Aut_L L \\ & & | & & | & & \\ L^{H} & = & M & - & H & = & Aut_M L \\ & & | & & | & & \\ L^{G} & = & K & - & G & = & Aut_K L. \end{array}$$

Exemplo 4.2.1. *Seja $L = Gal(x^3 - 2, \mathbb{Q})$ o corpo de decomposição do polinômio $f(x) = x^3 - 2$. As 3 raízes de $x^3 - 2$ são $\sqrt[3]{2}$, $\sqrt[3]{2}u$ e $\sqrt[3]{2}u^2$, onde $u = cos\frac{2\pi}{3} + isen\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Temos então que $L = \mathbb{Q}[\sqrt[3]{2}, u]$.*

Logo $L \supset \mathbb{Q}$ é uma extensão normal cujo grau é 6.

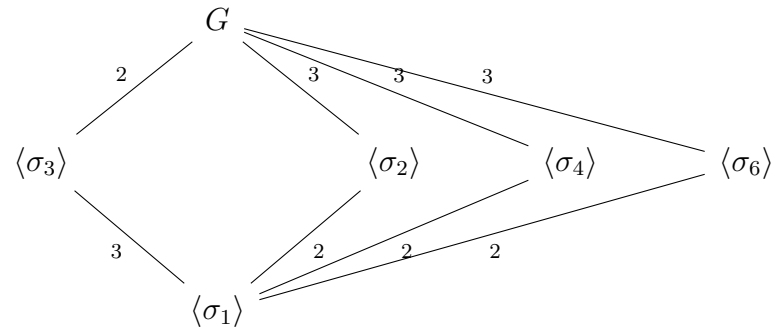


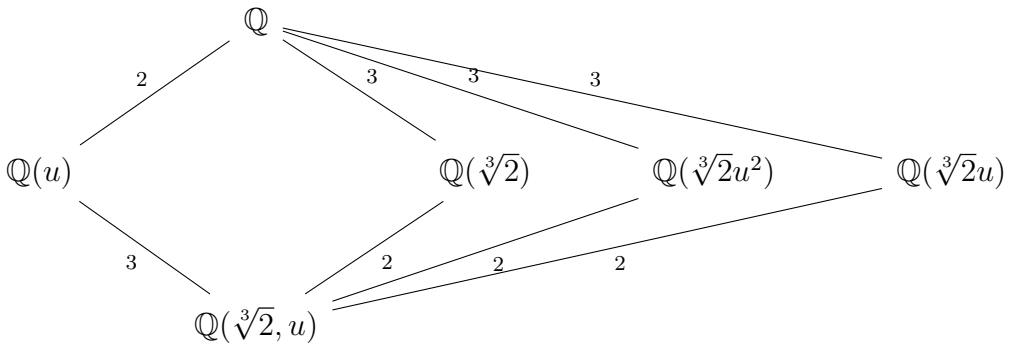
Todo o automorfismo σ de $G = Gal_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, u))$ ficam completamente determinado por sua ação em $\sqrt[3]{2}$ e u.

$$\begin{aligned}
\sigma_1 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad u \mapsto u \\
\sigma_2 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad u \mapsto u^2 \\
\sigma_3 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}u, \quad u \mapsto u \\
\sigma_4 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}u, \quad u \mapsto u^2 \\
\sigma_5 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}u^2, \quad u \mapsto u \\
\sigma_6 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}u^2, \quad u \mapsto u^2
\end{aligned}$$

$G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

Abaixo os diagramas que descrevem a correspondência:





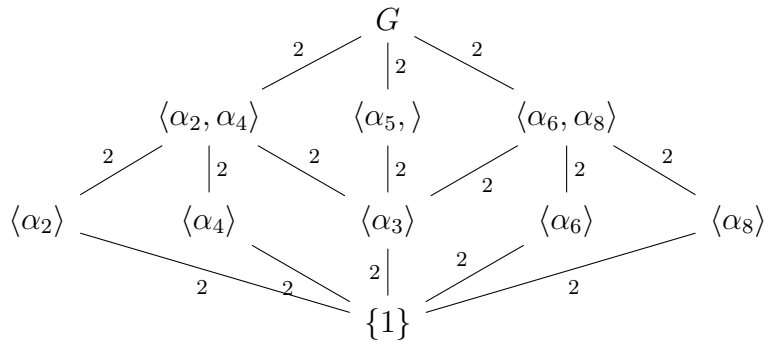
Exemplo 4.2.2. *Seja $L = Gal(x^4 - 2, \mathbb{Q})$ o corpo de decomposição do polinômio $p(x) = x^4 - 2$, cujas raízes são: $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ e $-i\sqrt[4]{2}$, onde $i = \sqrt{-1}$.*

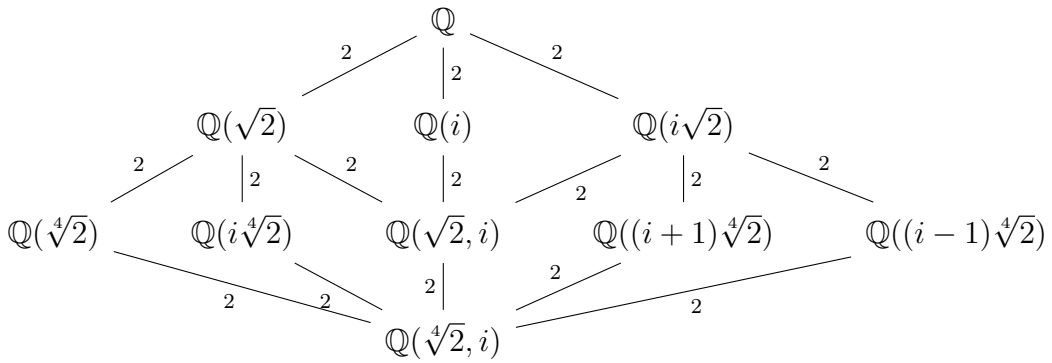
Como $[\mathbb{Q}[i, \sqrt[4]{2}] : \mathbb{Q}[i]] = 4$ e $[\mathbb{Q}[i] : \mathbb{Q}] = 2$, temos $[\mathbb{Q}[i, \sqrt[4]{2} : \mathbb{Q}] = 8$.

Os automorfismos σ de $Gal_{\mathbb{Q}}[\mathbb{Q}[i, \sqrt[4]{2}, i]$ são:

$$\begin{aligned}
\sigma_1 &: \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad i \mapsto i \\
\sigma_2 &: \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad i \mapsto -i \\
\sigma_3 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}, \quad i \mapsto i \\
\sigma_4 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}, \quad i \mapsto -i \\
\sigma_5 &: \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \quad i \mapsto i \\
\sigma_6 &: \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \quad i \mapsto -i \\
\sigma_7 &: \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, \quad i \mapsto i \\
\sigma_8 &: \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, \quad i \mapsto -i
\end{aligned}$$

Abaixo os diagramas que descrevem a correspondência:





5 Considerações finais

Ao término deste trabalho foi possível compreender os conteúdos básicos ao entendimento da teoria de Galois. Este trabalho possibilitou a compreensão, de forma simples, à teoria dos corpos. Que de um corpo base se pode construir um corpo maior que o contém, ao qual chamamos de extensão. Também foi possível compreender as propriedades das extensões, os elementos e as extensões algébricas e transcendentais. No capítulo quatro, podemos compreender a correspondência entre extensões intermediárias e subgrupos de Galois. Neste trabalho foi possível um conhecimento maior nos conteúdos da Álgebra Abstrata.

Referências

COELHO, F. U.; LOURENÇO, M. L. *Um Curso de Álgebra Linear*. [S.l.]: EdUSP, 2007. Citado na página 19.

DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. [S.l.]: Atual, 2011. Citado na página 9.

GONÇALVES, A. *Introdução à Álgebra*. [S.l.]: IMPA, 2002. Citado na página 10.

OLIVEIRA, A. C. de; NEUMAN, V. G. L. Correspondência de galois. 2014. Citado 2 vezes nas páginas 10 e 51.

SILVA, E. de O. Extensões algébricas dos racionais. 2013. Citado na página 10.