INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
GOIANO-CAMPUS URUTAÍ
NÚCLEO DE MATEMÁTICA, EDUCAÇÃO E MATEMÁTICA APLICADA
CURSO DE MATEMÁTICA

JOSÉ ARMANDO OLIVEIRA MENDES

UM BREVE ESTUDO SOBRE EXTENSÕES DE CORPOS

Urutaí, 15 de dezembro de 2023

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO-
NÚCLEO DE MATEMÁTICA, EDUCAÇÃO E MATEMÁTICA APLICADA
MATEMÁTICA

JOSÉ ARMANDO OLIVEIRA MENDES

UM BREVE ESTUDO SOBRE EXTENSÕES DE CORPOS

Monografia apresentada ao Curso de Matemática do Núcleo de Matemática, Educação e Matemática Aplicada do Instituto Federal de Educação, Ciência e Tecnologia Goiano-Campus Urutaí, como requisito parcial para obtenção do título de Licenciatura em Matemática.

Orientador:
Davidson Freitas Nogueira
Coorientador:
Dassael Fabrício dos Reis Santos

Urutaí, 15 de dezembro de 2023

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

Mendes, José Armando Oliveira
M538b UM BREVE ESTUDO SOBRE EXTENSÕES DE CORPOS / José Armando Oliveira Mendes; orientador Davidson Freitas Nogueira; co-orientador Dassael Fabrício dos Reis Santos. -- Urutaí, 2023.
52 p.

TCC (Graduação em Licenciatura em Matemática) -- Instituto Federal Goiano, Campus Urutaí, 2023.

1. Corpos. 2. Extensões de Corpos. 3. Polinômios. I. Nogueira, Davidson Freitas, orient. II. Santos, Dassael Fabrício dos Reis , co-orient. III. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

INSTITUTO FEDERAL
Goiano

Repositório Institucional do IF Goiano - RIIF Goiano
Sistema Integrado de Bibliotecas

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

- ☐ Tese (doutorado)
- ☐ Dissertação (mestrado)
- ☐ Monografia (especialização)
- ☑ TCC (graduação)
- ☐ Artigo científico
- ☐ Capítulo de livro
- ☐ Livro
- ☐ Trabalho apresentado em evento
- ☐ Produto técnico e educacional - Tipo:

Nome completo do autor: José Armando Oliveira Mendes

Matrícula: 2019101221230096

Título do trabalho: UM BREVE ESTUDO SOBRE EXTENSÕES DE CORPOS

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: ☑ Não ☐ Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: ☐/☐/☐

O documento está sujeito a registro de patente? ☐ Sim ☑ Não

O documento pode vir a ser publicado como livro? ☐ Sim ☑ Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

- Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Urutaí (Local) 14/12/2023 (Data)

José Armando Oliveira Mendes
Assinatura do autor e/ou detentor dos direitos autorais

Ciente e de acordo: Deodson Freitas Nogueira
Assinatura do(a) orientador(a)

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Ata nº 187/2023 - DE-UR/CMPURT/IFGOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Na presente data realizou-se a sessão pública de defesa do Trabalho de Conclusão de Curso intitulada Um Breve Estudo Sobre Extensões de Corpos, sob orientação de Davidson Freitas Nogueira apresentada pelo aluno José Armando Oliveira Mendes (2019101221230096) do Curso Licenciatura em Matemática (Campus Urutaí). Os trabalhos foram iniciados às 15:02 pelo Professor Presidente da banca examinadora, constituída pelos seguintes membros:

- Davidson Freitas Nogueira (Orientador)
- Marcelo Bezerra Barboza (Examinador Externo)
- José Lucas Pereira Luiz (Examinador Externo)

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

[x] Aprovado [ ] Reprovado Nota: 9,2

Observação/ Apreciações:

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

Urutaí - GO, 13/12/2023

(Assinado Eletronicamente)
Davidson Freitas Nogueira
Orientador(a)

(Assinado Eletronicamente)
Marcelo Bezerra Barboza
Membro

(Assinado Eletronicamente)
José Lucas Pereira Luiz
Membro

Documento assinado eletronicamente por:
- José Lucas Pereira Luiz, José Lucas Pereira Luiz - Professor Avaliador de Banca - Instituto Federal do Norte de Minas Gerais – Ifnmg (10727655000543), em 13/12/2023 16:15:42.
- Marcelo Bezerra Barboza, Marcelo Bezerra Barboza - Professor Avaliador de Banca - Universidade Federal de Goiás (01567601000143), em 13/12/2023 16:13:47.
- Davidson Freitas Nogueira, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 13/12/2023 16:10:30.

Este documento foi emitido pelo SUAP em 12/12/2023. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 556804
Código de Autenticação: b8f696623b

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Formulário 1044/2023 - DE-UR/CMPURT/IFGOIANO

José Armando Oliveira Mendes

Um Breve Estudo Sobre Extensões de Corpos

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia Goiano–Campus Urutaí como requisito parcial para obtenção do titulo de Licenciada em Matemática, aprovado em 13 de dezembro de 2023, pela Banca Examinadora constituída pelos professores

(Assinado eletronicamente)
Prof. Dr. Davidson Freitas Nogueira
Instituto Federal Goiano - Campus Urutaí
Presidente da Banca (Orientador)

(Assinado eletronicamente)
Prof. Dr. Marcelo Bezerra Barboza
Instituto de Matemática e Estatística - UFG

(Assinado eletronicamente)
Prof. Dr. José Lucas Pereira Luiz
Instituto Federal do Norte de Minas Gerais - Campus Araçuaí

Documento assinado eletronicamente por:

- Marcelo Bezerra Barboza, Marcelo Bezerra Barboza - Professor Avaliador de Banca - Universidade Federal de Goiás (01567601000143), em 14/12/2023 17:52:59.
- José Lucas Pereira Luiz, José Lucas Pereira Luiz - Professor Avaliador de Banca - Instituto Federal do Norte de Minas Gerais – Ifnmg (10727655000543), em 14/12/2023 17:39:32.
- Davidson Freitas Nogueira, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 14/12/2023 17:06:57.

Este documento foi emitido pelo SUAP em 14/12/2023. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 558201
Código de Autenticação: 810ec618e1

AGRADECIMENTOS

Agradeço a Deus, pela vida com saúde.

Agradeço à minha família, em especial minha mãe, Rosimeire, e minhas tias, “Lena”, “Tê”, “Pá” e “Lú”, também o tio “Dé” e minha prima Marília, pelo apoio incondicional e incentivo constante durante a minha graduação, sem isso eu não conseguiria concluir o curso com a tranquilidade que estou agora.

Agradeço aos professores do IFGOIANO Campus Urutaí, por todos os ensinamentos e contribuições para a minha formação.

Agradeço ao meu orientador, Davidson Freitas, e meu coorientador, Dassael Fabrício, por terem acreditado no meu potencial e me guiado no decorrer do desenvolvimento deste trabalho. Na verdade, muito mais que isso, além de excelentes professores, foram grandes motivadores e incentivadores dos meus estudos. Gostaria também de agradecer aos avaliadores Marcelo Bezerra e José Lucas, por terem disponibilizado um tempinho para avaliar este trabalho.

Agradeço aos colegas de curso, por toda a vivência nesses anos. Em especial, agradeço três pessoinhas que se tornaram muito mais que colegas de curso: Ana Hellen, por todo cuidado empregado à minha pessoa, Danilo, pela sincera amizade, repleta de cafés e boas risadas, e Yara, pela compreensão e por toda a amizade construída para além das incontáveis horas de estudos (além dos enjoos constantes na minha cabeça).

Agradeço, finalmente, ao IFGOIANO Campus Urutaí, pela oportunidade de fazer o curso dos meus sonhos e conhecer todas essas pessoas.

RESUMO

Diante dos critérios estabelecidos por Évariste Galois para a solubilidade de equações algébricas por meio de radicais, o presente trabalho tem o objetivo de abordar de forma introdutória o conceito de extensões de corpos, que é fundamental para o desenvolvimento da teoria de Galois. Esse conceito será abordado por meio de propriedades e exemplos.

Palavras-chave:

Corpos. Extensões de corpos. Polinômios.

ABSTRACT

Given the criteria established by Évariste Galois for the solubility of algebraic equations through radicals, the present work aims to approach in an introductory way the concept of field extensions, which is fundamental for the development of the theory of Galois. This concept will be approached through properties and examples.

Key-words:

Fields. Fields Extensions. Polynomials.

LISTA DE SIMBOLOS

$[K : F]$ Grau de K sobre F

$\ker(\varphi)$ Kernel do morfismo φ

$\langle a \rangle$ Conjunto gerado por a

$\mathbb{C}$ Corpo dos números complexos

$\mathbb{N}$ Conjunto dos números naturais

$\mathbb{Q}$ Corpo dos números racionais

$\mathbb{R}$ Corpo dos números reais

$\mathbb{Z}$ Anel dos números inteiros

$\mathbb{Z}_p$ Corpo dos inteiros módulo p

$\partial f(X)$ Grau do polinômio $f(X)$

A/I Conjunto quociente de A pelo ideal I

$F(\alpha)$ Menor corpo que contém $F \cup \{\alpha\}$

$F(S)$ Menor corpo que contém F

$F[\alpha]$ Imagem de $F[X]$ por v_α

$F[X]$ Anel de polinômios sobre o corpo F

v_α Morfismo valoração

SUMÁRIO

INTRODUÇÃO

A busca por métodos de resolução de equações algébricas é algo de interesse desde a antiguidade. Há comprovações que os babilônios já conseguiam resolver uma equação quadrática completa utilizando apenas operações algébricas, que hoje conhecemos como adição e multiplicação.

No século XVI, com a resolução para uma equação de segundo grau já consolidada, os matemáticos se voltaram para as equações de grau maior ou igual a três. Foi Girolamo Cardano, em 1545, quem publicou a resolução para equações cúbicas e quárticas, em sua obra *Ars Magna*. Vale ressaltar, no entanto, que não foi ele o responsável pelo desenvolvimento de tais métodos de resolução, sendo Nicollo Tartaglia o criador da solução para as cúbicas e Ludovico Ferrari o responsável pelas quárticas.

A publicação de *Ars Magna* despertou a curiosidade dos matemáticos para um tipo de número até então desconhecido, o número complexo. Rafael Bombelli foi o primeiro a trabalhar e fazer importantes observações sobre as relações entre números complexos e a resolução de uma cúbica. Apesar de não ter sido tão útil na época, foi um ponta pé inicial para o desenvolvimento da teoria dos números complexos.

Após o desenvolvimento de métodos para a resolução das cúbicas e quárticas, no século XVI, os matemáticos naturalmente começaram a estudar as equações de grau cinco. No entanto, enquanto tentava resolver esse problema, Niels Henrik Abel acabou demonstrando exatamente o contrário, isto é, não há uma forma geral para se resolver uma equação algébrica de grau maior que quatro apenas utilizando operações algébricas explícitas sobre os seus coeficientes. Abel publicou sua demonstração para esse resultado em 1824, momento em que já havia uma demonstração esquecida e menos satisfatória para o mesmo, publicada em 1799 por Paolo Ruffini.

Dessa forma, o resultado ficou conhecido como teorema de Abel-Ruffini.

Apesar da impossibilidade de se resolver equações com grau maior que quatro por meio de radicais, o estudo sobre as equações algébricas não se encerrou aí. O trabalho de Évariste Galois, publicado em 1846 (12 anos após sua morte), estabeleceu condições para a solubilidade de uma equação algébrica por meio radicais, para isso, relacionou a teoria de grupos com a teoria de corpos. A saber, essas duas teorias constituem hoje o que chamamos de teoria de Galois.

É preciso mencionar que todas essas informações referentes a história da matemática aqui expostas podem ser encontradas em [1], [8] e [3].

Dada a relevância das extensões de corpos para o estudo da teoria de Galois, este trabalho tem o objetivo de abordar de forma introdutória o conceito de extensões de corpos, algumas propriedades e exemplos. A principal referência adotada para o desenvolvimento deste trabalho foi [2], sendo [4] e [7] leituras complementares.

No primeiro capítulo apresentamos conceitos e resultados sobre Anéis e Corpos, Anel de Polinômios e Espaços Vetoriais, os quais serão muito importantes para o desenvolvimento deste trabalho. Vale mencionar que nesse capítulo em particular estamos interessados apenas na existência dos resultados, sendo assim, guiaremos o leitor para que encontre as demonstrações de tais resultados em [2], [4], [5], [7], [6].

No segundo capítulo vamos fazer um primeiro contato com as extensões de corpos, através de exemplos e resultados. Também abordaremos o conceito de elementos algébricos e elementos transcendentes. Na sequência estudaremos o polinômio minimal relacionado a um elemento algébrico, o qual será um conceito extremamente importante no decorrer do texto. No último tópico do capítulo, estudaremos as extensões simples, mostraremos alguns isomorfismos e faremos algumas caracterizações para essas extensões, dependendo unicamente do fato de o elemento gerador da extensão ser algébrico ou transcendente.

No terceiro capítulo estudaremos extensões finitas, para tanto, vamos observar o conceito de extensão de corpos por meio do conceito de espaços vetoriais, isso nos fornecerá uma gama de novas ferramentas e um olhar diferente para as extensões de corpos. Demonstraremos alguns resultados e focaremos nas extensões chamadas de quadráticas, biquadráticas e aquelas do tipo $\mathbb{Q}(\sqrt[3]{a}, \sqrt{b})$.

CAPÍTULO 1

PRELIMINARES

1.1 Anéis e corpos

Nesta primeira seção vamos apresentar algumas definições sobre anéis e corpos e enunciaremos alguns resultados que serão importantes no decorrer deste trabalho.

Começamos definindo o que é um anel e alguns casos particulares do mesmo.

Definição 1.1.1. Um conjunto não vazio A é dito anel associativo (ou simplesmente anel) se em A são definidas duas operações, usualmente denominadas adição e multiplicação, denotadas por $+$ e $\cdot$, respectivamente, tais que para todo a, b e c em A:

1. $a+b \in A$
2. $a+b = b+a$
3. $(a+b)+c = a+(b+c)$
4. Existe um elemento $0 \in A$, tal que $a+0 = a$
5. Dado $a \in A$, existe um elemento $-a$, tal que $a+(-a) = 0$
6. $a \cdot b \in A$
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
8. $a \cdot (b+c) = a \cdot b + a \cdot c$
9. $(a+b) \cdot c = a \cdot c + b \cdot c$

Se existe um elemento $1 \in A$, tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in A$, então dizemos que A é um anel com unidade. Além disso, se a multiplicação é comutativa, isto é, $a \cdot b = b \cdot a$, para todo $a, b \in A$, dizemos que A é um anel comutativo.

De agora em diante nesta seção, a menos de menção contrária, os símbolos A e B denotarão anéis. Além disso, quando não houver dúvida quanto a operação de multiplicação, escreveremos simplesmente ab ao invés de $a \cdot b$.

Definição 1.1.2. Se A é comutativo e $a \in A$ é um elemento não nulo, dizemos que a é divisor de zero se existe um elemento não nulo $b \in A$, tal que $ab = 0$.

Definição 1.1.3. Dizemos que A é um domínio de integridade se A é comutativo e não possui divisores de zero.

Reservaremos o símbolo D para domínio de integridade nas definições e resultados seguintes.

Definição 1.1.4. Dizemos que A é um anel de divisão se para todo $a \in A \setminus \{0\}$ existe um elemento $a^{-1} \in A$, tal que $aa^{-1} = 1$, ou seja, todo elemento não nulo possui inverso.

Finalmente, a definição de corpo, a principal estrutura utilizada neste texto.

Definição 1.1.5. Definimos corpo como sendo um anel de divisão comutativo.

Proposição 1.1.6. *Todo corpo é um domínio de integridade.*

Demonstração. Ver [7, Observação 9.3.3]. □

Exemplo 1.1.7. *Se p é um número primo, então $\mathbb{Z}_p$, o anel de inteiros módulo p, é um corpo.*

Definição 1.1.8. Se existe um natural m, tal que $ma = 0$, para todo $a \in D$, então o menor natural n com essa propriedade é chamado de característica de D. Dizemos então que D tem característica finita igual a n. Caso contrário, dizemos que D tem característica zero.

A seguir temos algumas definições e resultados sobre morfismos de anéis.

Definição 1.1.9. Um homomorfismo (ou morfismo) de anéis é uma função $\varphi: A \to B$ que tem as seguintes propriedades: $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$ e $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2)$, para todo $a_1, a_2 \in A$.

Definição 1.1.10. Um isomorfismo $\varphi: A \to B$ é um morfismo bijetor. Neste caso, dizemos que A e B são isomorfos.

Definição 1.1.11. O kernel (ou núcleo) de um morfismo $\varphi: A \to B$ é o conjunto $\ker(\varphi) := \{a \in A;\ \varphi(a) = 0\}$

Vejamos um pouco agora sobre ideais de um anel.

Definição 1.1.12. Um conjunto $I \subseteq A$ é um ideal à esquerda de A se $a_1x_1 + a_2x_2 \in A$, para todo $a_1, a_2 \in A$ e $x_1, x_2 \in I$. Analogamente, definimos ideal à direita. Dizemos que um ideal é bilateral se é ideal à esquerda e à direita.

Proposição 1.1.13. *O kernel de um morfismo é um ideal bilateral.*

Demonstração. Considere o morfismo $\varphi: A \to B$ e vejamos que $\ker(\varphi) \subseteq A$ é um ideal de A. Dados $a_1, a_2 \in A$ e $x_1, x_2 \in \ker(\varphi)$, como φ é morfismo, temos que

$$\varphi(a_1x_1 + a_2x_2) = \varphi(a_1x_1) + \varphi(a_2x_2) = \varphi(a_1)\varphi(x_1) + \varphi(a_2)\varphi(x_2) \tag{1.1}$$

Além disso, como $x_1, x_2 \in \ker(\varphi)$, segue $\varphi(x_1) = \varphi(x_2) = 0$. Logo, de (1.1), segue que $\varphi(a_1x_1 + a_2x_2) = \varphi(a_1)0 + \varphi(a_2)0 = 0$. Sendo assim, $a_1x_1 + a_2x_2 \in \ker(\varphi)$, donde concluímos que $\ker(\varphi)$ é um ideal à esquerda de A. De maneira análoga, podemos mostrar que $\ker(\varphi)$ é um ideal à direita de A, o que conclui o resultado. □

Definição 1.1.14. Um ideal $I \neq A$ é dito maximal se, dado um ideal $J \subseteq A$, tem-se $I \subseteq J \Rightarrow J = I$ ou $J = A$.

Definição 1.1.15. Se $I \subseteq A$ é um ideal, então definimos o quociente de A por I como sendo o conjunto $A/I = \{a + I;\ a \in A\}$. Definimos também as seguintes operações nesse conjunto: $(a+I) + (b+I) = (a+b) + I$ e $(a+I)(b+I) = (ab) + I$, para todo $a, b \in A$.

Com as operações definidas acima, é fácil verificar que A/I é um anel. Disso, temos um dos principais resultados do estudo de morfismos, que é o seguinte.

Teorema 1.1.16. *(Teorema Fundamental do Homomorfismo) Se $\varphi: A \to B$ é um morfismo, então $A/\ker(\varphi)$ é isomorfo a $\varphi(A)$.*

Demonstração. Ver [2, Teorema 1.2.5]. □

Teorema 1.1.17. *Se A é comutativo com unidade e I é um ideal de A, então I é maximal se e só se A/I é corpo.*

Demonstração. Ver [4, Theorem 3.5.1]. □

Teorema 1.1.18. *Dado um domínio de integridade D, é possível construir o menor corpo $Frac(D)$ contendo D, o chamado corpo de frações de D. Na prática, esse corpo é gerado invertendo-se os seus elementos não nulos.*

Demonstração. Ver [2, Sezione 1.5]. □

Teorema 1.1.19. *Anéis isomorfos possuem corpos de frações isomorfos.*

Demonstração. Ver [2, Teorema 1.5.1]. □

Proposição 1.1.20. *Todo homomorfismo não nulo entre corpos é injetivo.*

Demonstração. Ver [2, Corollario 1.2.7]. □

A seguir temos dois tipos especiais de anéis.

Definição 1.1.21. Dizemos que um domínio de integridade D é um anel euclidiano se para todo $a \neq 0$ em D é possível definir um natural $d(a)$, tal que:

(1) se $a, b \in D$, ambos não nulos, então $d(a) \leq d(ab)$;

(2) se $a, b \in D$, ambos não nulos, então existem $q, r \in D$, tais que $a = bq + r$, onde $r = 0$ ou $d(r) < d(b)$.

Definição 1.1.22. Um domínio de integridade D com unidade é chamado de anel de ideais principais se todo ideal I de D é da forma $I := \langle x \rangle := \{ax,\ a \in D,\ x \in I\}$.

Alguns outros resultados sobre corpos que serão utilizados no inicio do próximo capítulo são os seguintes.

Definição 1.1.23. Se K é um corpo, a interseção de todos os subcorpos de K é um corpo e é chamado de subcorpo fundamental de K. Claramente, esse é o menor subcorpo de K. Denotamos por $\mathbb{K}$.

Proposição 1.1.24. *Se K é um corpo seu subcorpo fundamental é isomorfo a $\mathbb{Q}$ ou a $\mathbb{Z}_p$, para algum primo $p \geq 2$.*

Demonstração. Ver [2, Corollario 1.6.3]. □

Proposição 1.1.25. *Se dois corpos F e K são isomorfos, então eles tem a mesma característica.*

Demonstração. Ver [2, Corollario 3.1.2]. □

Para finalizar essa seção, não é difícil mostrar que dado um corpo, então todo subcorpo seu possui a mesma característica [2, Corollario 1.6.5]. Além disso, todo corpo numérico, isto é, subcorpo dos complexos, tem característica igual a zero [2, Esempio 1.6.6].

1.2 Anel de polinômios

Nesta seção iremos definir alguns conceitos importantes sobre polinômios. Além disso, enunciaremos resultados que serão necessários no decorrer do texto, para tanto, o símbolo F, a menos de menção contrária, denotará um corpo.

Começamos definindo o que é o anel de polinômios sobre um corpo F.

Definição 1.2.1. O anel de polinômios na indeterminada X com coeficientes em F é dado por

$$F[X] := \{a_0 + a_1X + \cdots + a_nX^n;\ n \in \mathbb{N},\ a_0, \ldots, a_n \in F\}$$

Definição 1.2.2. Um polinômio $f(X) \in F[X]$ é dito nulo se, e somente se os seus coeficientes são todos nulos. Nesse caso, denotamos $f(X) = 0$.

A seguir, faremos algumas definições básicas sobre igualdade e operações de polinômios.

Definição 1.2.3. Se $f(X) = a_0 + \cdots + a_nX^n \in F[X]$ e $g(X) = b_0 + \cdots + b_mX^m \in F[X]$, então $f(X) = g(X)$ se, e somente se $a_i = b_i$, para todo natural $i \geq 0$.

Definição 1.2.4. Se $f(X) = a_0 + \cdots + a_nX^n \in F[X]$ e $g(X) = b_0 + \cdots + b_mX^m \in F[X]$, com $m \geq n$ então $f(x) + g(X) = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \cdots + b_mX^m$.

Definição 1.2.5. Se $f(X) = a_0 + \cdots + a_nX^n \in F[X]$ e $g(X) = b_0 + \cdots + b_mX^m \in F[X]$, então $f(X)g(X) = (a_0b_0) + (a_0b_1 + a_1b_0)X + \cdots + \sum_{i+j=k}(a_ib_j)X^k + \cdots + (a_nb_m)X^{n+m}$.

Definiremos agora o que é o grau de um polinômio não nulo, e apresentaremos um resultado sobre o grau do produto entre dois polinômios não nulos.

Definição 1.2.6. Se $f(X) = a_0 + \cdots + a_nX^n \in F[X]$, com $a_n \neq 0$, então o grau de $p(X)$, denotado por $\partial f(X)$, é n.

Definição 1.2.7. *Se $f(X) \in F[X]$ é um polinômio com grau n, então dizemos que o a_n é o coeficiente diretor de $f(X)$.*

Definição 1.2.8. Um polinômio $f(X) \in F[X]$ com grau n é dito mônico se seu coeficiente diretor é um.

Proposição 1.2.9. *Se $f(X), g(X) \in F[X]$ são dois polinômios não nulos, então $\partial(f(X)g(X)) = \partial f(X) + \partial g(X)$.*

Demonstração. Ver [4, Lemma 3.9.1]. □

Em um anel de polinômios temos um algoritmo para divisão, com o seguinte resultado.

Lema 1.2.10. *Dados dois polinômios $f(X), g(X) \in F[X]$, com $g(X) \neq 0$, então existem dois únicos polinômios $q(X), r(X) \in F[X]$, tais que $f(X) = g(X)q(X) + r(X)$, onde $r(X) = 0$ ou $\partial r(X) < \partial g(X)$.*

Demonstração. Ver [2, Corollario 2.2.2]. □

Definição 1.2.11. Dados dois polinômios $f(X), g(X) \in F[X]$, dizemos que $g(X)$ divide $f(X)$ se existe um polinômio $h(X) \in F[X]$, tal que $f(X) = g(X)h(X)$.

Uma consequência imediata desse lema é que $F[X]$ é um anel euclidiano, além disso, é possível provar os seguintes resultados.

Exemplo 1.2.12. *$F[X]$ é um anel euclidiano.*

Teorema 1.2.13. *$F[X]$ é um anel de ideais principais. Isto é, se $I \subseteq F[X]$ é um ideal não nulo, então $I = \langle m(X) \rangle$, onde $m(x)$ é um polinômio de grau mínimo em I. Além disso, I possui um único gerador mônico.*

Demonstração. Ver [2, Teorema 2.2.4]. □

Lema 1.2.14. *Dois polinômios não nulos $f(X), g(X) \in F[X]$ sempre possuem máximo divisor comum. Mais precisamente, se $d(X) \in F[X]$ é o máximo divisor comum de $f(X)$ e $g(X)$, então existem $a(X), b(X) \in F[X]$, tais que $d(X) = a(X)f(X) + b(X)g(X)$.*

Demonstração. Ver [2, Corollario 2.2.5]. □

Chamamos a expressão acima de Identidade de Bezout. Falando em máximo divisor comum, a seguinte definição nos oferece uma correspondência do conceito já conhecido de número primo para o contexto de polinômios.

Definição 1.2.15. Um polinômio $f(X) \in F[X]$ é dito irredutível se ao escrever $f(X) = a(X)b(X)$, com $a(X), b(X) \in F[X]$, então ou $a(X)$ é constante, ou $b(X)$ é constate.

Também como esperado, a fatoração de um polinômio por polinômios irredutíveis é única.

Lema 1.2.16. *Se $f(X) \in F[X]$, então $f(X)$ pode ser escrito de forma única como produto de polinômios irredutíveis em $F[X]$.*

Demonstração. Ver [4, Lemma 3.9.5]. □

Lema 1.2.17. *Um ideal $\langle p(X) \rangle \subseteq F[X]$ é maximal se, e somente se $p(X)$ é irredutível.*

Demonstração. Ver [4, Lemma 3.9.6]. □

Proposição 1.2.18. *$F[X]/\langle m(X) \rangle$ é um corpo se, e somente se $m(X) \in F[X]$ é irredutível.*

Demonstração. Ver [2, Proposizione 2.2.9]. □

Retomando um conceito da seção anterior, agora temos condições de falar sobre um morfismo particularmente importante para o desenvolvimento deste trabalho, chamado de morfismo avaliação (ou valoração).

Exemplo 1.2.19. *Dados dois corpos F e K, com $F \subseteq K$, e $\alpha \in K$, então a função $v_\alpha : F[X] \to K$; $f(X) \mapsto f(\alpha)$ que pega um polinômio e leva em seu valor numérico em α é um morfismo*

Por fim, o seguinte corolário garante que $F[X]$ é um domínio de integridade. Sendo assim, de acordo com a proposição (1.1.18), conseguimos construir o corpo de frações desse conjunto, como no exemplo subsequente.

Exemplo 1.2.20. *$F[X]$ é um domínio de integridade.*

Exemplo 1.2.21. *O corpo de frações de $F[X]$ é chamado de corpo de funções racionais e denotado por* $F(X) := \left\{ \dfrac{f(X)}{g(X)};\ f(X), g(X) \in F[X],\ g(X) \neq 0 \right\}$.

1.3 Espaços vetoriais

Nesta seção iremos definir alguns conceitos importantes sobre espaços vetoriais. Também, enunciaremos resultados que serão utilizados no decorrer do texto.

Começamos com a definição de espaço e subespaço vetorial.

Definição 1.3.1. Um conjunto não vazio V é dito espaço vetorial sobre um corpo F se em V são definidas duas operações, usualmente denominadas adição e multiplicação por escalar, denotadas por $+$ e $\cdot$, respectivamente, tais que para todo $u, v, w \in V$ e $\alpha, \beta \in F$:

1. $u + v \in V$
2. $u + v = v + u$
3. $(u + v) + w = u + (v + w)$
4. Existe um elemento $0 \in V$, tal que $u + 0 = u$
5. Dado $u \in V$, existe um elemento $-u$, tal que $u + (-u) = 0$
6. $\alpha \cdot u \in V$
7. $\alpha \cdot (\beta \cdot u) = (\alpha \cdot \beta) \cdot u$
8. $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$
9. $(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$
10. $1_F \cdot u = u$

Podemos também dizer que V é um $F-$espaço vetorial. Além disso, os elementos de um espaço vetorial V são chamados de vetores e os elementos de F de escalares.

Definição 1.3.2. *Um subconjunto W de V é um subespaço vetorial de V se a restrição das operações de V a W torna esse conjunto um $F-$ espaço vetorial.*

Para as definições e resultados a seguir, o símbolo V, a menos de menção contrária, denotará um espaço vetorial sobre um corpo F.

Definição 1.3.3. Um vetor $v \in V$ é uma combinação linear dos vetores $v_1, \ldots, v_n \in V$ se existem escalares $\alpha_1, \ldots, \alpha_n \in F$ tais que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$.

Definição 1.3.4. Um subconjunto $S \subseteq V$ é gerador de V se todo elemento de V pode ser escrito como combinação linear dos vetores de S.

Definição 1.3.5. Um subconjunto $S \subseteq V$ é linearmente independente se dado $n \in \mathbb{N}$ e $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$, para cada $v_i \in S$ e $\alpha_i \in F$, com $i \in \{1, \ldots, n\}$, implica que $\alpha_i = 0$, para todo $i \in \{1, \ldots, n\}$. Dizemos que S é linearmente dependente se não for linearmente independente.

A seguinte definição é extremante importante para o estudo de espaços vetoriais e será muito utilizada no terceiro capítulo, bem como as definições e resultados subsequentes.

Definição 1.3.6. Um subconjunto $B \subseteq V$ é base de V se é linearmente independente e um conjunto gerador de V.

Definição 1.3.7. Dizemos que V é finitamente gerado se possuir um conjunto gerador finito.

Proposição 1.3.8. *Todas as bases de um espaço vetorial finitamente gerado possuem a mesma quantidade de elementos.*

Demonstração. Ver [6, Corolário 2.3.5]. □

Definição 1.3.9. Se V admite uma base finita, então chamamos a quantidade de elementos de tal base de dimensão de V. Caso contrário, dizemos que a dimensão de V é infinita.

Proposição 1.3.10. *Se V possui dimensão finita $n \geq 1$ e $B \subseteq V$ possui n elementos, então são equivalente as seguintes afirmações:*

(1) *B é base;*

(2) *B é um subconjunto linearmente independente maximal de V;* (3) *B é um subconjunto gerador minimal de V.*

Demonstração. Ver [5, pág. 44-45]. □

Teorema 1.3.11. *Todo espaço vetorial possui base.*

Demonstração. Ver [6, Apêncie 8]. □

Proposição 1.3.12. *Se W é um subespaço de V, e V tem dimensão finita, então W também tem dimensão finita.*

Demonstração. Ver [5, pág. 45]. □

Proposição 1.3.13. *Se V é finitamente gerado e B é linearmente independente, então existe uma base de V que contém B.*

Demonstração. Ver [5, pág. 46]. □

CAPÍTULO 2

EXTENSÕES DE CORPOS

2.1 Extensões de corpos

O principal conceito trabalhado no texto é o de extensão de corpos e para definir o que isso significa utilizaremos a proposição (1.1.20), a qual nos garante que todo homomorfismo não nulo entre corpos $\varphi : F \to K$ é injetivo, ou seja, conseguimos identificar, de maneira única, cada elemento de F como um elemento de K. Esse fato justifica a nossa primeira definição.

Definição 2.1.1. Dados dois corpos F e K, um homomorfismo não nulo $\varphi : F \to K$ é chamado de imersão de F em K.

Nesse caso, dizemos que F está imerso em K ou que K é uma extensão de F. Nesse sentido, identificamos o corpo F como sua imagem isomorfa em K e denotamos $F \subseteq K$. Se existe um corpo L satisfazendo $F \subseteq L \subseteq K$, então L é chamado de corpo intermediário da extensão $F \subseteq K$.

Uma forma interessante e útil de representar extensões de corpos é por meio de diagramas, podemos, por exemplo, representar as extensões $F \subseteq L \subseteq K$ através do seguinte diagrama.

$$\begin{array}{c} K \\ \uparrow \\ L \\ \uparrow \\ F \end{array}$$

Como primeiro exemplo, vejamos uma extensão bastante natural e que trabalha com dois corpos já muito conhecidos.

Exemplo 2.1.2. *O corpo dos números complexos é uma extensão do corpo dos números reais. Com efeito, basta observar que existe uma imersão de $\mathbb{R}$ em $\mathbb{C}$, da seguinte forma*

$$\begin{aligned} \varphi: \mathbb{R} &\to \mathbb{C} \\ \alpha &\mapsto \varphi(\alpha) = \alpha + 0i \end{aligned}$$

onde $i = \sqrt{-1}$ é a unidade imaginária.

Um outro exemplo de extensão de corpos é o seguinte.

Exemplo 2.1.3. *Se F é um corpo, então o corpo das funções racionais $F(X)$ é uma extensão de F. Com efeito, basta definir a imersão*

$$\begin{aligned} \varphi: F &\to F(X) \\ \alpha &\mapsto \varphi(\alpha) = \frac{\alpha}{1} \end{aligned}$$

onde α e 1 são os polinômios constantes $f(X) = \alpha$ e $g(X) = 1$, respectivamente.

O exemplo a seguir nos propicia uma informação valiosa de que todo corpo K é extensão do corpo dos números racionais ou do corpo dos inteiros módulo p, sendo necessário e suficiente analisar a sua característica.

Exemplo 2.1.4. *(i) Todo corpo K é extensão do seu subcorpo fundamental (Definição 1.1.23). Basta observar que K é trivialmente extensão de qualquer subcorpo de K, em particular, de seu subcorpo fundamental.*

(ii) K tem característica zero se, e somente se, $\mathbb{Q} \subseteq K$. Com efeito, por um lado, se fosse $\mathbb{Q} \subseteq K$ com a característica de K sendo diferente de zero, teríamos que a característica de $\mathbb{Q}$ também seria diferente de zero, o que é um absurdo. Logo, K também tem característica zero.

Por outro lado, suponha que K tem característica zero e denote por $\mathbb{K}$ o seu subcorpo fundamental, assim, $\mathbb{K}$ também tem característica zero. Pela proposição (1.1.24), $\mathbb{K}$ é isomorfo a $\mathbb{Q}$ ou a $\mathbb{Z}_p$. Nesse caso, como a característica de $\mathbb{Z}_p$ é p segue que $\mathbb{K}$ é isomorfo a $\mathbb{Q}$. Diante disso, existirão um isomorfismo $\varphi_1 : \mathbb{Q} \to \mathbb{K}$ e uma imersão $\varphi_2 : \mathbb{K} \to K$, o que possibilita definir a imersão $\varphi = \varphi_2 \circ \varphi_1 : \mathbb{Q} \to K$ e, portanto, $\mathbb{Q} \subseteq K$.

(iii) De maneira análoga ao item anterior, conseguimos provar que K tem característica finita igual a p, com $p \geq 2$ primo, se, e somente se, $\mathbb{Z}_p \subseteq K$.

(iv) Em particular, todo corpo numérico tem característica zero, sendo assim, pelo item (ii), é extensão de $\mathbb{Q}$. Ou seja, todo corpo numérico é extensão de $\mathbb{Q}$.

No decorrer do texto, estaremos interessados em estudar alguns casos particulares de extensões intermediárias, no seguinte sentido, se $F \subseteq K$ é uma extensão de corpos e $\alpha \in K$, vamos olhar para o menor intermediário da extensão $F \subseteq K$ que contém F e $\{\alpha\}$. Para generalizar essa ideia, note que se L é um subcorpo qualquer de K, então L será uma extensão de F e K será uma extensão de L, ou seja, $F \subseteq L \subseteq K$. Dessa forma, se S é um subconjunto não vazio de K, a interseção de todos os subcorpos de K que contêm S, que é um subcorpo de K, será um corpo intermediário da extensão $F \subseteq K$ e, evidentemente, é o menor subcorpo de K que contém S.

Definição 2.1.5. Seja $F \subseteq K$ uma extensão de corpos e S um subconjunto não vazio de K. Definimos a extensão de F em K gerada por S como sendo o menor subcorpo de K que contém $F \cup S$ e a denotaremos $F(S)$.

Para fixar as ideias, observe que, como $F(S)$ contém F e é um subcorpo de K, tem-se que $F \subseteq F(S) \subseteq K$, qualquer que seja $S \subseteq K$. A depender da cardinalidade do subconjunto S, podemos adequar a notação definida acima. Se $S = \{\alpha_1, \ldots, \alpha_n\}$ for finito, podemos escrever $F(S) := F(\alpha_1, \ldots, \alpha_n)$, em particular, se for unitário, digamos $S = \{\alpha\}$, escrevemos $F(S) := F(\alpha)$.

Algumas das extensões de particular interesse, como supramencionado, são aquelas em que $F(S) = K$, onde S é finito ou unitário. Para esses casos, temos a seguinte definição.

Definição 2.1.6. Dizemos que K é uma extensão finitamente gerada por F, se existem $\alpha_1, \ldots, \alpha_n \in K$, tais que $K = F(\alpha_1, \ldots, \alpha_n)$, nesse caso, chamamos $\alpha_1, \ldots, \alpha_n$ de geradores de K sobre F.

No caso em que $K = F(\alpha)$, dizemos que K é uma extensão simples de F gerada por α.

Exemplo 2.1.7. *Considerando K um corpo qualquer e $S = \{1_K\}$, o subcorpo de K gerado por S é o subcorpo fundamental de K. Além disso, para todo subconjunto S de K, o menor subcorpo de K que contém $S \cup \{1_K\}$ é o corpo $\mathbb{K}(S)$. De fato, para a primeira afirmação, devemos mostrar que o menor subcorpo de K que contém S é o subcorpo fundamental. Mas S está contido em todos os subcorpos de K e, sendo assim, estará na interseção desses subcorpos que, por definição, é o subcorpo fundamental de K.*

O exemplo a seguir nos dá uma condição necessária e suficiente para que o subcorpo de K gerado por S seja igual ao próprio F. Vale mencionar que resultados semelhantes a esse

aparecerão mais adiante no texto e serão de grande importância para o desenvolvimento de outros.

Exemplo 2.1.8. *Dada uma extensão $F \subseteq K$ e dois subconjuntos não vazios S e T de K, temos que*

(i) $F(S) \subseteq F(T)$ se, e somente se, $S \subseteq F(T)$. De fato, por um lado, considere que $F(S) \subseteq F(T)$ e tome $x \in S$. Segue que $x \in S \cup F$ e, portanto, $x \in F(S) \subseteq F(T)$. Por outro lado, se $S \subseteq F(T)$, então $F(S) \subseteq F(F(T)) = F(T)$, donde $F(S) \subseteq F(T)$.

(ii) Em particular, $F(S) = F$ se, e somente se, $S \subseteq F$. Com efeito, considerando $F(S) = F$ teremos que $S \subseteq F \cup S \subseteq F(S) = F$. Por outro lado, se $S \subseteq F$, então $F(S) \subseteq F(F) = F$, donde $F(S) \subseteq F$. Além disso, por definição, temos que $F \subseteq F(S)$. Portanto, $F(S) = F$.

Vamos agora fazer uma primeira caracterização para extensões finitamente geradas. Se $F \subseteq K$ é uma extensão de corpos, $\mathbf{X} = \{X_1, \ldots, X_n\}$ é um conjunto de n indeterminadas sobre K e $\alpha_1, \ldots, \alpha_n \in K$, posto $\alpha := (\alpha_1, \ldots, \alpha_n)$, indicamos $f(\alpha)$ como o valor do polinômio $f(\mathbf{X})$ calculado em α. A função avaliação

$$\begin{aligned} v_\alpha : F[\mathbf{X}] &\to K \\ f(\mathbf{X}) &\mapsto f(\alpha) \end{aligned}$$

é um homomorfismo de anéis com imagem

$$\begin{aligned} F[\alpha] := F[\alpha_1, \ldots, \alpha_n] &:= \{f(\alpha);\ f(\mathbf{X}) \in F[\mathbf{X}]\} \\ &= \left\{ \sum c_{k_1 \ldots k_n} \alpha_1^{k_1} \cdots \alpha_n^{k_n};\ c_{k_1,\ldots,k_n} \in F, k_i \in \mathbb{N} \right\} \end{aligned}$$

Nesses termos, temos o seguinte resultado.

Proposição 2.1.9. *Sejam $F \subseteq K$ uma extensão de corpos e $\alpha = (\alpha_1, \ldots, \alpha_n)$, com $\alpha_1, \ldots, \alpha_n \in K$. Então*

$$F(\alpha) = \left\{ f(\alpha) g(\alpha)^{-1};\ f(\mathbf{X}), g(\mathbf{X}) \in F[\mathbf{X}], g(\alpha) \neq 0 \right\}.$$

Além disso, para qualquer $S \subseteq K$, teremos que

$$F(S) = \bigcup \{ F(\alpha_{i_1}, \ldots, \alpha_{i_n}) : n \in \mathbb{N}, \alpha_{i_j} \in S, \forall j = 1, \ldots, n \}.$$

Demonstração. Considere o anel $F[\alpha]$ e note que $F \cup \{\alpha_1, \ldots, \alpha_n\} \subseteq F[\alpha]$, pois $F \subseteq F[\alpha]$ e $\alpha_i \in F[\alpha]$, para todo $i \in \{1, \ldots, n\}$. Vejamos agora que esse é o menor anel que contém $F \cup \{\alpha_1, \ldots, \alpha_n\}$, para isso, suponha que B seja um subanel de K que contém essa união. Pelo fato de as operações serem fechadas, temos que $F[\alpha] \subseteq B$, donde $F[\alpha]$ é o menor anel que contém $F \cup \{\alpha_1, \ldots, \alpha_n\}$. Sendo assim, o menor corpo que contém $F[\alpha]$ também será o menor corpo que contém $F \cup \{\alpha_1, \ldots, \alpha_n\}$. Pelo teorema (1.1.18), temos que esse corpo é o corpo de frações de $F[\alpha]$ em K, ou seja, o conjunto $\{f(\alpha)g(\alpha)^{-1};\ f(\mathbf{X}), g(\mathbf{X}) \in F[\mathbf{X}], g(\alpha) \neq 0\}$. Portanto,

$$F(\alpha) = \{f(\alpha)g(\alpha)^{-1};\ f(\mathbf{X}), g(\mathbf{X}) \in F[\mathbf{X}], g(\alpha) \neq 0\}$$

Além disso, dado $S \subseteq K$, note que, para quaisquer $\alpha_{i_j} \in S$, com $i_1, \ldots, i_n \in \mathbb{N}$, temos que $F(\alpha_{i_1}, \ldots, \alpha_{i_n}) \subseteq F(S)$. Logo

$$L := \bigcup \{F(\alpha_{i_1}, \ldots, \alpha_{i_n}) : n \in \mathbb{N}, \alpha_{i_j} \in S, \forall j = 1, \ldots, n\} \subseteq F(S)$$

Dado que $F \cup S \subseteq L$, pela minimalidade de $F(S)$, basta mostrar que L é um corpo. Para isso, se considerarmos $x, y \in L$, existirão $n, m \in \mathbb{N}$, $\alpha_{i_1}, \ldots, \alpha_{i_n}, \alpha_{j_1}, \ldots, \alpha_{j_m} \in S$, tais que

$$x \in F(\alpha_{i_1}, \ldots, \alpha_{i_n}) \ \text{ e } \ y \in F(\alpha_{j_1}, \ldots, \alpha_{j_m})$$

Donde

$$xy^{-1}, x - y \in F(\alpha_{i_1}, \ldots, \alpha_{i_n}, \alpha_{j_1}, \ldots, \alpha_{j_m}) \subseteq L$$

Portanto, L é corpo e está provado o resultado. □

Um caso particular das extensões finitamente geradas são aquelas geradas por um único elemento, como já denominamos, as extensões simples. Mais adiante, sob certas condições, iremos caracterizar algumas extensões simples, o que é de grande valia para o estudo de extensões de corpos, já que toda extensão finitamente gerada pode ser construída, por recursão, como um sequência finita de extensões simples. De fato, dados $n \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_n \in K$, para construir $F(\alpha_1, \ldots, \alpha_n)$ como uma sequência finita de extensões simples coloque

$$F_0 := F, \ \ F_i = F_{i-1}(\alpha_i), \ \ \text{para } i = 1, \ldots, n$$

o que resultará em

$$\begin{aligned} F \subseteq F_1 &= F(\alpha_1) \\ F \subseteq F_1 \subseteq F_2 &= F_1(\alpha_2) = F(\alpha_1)(\alpha_2) = F(\alpha_1, \alpha_2) \\ &\vdots \\ F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n &= F_{n-1}(\alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = F(\alpha_1, \ldots, \alpha_n) \end{aligned}$$

Observe que, pelas propriedades das operações em K, essa construção independe da ordem de escolha dos α_i.

O exemplo a seguir ilustra uma extensão simples gerada por um elemento α que não pertence ao corpo de partida da extensão, no entanto, seu quadrado pertence. Esse tipo de extensão será estudada da sessão (3.2) e, a saber, é chamada de extensão quadrática.

Exemplo 2.1.10. *Seja F um corpo numérico e seja $\alpha \in \mathbb{C}\backslash F$, tal que $\alpha^2 \in F$. Então, a extensão simples de F em $\mathbb{C}$ gerada por α é*

$$F(\alpha) = \{a + b\alpha;\ a, b \in F\}$$

Com efeito, é claro que $E := \{a+b\alpha;\ a,b \in F\} \subseteq F(\alpha)$ e que $F \cup \{\alpha\} \in E$ e, sendo assim, pela minimalidade de $F(\alpha)$, basta mostrar que E é um corpo. Para isso, considere $x, y \in E$, então, existem $a_1, a_2, b_1, b_2 \in F$, tais que

$$x = a_1 + b_1\alpha \ \ e \ \ y = a_2 + b_2\alpha$$

Note que $-y = -a_2 - b_2\alpha$ e que $y^{-1} = \dfrac{a_2 - b_2\alpha}{a_2^2 - b_2^2\alpha^2}$. Com isso,

$$x - y = a_1 + b_1\alpha - a_2 - b_2\alpha = (a_1 - a_2) + (b_1 - b_2)\alpha \in E$$

e

$$xy^{-1} = (a_1 + b_1\alpha)\left(\frac{a_2 - b_2\alpha}{a_2^2 - b_2^2\alpha^2}\right) = \frac{a_1a_2 - b_1b_2\alpha^2}{a_2^2 - b_2^2\alpha^2} - \frac{b_1a_2 - a_1b_2}{a_2^2 - b_2^2\alpha^2}\alpha \in E.$$

Logo, E é corpo e segue o resultado.

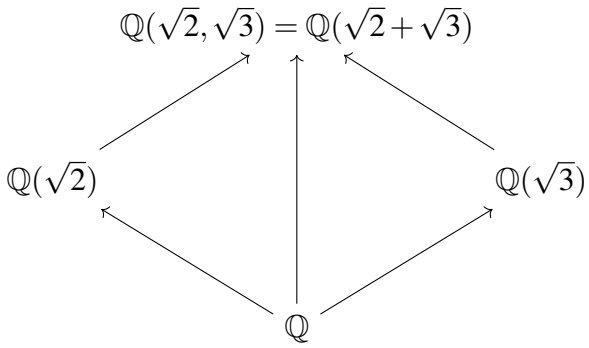
A partir do exemplo anterior, conseguimos outra forma de enxergar $\mathbb{C}$ como uma extensão de $\mathbb{R}$, basta observar que a unidade imaginária $i \in \mathbb{C}\backslash\mathbb{R}$ é tal que $i^2 := -1 \in \mathbb{R}$, como segue.

Exemplo 2.1.11. *O corpo $\mathbb{C}$ é uma extensão simples de $\mathbb{R}$. De fato, nas condições do exemplo anterior, temos*

$$\mathbb{C} = \{a + bi;\ a, b \in \mathbb{R}, i = \sqrt{-1}\} = \mathbb{R}(i)$$

Para o próximo exemplo, tomaremos uma extensão finitamente gerada por dois elementos e iremos contruí-la a partir de uma extensão simples.

Exemplo 2.1.12. *A extensão $\mathbb{Q}(\sqrt{2},\sqrt{3})$ pode ser vista como uma extensão simples de $\mathbb{Q}$ gerada por $\sqrt{2}+\sqrt{3}$, ou seja, $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. O seguinte diagrama representa essas extensões.*



Vejamos, primeiramente, que

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = F(\sqrt{3}), \quad \text{onde } F := \mathbb{Q}(\sqrt{2}).$$

De fato, pelo exemplo (2.1.10), temos $F = \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2};\ a,b \in \mathbb{Q}\}$. Agora, note que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ pois, caso contrário, existiriam $a,b \in \mathbb{Q}$, tais que

$$\begin{aligned} \sqrt{3} = a + b\sqrt{2} &\Rightarrow 3 = a^2 + 2ab\sqrt{2} + 2b^2 \\ &\Rightarrow \sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab}, \end{aligned}$$

o que significaria $\sqrt{2}$ ser racional, o que é uma contradição. Com isso, $\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2},\sqrt{3})$ e resulta

$$\begin{aligned} \mathbb{Q}(\sqrt{2},\sqrt{3}) = F(\sqrt{3}) &= \{a' + b'\sqrt{3};\ a',b' \in F\} \\ &= \{a_1 + a_2\sqrt{2} + (b_1 + b_2\sqrt{2})\sqrt{3};\ a_1,a_2,b_1,b_2 \in \mathbb{Q}\} \\ &= \{a_1 + a_2\sqrt{2} + b_1\sqrt{3} + b_2\sqrt{2}\sqrt{3};\ a_1,a_2,b_1,b_2 \in \mathbb{Q}\} \end{aligned}$$

A mesma conclusão poderia ser obtida considerando primeiro

$$F' := \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3};\ a,b \in \mathbb{Q}\}$$

e, de maneira análoga, teríamos

$$\begin{aligned} \mathbb{Q}(\sqrt{2},\sqrt{3}) = F'(\sqrt{2}) &= \{a' + b'\sqrt{2};\ a',b' \in F'\} \\ &= \{a_1 + a_2\sqrt{3} + (b_1 + b_2\sqrt{3})\sqrt{2};\ a_1,a_2,b_1,b_2 \in \mathbb{Q}\} \\ &= \{a_1 + a_2\sqrt{3} + b_1\sqrt{2} + b_2\sqrt{3}\sqrt{2};\ a_1,a_2,b_1,b_2 \in \mathbb{Q}\} \end{aligned}$$

O que foi feito é perceber que $\mathbb{Q}(\sqrt{2},\sqrt{3})$ pode ser construído através de sucessivas extensões simples. Vejamos agora que

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha); \;\; \alpha := \sqrt{2}+\sqrt{3}.$$

Por um lado, claro que $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. Por outro lado, temos que

$$\begin{aligned} \alpha = \sqrt{2}+\sqrt{3} \;\; &\Rightarrow \;\; \sqrt{2} = \alpha - \sqrt{3} \\ &\Rightarrow \;\; 2 = (\alpha-\sqrt{3})^2 = \alpha^2 - 2\alpha\sqrt{3} + 3, \end{aligned}$$

donde $\sqrt{3} = \dfrac{\alpha^2+1}{2\alpha} \in \mathbb{Q}(\alpha)$ e, de forma análoga, também temos que $\sqrt{2} = \dfrac{\alpha^2+1}{2\alpha} \in \mathbb{Q}(\alpha)$. Isso implica que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)$ e $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\alpha)$. Portanto, $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$, o que conclui o resultado.

Para finalizar esse exemplo, note que $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$ e $(\sqrt{2})^2 \in \mathbb{Q}$. Como adiantamos, extensões dessa forma serão chamadas de quadráticas, assim como $\mathbb{Q}(\sqrt{3})$. Já a extensão $\mathbb{Q}(\sqrt{2},\sqrt{3})$ será chamada de biquadrática, a qual estudaremos, de forma geral, na sessão (3.3).

Exemplo 2.1.13. *Se F é um corpo e $f(X) = c_0 + c_1X + \cdots + c_nX^n \in F[X]$, o menor subcorpo de F que contém os coeficientes de $f(X)$ é o corpo $\mathbb{F}(c_0,\ldots,c_n)$, onde $\mathbb{F}$ é o subcorpo fundamental de F (pelo exemplo (2.1.7), o resultado é imediato). Esse corpo é chamado corpo de definição (ou de racionalidade) de $f(X)$. Por exemplo, o corpo de definição do polinômio $X^5+\sqrt{3}X^2+\sqrt{2}+1$ é o corpo $\mathbb{Q}(\sqrt{2},\sqrt{3})$.*

2.2 Elementos algébricos e elementos transcendentes

Relembre que, se $F \subseteq K$ é uma extensão de corpos e $\alpha \in K$, a extensão de F em K gerada por α é dada por

$$F(\alpha) = \{f(\alpha)g(\alpha)^{-1}; f(X), g(X) \in F[X], g(\alpha) \neq 0\}$$

Para construir essa extensão é necessário dizer se α é ou não raiz de algum polinômio não nulo em $F[X]$.

Definição 2.2.1. Seja $F \subseteq K$ uma extensão de corpos e $\alpha \in K$. Dizemos que α é algébrico sobre F se é raiz de algum polinômio não nulo com coeficientes em F. Caso contrário, dizemos que α é transcendente sobre F.

Em outras palavras, dizemos que $\alpha \in K$ é algébrico sobre F se existe um polinômio não nulo $p(X) \in F[X]$, tal que $p(\alpha) = 0$. Um simples exemplo para ilustrar essa definição é o seguinte.

Exemplo 2.2.2. *Todo elemento $\alpha \in F$ é algébrico sobre F e para ver isso basta observar que α é raiz do polinômio $X - \alpha \in F[X]$.*

Considerando as extensões $F \subseteq L \subseteq K$, o exemplo a seguir mostra que um elemento $\alpha \in K$ algébrico sobre F também será algébrico sobre L.

Exemplo 2.2.3. *Se L é um corpo intermediário da extensão $F \subseteq K$ e $\alpha \in K$ é um elemento algébrico sobre F, então α também é algébrico sobre L. De fato, se α é algébrico sobre F, existe $f(X) = a_0 + a_1X + \cdots + a_nX \in F[X]$ não nulo, tal que $f(\alpha) = 0$. Mas $a_0, a_1, \ldots, a_n \in F$ implica que $a_0, a_1, \ldots, a_n \in L$, já que $F \subseteq L$. Sendo assim, α também anula um polinômio com coeficientes em L, logo, é algébrico sobre L.*

Por outro lado, o fato de α ser algébrico sobre L não implica que será algébrico sobre F, segue um contra exemplo.

Exemplo 2.2.4. *Considere as extensões $\mathbb{Q} \subseteq \mathbb{Q}(\pi) \subseteq \mathbb{R}$. Do exemplo (2.2.2), temos que π é algébrico sobre $\mathbb{Q}(\pi)$, no entanto, π é transcendente sobre $\mathbb{Q}$, veja a demonstração desse fato em [2, Corollario 3.3.9].*

2.3 Polinômio minimal de um elemento algébrico

Nesta seção, vamos estudar as relações entre um elemento algébrico e os polinômios que o tem como raiz. Começamos considerando uma extensão de corpos $F \subseteq K$. Para dizer se um elemento $\alpha \in K$ é algébrico ou transcendente sobre F, podemos estudar o homomorfismo avaliação

$$\begin{aligned} v_\alpha : F[X] &\to K \\ f(X) &\mapsto f(\alpha) \end{aligned}$$

Perceba que o núcleo de v_α é dado por $\ker(v_\alpha) = \{f(X) \in F[X];\ f(\alpha) = 0\}$, esse é, precisamente, o ideal de $F[X]$ constituído dos polinômios que se anulam em α. Portanto, α é algébrico sobre F se, e somente se, $I_\alpha := \ker(v_\alpha)$ é um ideal não nulo de $F[X]$. Com efeito, se α é algébrico sobre F, existe um polinômio não nulo $f(X) \in F[X]$, tal que $f(\alpha) = 0$, ou seja, $f(X) \in I_\alpha$ e, portanto,

I_α é um ideal não nulo de $F[X]$. Por outro lado, se I_α é um ideal não nulo de $F[X]$, existe um polinômio não nulo em $F[X]$ que se anula em α, ou seja, α é algébrico sobre F.

Nesse caso, como $F[X]$ é um anel de ideais principais, temos que $I_\alpha = \langle m(X) \rangle$, onde $m(X)$ é o único polinômio mônico de grau mínimo em I_α, como garante o teorema (1.2.13). Atribuiremos um nome especial para esse polinômio.

Definição 2.3.1. Seja $F \subseteq K$ uma extensão de corpos e $\alpha \in K$ um elemento algébrico sobre F. O polinômio mônico e de grau mínimo em $F[X]$ que se anula em α é chamado de polinômio minimal de α sobre F. O elemento α é dito algébrico de grau n se o seu polinômio minimal é de grau n.

Antes de demonstrarmos a primeira proposição desta seção, observe que se $p(X) \in F[X]$ é um polinômio não nulo tal que $p(\alpha) = 0$, então $p(X) \in I_\alpha = \langle m(X) \rangle$, ou seja, existe um polinômio $q(X) \in F[X]$, tal que $p(X) = m(X)q(X)$. Em outros termos, podemos dizer que o polinômio minimal de α divide todo polinômio que se anula em α. Na proposição a seguir, mostraremos que é necessário e suficiente que esse polinômio $p(X)$ seja mônico e irredutível para que seja o polinômio minimal de α.

Proposição 2.3.2. *Sejam $F \subseteq K$ uma extensão de corpos, $\alpha \in K$ e $p(X) \in F[X]$ um polinômio não nulo que se anula em α. Então $p(X)$ é o polinômio minimal de α sobre F se, e somente se, $p(X)$ é mônico e irredutível sobre F.*

Demonstração. Por um lado, considere que $m(X)$ é o polinômio minimal de α sobre F. Por definição, $m(X)$ é mônico, devemos então mostrar que é irredutível, isto é, não pode ser escrito como produto de dois polinômios, ambos com grau maior que zero. Suponha, por absurdo, que existem $g(X), h(X) \in F[X]$, com $\partial g(X), \partial h(X) > 0$, tais que

$$m(X) = g(X)h(X) \tag{2.1}$$

onde, $\partial g(X), \partial h(X) < \partial m(X)$. De (2.1) segue que $0 = m(\alpha) = g(\alpha)h(\alpha)$. Como $g(\alpha), h(\alpha) \in K$ e K é corpo, temos que $g(\alpha) = 0$ ou $h(\alpha) = 0$. Se $g(\alpha) = 0$, teremos uma contradição. Com efeito, se $g(X)$ for mônico, estamos contradizendo a minimalidade do grau de $m(X)$. Caso contrário, podemos criar o polinômio $qg(X)$, onde q é o inverso do coeficiente diretor de $g(X)$, dessa forma, $qg(X)$ será mônico e terá grau menor que o grau de $m(X)$, o que nos leva a mesma contradição. A demonstração segue de maneira análogo no caso em que $h(\alpha) = 0$. Portanto, $m(X)$ é irredutível.

Reciprocamente, seja $m(X)$ o polinômio minimal de α sobre F, considere que $p(X)$ é um polinômio mônico e irredutível que se anula em α e vejamos que $p(X) = m(X)$. Como $p(\alpha) = 0$, temos que $p(X) = m(X)h(X)$, para algum $h(X) \in F[X]$. Como $p(X)$ é irredutível e $\partial m(X) \geq 1$, temos que $\partial h(X) = 0$ e, pela proposição (1.2.9), devemos ter

$$\partial p(X) = \partial m(X) + \partial h(X) \Rightarrow \partial p(X) = \partial m(X)$$

Assim, $h(X) := h \in F$ e $p(X) = m(X)h$. Do fato de que $p(X)$ e $m(X)$ são mônicos, segue que $h = 1$. Portanto, $p(X) = m(X)$. □

Podemos agora incrementar o comentário feito antes dessa proposição, se $p(X) \in F[X]$ é um polinômio não nulo que se anula em α, vimos que o polinômio minimal de α sobre F divide $p(X)$, a partir da proposição, podemos concluir que $m(X)$ não só divide $p(X)$, como também é um fator mônico e irredutível de $p(X)$.

Os dois próximos exemplos, apesar de muito simples, serão de suma importância para resultados que faremos posteriormente.

Exemplo 2.3.3. *Seja $F \subseteq K$ uma extensão de corpos. Um elemento $\alpha \in K$ é algébrico de grau um sobre F se, e somente se, $\alpha \in F$. De fato, se α é algébrico de grau um sobre F, então existe um polinômio $f(X) = X + a \in F[X]$ que se anula em α, isto é, $f(\alpha) = \alpha + a = 0$, donde $\alpha = -a \in F$. Por outro lado, se $\alpha \in F$, basta observar que α é raiz do polinômio mônico e irredutível $f(X) = X - \alpha \in F[X]$. Logo, é algébrico de grau um sobre F.*

Exemplo 2.3.4. *Seja $F \subseteq K$ uma extensão de corpos e $\alpha \in K \backslash F$. Como consequência imediata do exemplo anterior, se $\alpha \notin F$, então α tem no mínimo grau dois sobre F. Sendo assim, basta que α seja raiz de um polinômio quadrático com coeficientes em F para que tenha grau dois sobre F.*

Façamos agora um exemplo mais prático.

Exemplo 2.3.5. *Todo número complexo não real tem grau dois sobre $\mathbb{R}$. Com efeito, $\alpha := a + bi \in \mathbb{C}$, com $b \neq 0$, é raiz do polinômio*

$$f(X) \quad = \quad X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha} = X^2 - (2a)X + (a^2 + b^2) \in \mathbb{R}[X]$$

De fato,

$$\begin{aligned} f(\alpha) &= f(a+bi) \\ &= (a+bi)^2 - 2a(a+bi) + a^2 + b^2 \\ &= a^2 + 2abi - b^2 - 2a^2 - 2abi + a^2 + b^2 \\ &= 2a^2 - 2a^2 + 2abi - 2abi - b^2 + b^2 \\ &= 0 \end{aligned}$$

Um resultado já esperado é que o grau de um elemento algébrico não é único, ele pode variar de acordo com o corpo sobre o qual ele é algébrico. O exemplo a seguir ilustra essa afirmação.

Exemplo 2.3.6. *O número $\alpha := \sqrt{2}+\sqrt{3}$ tem grau 2 sobre $\mathbb{Q}(\sqrt{2})$ e grau 4 sobre $\mathbb{Q}$. Para mostrar esse exemplo, observe que $\alpha \notin \mathbb{Q}(\sqrt{2})$, caso contrário, pelo exemplo (2.1.10), existiriam $a,b \in \mathbb{Q}$, tais que*

$$\alpha = \sqrt{2}+\sqrt{3} = a + b\sqrt{2} \Rightarrow \sqrt{3} = a + (b-1)\sqrt{2}$$

Como $a,(b-1) \in \mathbb{Q}$, isso implica que $\sqrt{3} = a+(b-1)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, o que é um absurdo, pois, pelo exemplo (2.1.12), $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Com isso, pelo exemplo (2.3.3), α tem pelo menos grau dois sobre $\mathbb{Q}(\sqrt{2})$. Basta agora construir um polinômio de grau dois que se anula em α. Observe que

$$\begin{aligned} \alpha = \sqrt{2}+\sqrt{3} &\Rightarrow \sqrt{3} = \alpha - \sqrt{2} \\ &\Rightarrow 3 = \alpha^2 - 2\alpha\sqrt{2} + 2 \\ &\Rightarrow \alpha^2 - 2\sqrt{2}\alpha - 1 = 0 \end{aligned}$$

Como $1, -2\sqrt{2}, -1 \in \mathbb{Q}(\sqrt{2})$, segue que α é raiz do polinômio quadrático

$$f(X) = X^2 - 2\sqrt{2}X - 1 \in \mathbb{Q}(\sqrt{2})[X]$$

Vejamos agora que α tem grau quatro sobre $\mathbb{Q}$. Para isso, note que

$$\begin{aligned} \alpha^2 - 2\sqrt{2}\alpha - 1 = 0 &\Rightarrow 2\sqrt{2}\alpha = \alpha^2 - 1 \\ &\Rightarrow 4 \cdot 2\alpha^2 = \alpha^4 - 2\alpha^2 + 1 \\ &\Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0 \end{aligned}$$

Como $1, -10 \in \mathbb{Q}$*, segue que* α *é raíz do polinômio de grau 4*

$$f(X) = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$$

Observe que esse polinômio é mônico, assim, para mostrar que ele é o polinômio minimal de α *sobre* $\mathbb{Q}$*, basta mostrar que ele é irredutível sobre* $\mathbb{Q}$ *(proposição (2.3.2)). Começamos verificando que ele não possui raízes racionais, para isso, considerando* $Y = X^2$ *e calculando as raízes, temos*

$$\begin{aligned} Y^2 - 10Y + 1 = 0 \quad &\Rightarrow \quad Y = \frac{10 \pm \sqrt{100-4}}{2} \\ &\Rightarrow \quad Y = \frac{10 \pm 4\sqrt{6}}{2} \\ &\Rightarrow \quad Y = 5 \pm 2\sqrt{6} \end{aligned}$$

Fazendo $Y = 5 \pm 2\sqrt{6}$ *em* $Y = X^2$*, segue que*

$$X^2 = 5 \pm 2\sqrt{6} \Rightarrow X = \pm\sqrt{5 \pm 2\sqrt{6}}$$

Donde as raízes são $X_1 = \sqrt{5+2\sqrt{6}}$*,* $X_2 = \sqrt{5-2\sqrt{6}}$*,* $X_3 = -\sqrt{5+2\sqrt{6}}$ *e* $X_4 = -\sqrt{5-2\sqrt{6}}$*, todas não racionais. Dessa forma,* $f(X)$ *não possui fatores de grau um sobre* $\mathbb{Q}$*, consequentemente, não terá nenhum de grau três. Verificaremos agora que* $f(X)$ *não tem fatores de segundo grau com coeficientes em* $\mathbb{Q}$*. Observe que*

$$\begin{aligned} f(X) &= X^4 - 10X^2 + 1 \\ &= (X^2)^2 - 2 \cdot 5X^2 + 25 - 24 \\ &= (X^2 - 5)^2 - (\sqrt{24})^2 \\ &= (X^2 - 5 - \sqrt{24})(X^2 - 5 + \sqrt{24}) \\ &= (X^2 - 5 - 2\sqrt{6})(X^2 - 5 + 2\sqrt{6}) \end{aligned}$$

Observamos que os polinômios $(X^2 - 5 - 2\sqrt{6})$ *e* $(X^2 - 5 + 2\sqrt{6})$ *não têm todos os coeficientes em* $\mathbb{Q}$*. Portanto,* $f(X) = X^4 - 10X^2 + 1$ *é irredutível sobre* $\mathbb{Q}$*, o que conclui o exemplo.*

2.4 Extensões simples

Agora temos condições suficientes para caracterizar extensões simples $F(\alpha)$, dependendo unicamente do fato de α ser algébrico ou transcendente sobre F. Faremos essa caracterização com o próximo teorema. Antes disso, relembre que na seção anterior mostramos que α é

algébrico sobre F se, e somente se, $\ker(v_\alpha)$ é não nulo, nesse caso, $\ker(v_\alpha) = \langle m(X)\rangle$, onde $m(X)$ é o polinômio minimal de α sobre F.

Teorema 2.4.1. *Seja $F \subseteq K$ uma extensão de corpos e $\alpha \in K$. Então:*

(a) Se α é transcendente sobre F, então $F(\alpha)$ é isomorfo a $F(X)$.

(b) Se α é algébrico sobre F, então $F(\alpha) = F[\alpha]$.

Demonstração. Para fazer a demonstração do teorema, utilizaremos o homomorfismo

$$v_\alpha : F[X] \to K; \quad f(X) \mapsto f(\alpha)$$

cuja imagem é dada por $v_\alpha(F[X]) = F[\alpha]$.

(a) Se α é transcendente sobre F, então $\ker(v_\alpha)$ é nulo. Donde v_α é injetiva. Com isso, temos que

$$v_\alpha : F[X] \to F[\alpha]$$

é um isomorfismo. Como $F[X]$ é isomorfo a $F[\alpha]$, então, pelo teorema (1.1.19) os seus respectivos corpos de frações também são isomorfos, isto é, $F(X)$ é isomorfo a $F(\alpha)$.

(b) Sendo α algébrico sobre F com polinômio minimal $m(X)$, temos que $\ker(v_\alpha) = \langle m(X)\rangle$ é não nulo. Pelo teorema (1.1.16), temos que a aplicação

$$v_\alpha : F[X]/\langle m(X)\rangle \to F[\alpha]$$

é um isomorfismo. Pela proposição (2.3.2), $m(X)$ é irredutível, logo, de acordo com a proposição (1.2.18), segue que $F[X]/\langle m(X)\rangle$ é um corpo, sendo assim, $F[\alpha] \subseteq F(\alpha)$ também é um corpo. Logo, pela minimalidade de $F(\alpha)$, temos que $F[\alpha] = F(\alpha)$.

□

Com esse teorema em mãos, podemos demonstrar uma nova caracterização para extensões simples geradas por um elemento algébrico.

Corolário 2.4.2. *Seja $F \subseteq K$ uma extensão de corpos e $\alpha \in K$. Então α é algébrico sobre F se, e somente se, $F[\alpha] = F(\alpha)$. Nesse caso,*

$$F(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1};\ c_0, \ldots, c_{n-1} \in F\}$$

onde n é o grau de α sobre F.

Demonstração. Se α é algébrico sobre F, então $F[\alpha] = F(\alpha)$, pelo teorema anterior. Por outro lado, considere $F[\alpha] = F(\alpha)$ e suponha, por absurdo, que α é transcendente sobre F. Como $F[\alpha] = F(\alpha)$, temos que $F[\alpha]$ é um corpo. No entanto, vimos na demonstração do teorema anterior que $F[\alpha]$ é isomorfo a $F[X]$, que não é um corpo. Sendo assim, $F[\alpha]$ não pode ser um corpo, o que contradiz a igualdade $F[\alpha] = F(\alpha)$. Portanto, α deve ser algébrico sobre F.

Para a segunda parte, considere que α seja algébrico de grau n com polinômio minimal $m(X)$. Assim, pelo algoritmo da divisão euclidiana, qualquer que seja $f(X) \in F[X]$ não nulo, existem $q(X), r(X) \in F[X]$, com $\partial r(X) = 0$ ou $\partial r(X) < \partial m(X)$, tais que $f(X) = m(X)q(X) + r(X)$. Aplicando em α, segue que $f(\alpha) = m(\alpha)q(\alpha) + r(\alpha)$, como $m(X)$ é o polinômio minimal de α, temos que $m(\alpha) = 0$, então $f(\alpha) = r(\alpha)$. Portanto,

$$\begin{aligned} F(\alpha) = F[\alpha] &= \{f(\alpha) \in K;\ f(X) \in F[X]\} \\ &= \{r(\alpha) \in K;\ r(X) \in F[X], \partial r(X) = 0 \text{ ou } \partial r(X) < \partial m(X)\} \\ &= \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1};\ c_0, c_1, \ldots, c_{n-1} \in F\} \end{aligned}$$

O que conclui o resultado. □

Esse corolário será uma grande motivação para a seção seguinte, mas, antes disso, vejamos uma aplicação bem interessante para ele nos dois próximos exemplos.

Exemplo 2.4.3. *Seja α um elemento algébrico de grau n sobre F com polinômio minimal $m(X)$. O inverso de um elemento não nulo $\beta \in F(\alpha)$ pode ser determinado com o algoritmo da divisão euclidiana. Com efeito, dado $\beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \in F(\alpha)$, temos o seu respectivo polinômio $r(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in F[X]$, isto é, $r(\alpha) = \beta$. Pela proposição (2.3.2), $m(X)$ é irredutível sobre F, além disso, o grau de $r(X)$ é menor que o grau de $m(X)$, sendo assim, $m(X)$ e $r(X)$ são coprimos. Disso, pela identidade de Bezout (1.2.14), existem $g(X), h(X) \in F[X]$, tais que $r(X)g(X) + m(X)h(X) = 1$. Aplicando em α e sabendo que $m(\alpha) = 0$, segue que $r(\alpha)g(\alpha) = 1$, ou seja, $\beta g(\alpha) = 1$. Portanto, $g(\alpha)$ é o inverso de β.*

Exemplo 2.4.4. *Vamos determinar o inverso racionalizado de $\beta = \sqrt{2} + \sqrt{3} + 1$. Observe que $\beta \in \mathbb{Q}(\alpha)$, onde $\alpha := \sqrt{2} + \sqrt{3}$, como vimos no exemplo (2.3.6), o polinômio minimal de $\alpha := \sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$ é $m(X) = X^4 - 10X^2 + 1$, que tem grau quatro. Pelo corolário anterior, temos que $\mathbb{Q}(\alpha) = \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3;\ c_1, c_2, c_3 \in \mathbb{Q}\}$, além disso, de acordo com o exemplo acima, vamos considerar o respectivo polinômio de β, ou seja, $r(X) = X + 1$. Ao dividir o polinômio minimal $m(X)$ por $r(X)$, obtemos*

$$X^4 - 10X^2 + 1 = (X+1)(X^3 - X^2 - 9X + 9) - 8 \Rightarrow m(X) = r(X)(X^3 - X^2 - 9X + 9) - 8$$

Aplicando em α, segue

$$\begin{aligned} m(\alpha) &= r(\alpha)(\alpha^3-\alpha^2-9\alpha+9)-8 \\ 8 &= \beta(\alpha^3-\alpha^2-9\alpha+9) \\ 1 &= \beta\frac{(\alpha^3-\alpha^2-9\alpha+9)}{8} \end{aligned}$$

Portanto, o inverso racionalizado de $\beta=\sqrt{2}+\sqrt{3}+1$ é

$$\beta^{-1}=\frac{(\alpha^3-\alpha^2-9\alpha+9)}{8}=\frac{2+\sqrt{2}-\sqrt{6}}{4}.$$

Outro corolário que podemos extrair desse teorema relaciona extensões simples geradas por elementos algébricos que possuem mesmo polinômio minimal sobre um corpo F, a saber, tais extensão são isomorfas.

Corolário 2.4.5. *Sejam $F\subseteq K$ uma extensão de corpos e $\alpha,\beta\in K$ dois elementos algébricos de grau n sobre F com o mesmo polinômio minimal $m(X)$. Então a aplicação*

$$F(\alpha)\to F(\beta);\quad c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}\mapsto c_0+c_1\beta+\cdots+c_{n-1}\beta^{n-1}$$

é um isomorfismo.

Demonstração. Pelo teorema (2.4.1), se $m(X)$ é o polinômio minimal de α e β, e $r(X)=c_0+c_1X+\cdots+c_{n-1}X^{n-1}\in F(X)$, então temos dois isomorfismos

$$\varphi_1: F[X]/\langle m(X)\rangle\to F(\alpha);\quad r(X)+\langle m(X)\rangle\mapsto r(\alpha)=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}$$

$$\varphi_2: F[X]/\langle m(X)\rangle\to F(\beta);\quad r(X)+\langle m(X)\rangle\mapsto r(\beta)=c_0+c_1\beta+\cdots+c_{n-1}\beta^{n-1}$$

Sendo assim, basta considerar a composição $\varphi: F(\alpha)\to F(\beta)=\varphi^{-1}\circ\varphi_2$, que será um isomorfismo. □

Note que a recíproca desse corolário não é verdadeira, como segue.

Exemplo 2.4.6. *O fato de $F(\alpha)$ e $F(\beta)$ serem isomorfos, ou mesmo iguais, não implica que α e β tem o mesmo polinômio minimal. Vejamos, como exemplo, que $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(a+b\sqrt{2})$, para todo $a,b\in\mathbb{Q}$, com $a\neq 0$, mas $\sqrt{2}$ e $\alpha=a+b\sqrt{2}$ possuem polinômios minimais diferentes. É claro que o polinômio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$ é X^2-2. Vamos agora encontrar o polinômio minimal de $\alpha=a+b\sqrt{2}$ sobre $\mathbb{Q}$, note que*

$$\begin{aligned} \alpha=a+b\sqrt{2} &\Rightarrow \alpha-a=b\sqrt{2} \\ &\Rightarrow \alpha^2-2\alpha a+a^2=2b^2 \\ &\Rightarrow \alpha^2-2a\alpha+a^2-2b^2=0 \end{aligned}$$

Assim, α é raiz do polinômio $f(X) = X^2 - 2aX + a^2 - 2b^2 \in \mathbb{Q}[X]$. Como $\alpha \notin \mathbb{Q}$, pelo exemplo (2.3.4), segue que $f(X)$ é o polinômio minimal de α sobre $\mathbb{Q}$. Já mostramos que os polinômios minimais são diferentes, basta verificar a igualdade das extensões. Como o grau de α sobre $\mathbb{Q}$ é dois, pelo corolário (2.4.2), temos que

$$\begin{aligned}
\mathbb{Q}(a+b\sqrt{2}) &= \{c_0 + c_1(a+b\sqrt{2});\ c_0, c_1 \in \mathbb{Q}\} \\
&= \{(c_0 + c_1 a) + (c_1 b)\sqrt{2};\ c_0, c_1 \in \mathbb{Q}\} \\
&= \{a' + b'\sqrt{2};\ a', b' \in \mathbb{Q}\} \\
&= \mathbb{Q}(\alpha)
\end{aligned}$$

Também, pelo exemplo (2.1.10), sabemos que $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}; a, b \in \mathbb{Q}\}$. Construímos então duas extensões simples iguais, mas com polinômios minimais dos elementos geradores diferentes.

Um exemplo particularmente interessante e, talvez contraintuitivo, é o seguinte.

Exemplo 2.4.7. *É possível construir extensões isomorfas entre corpos de números estritamente reais e corpos de números complexos. De fato, se $\beta \neq 1$ é uma raiz cúbica complexa da unidade, isto é, $\beta^3 = 1$, por exemplo, $\dfrac{-1+i\sqrt{3}}{2}$, então $\sqrt[3]{2}$ e $\sqrt[3]{2}\beta$ possuem o mesmo polinômio minimal $X^3 - 2$ sobre $\mathbb{Q}$. Dessa forma, pelo corolário anterior, a aplicação*

$$\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\beta); \quad r(\sqrt[3]{2}) \mapsto r(\sqrt[3]{2}\beta)$$

com $r(X) = c_0 + c_1 X + c_2 X^2 \in \mathbb{Q}(X)$, é um isomorfismo de corpos. Observe, no entanto, que $\mathbb{Q}(\sqrt[3]{2})$ é um corpo de números estritamente reais e $\mathbb{Q}(\sqrt[3]{2}\beta)$ não o é.

CAPÍTULO 3

EXTENSÕES FINITAS

3.1 Extensões finitas

Nesta seção estudaremos extensões finitamente geradas. Como motivação, se $F \subseteq K$ é uma extensão de corpos e $\alpha \in K$ é um elemento algébrico de grau n sobre F, temos que a extensão $F(\alpha)$ é, de acordo com o corolário (2.4.2), caracterizada da seguinte forma

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1};\ a_0, a_1, \ldots, a_{n-1} \in F\}.$$

Note que essa extensão é constituída de combinações lineares de potências de α, em termos da álgebra linear, tais potências geram $F(\alpha)$ sobre F.

Para formalizar e generalizar essa ideia, veremos que o corpo K pode ser visto como um espaço vetorial sobre o corpo F. Com efeito, se F é um corpo e $\varphi : F \to A$ é um homomorfismo de anéis não nulo, então A é um espaço vetorial sobre F (ou F- espaço vetorial) com a multiplicação por escalar definida por

$$\cdot : F \times A \to A; \quad (x, a) \mapsto x \cdot a := \varphi(x) \cdot a$$

Assim, se $F \subseteq K$ é uma extensão de corpos, existe uma imersão $\varphi : F \to K$ e, portanto, K é um espaço vetorial sobre F.

Definição 3.1.1. Seja $F \subseteq K$ uma extensão de corpos. A dimensão de K como F- espaço vetorial, denotada por $[K : F]$, é denominada grau de K sobre F. Dizemos que K tem dimensão finita sobre F (ou que K é finito sobre F) se K tem grau finito sobre F.

Agora, podemos acrescentar essa informação sobre o grau de uma extensão nos diagramas. Por exemplo, considere as extensões $F \subseteq L \subseteq K$ e suponha que $[K : L] = m$ e $[L : F] = n$, podemos fazer uma representação da seguinte forma.

$$\begin{array}{c} K \\ \uparrow m \\ L \\ \uparrow n \\ F \end{array}$$

Como primeiro exemplo desta seção vamos mostrar que dada uma extensão de corpos, podemos verificar se os corpos são iguais apenas observando o grau da extensão.

Exemplo 3.1.2. *Seja $F \subseteq K$ uma extensão de corpos. Então $F = K$ se, e somente se, $[K : F] = 1$. Por um lado, se $F = K$, basta observar que $\{1_K\}$ é uma base de K sobre F, de fato, dado $v \in K$, basta tomar $v \in F$ como escalar, assim $v = 1_k v$. Por outro lado, considere que $[K : F] = 1$ e $\{k\}$ uma base de K sobre F. Suponha que $F \neq K$. Então, existirá $v \in K \backslash F$. Se v pudesse ser escrito como combinação linear da base de K, existiria $a \in F$ tal que $v = ak$, donde $k = a^{-1}v \in F$. Logo, $v = ak = aa^{-1}v \in F$. O que será um absurdo. Portanto, $F = K$.*

Uma extensão já conhecida é $\mathbb{R} \subseteq \mathbb{C}$, nesse contexto de espaços vetoriais, podemos visualizar $\mathbb{C}$ como um espaço vetorial de dimensão finita sobre $\mathbb{R}$, mais ainda, podemos determinar o grau de $\mathbb{C}$ sobre $\mathbb{R}$. O seguinte exemplo elucida essa ideia.

Exemplo 3.1.3. *O corpo dos números complexos $\mathbb{C}$ é uma extensão finita de grau dois sobre $\mathbb{R}$. Com efeito, dado $z \in \mathbb{C}$, existem $a, b \in \mathbb{R}$, tais que $z = a + bi$, sendo assim, o conjunto linearmente independente $\{1, i\}$ gera $\mathbb{C}$ sobre $\mathbb{R}$ e, portanto, é uma base.*

Uma das vantagens em estudar extensões de corpos utilizando o conceito de espaços vetoriais é o ganho de todas as boas ferramentas da álgebra linear, as quais utilizaremos para provar diversos resultados relacionados às estruturas algébricas estudadas neste trabalho, em particular, as extensões finitas.

Como primeiro resultado desta seção, provaremos diversas equivalências para o fato da extensão $F \subseteq F(\alpha)$ ser finita, o qual será muito utilizando no restante do texto.

Proposição 3.1.4. *Se $F \subseteq K$ é uma extensão de corpos, então as afirmações a seguir são equivalentes:*

(i) $F \subseteq F(\alpha)$ *é uma extensão finita;*
(ii) α *é algébrico sobre* F*;*
(iii) $F[\alpha] = F(\alpha)$*;*

(iv) $F[\alpha]$ *é um espaço vetorial de dimensão finita sobre* F*;*

Além disso, $n := [F(\alpha) : F]$ *é igual ao grau de* α *sobre* F *e* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *é uma base de* $F(\alpha)$ *sobre* F*.*

Demonstração. $(i) \implies (iv)$ Suponhamos que $F \subseteq F(\alpha)$ seja uma extensão finita de grau $n \geq 1$. Isso implica que existe uma base de $F(\alpha)$ sobre F com n elementos. Como $F[\alpha] \subseteq F(\alpha)$, teremos que os n elementos da base de $F(\alpha)$ também geram $F[\alpha]$. Sendo assim, o conjunto $\{1, \alpha, \ldots, \alpha^n\} \subseteq F[\alpha]$, que possui $n+1$ elementos, é linearmente dependente sobre F. Logo, é possível extrair dele uma base finita de $F[\alpha]$ sobre F. Portanto, $F[\alpha]$ é um espaço vetorial de dimensão finita sobre F.

$(iv) \implies (ii)$ Seja $F[\alpha]$ um espaço vetorial de dimensão finita $n \geq 1$ sobre F. Pelo mesmo argumento utilizado no item anterior, os $n+1$ elementos $\{1, \alpha, \ldots, \alpha^n\} \subseteq F[\alpha]$ são linearmente dependentes sobre F. Daí, existem escalares $c_0, c_1, \ldots, c_n \in F$, não todos nulos, tais que $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$. Ou seja, α anula o polinômio não nulo $c_0 + c_1X + \cdots + c_nX^n \in F[X]$. Portanto, é algébrico sobre F.

$(ii) \iff (iii)$ O resultado é imediato, pelo corolário (2.4.2).

$(ii) \implies (i)$ Considere α algébrico de grau $n \geq 1$ sobre F, com polinômio minimal $m(X)$. Veremos que o conjunto $\beta = \{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $F(\alpha)$ sobre F e, portanto, $[F(\alpha) : F] = n$ coincide com o grau de α sobre F. Com efeito, pelo corolário (2.4.2), temos que

$$F(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1};\ c_0, \ldots, c_{n-1} \in F\}$$

ou seja, β é um conjunto gerador de $F(\alpha)$. Basta agora verificar que esse conjunto é linearmente independente. Suponha, por absurdo, que β é um conjunto linearmente dependente. Sendo assim, existem escalares $c_0, c_1, \ldots, c_{n-1} \in F$, não todos nulos, tais que $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n1-1} = 0$. Donde α anula o polinômio $c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in F[X]$, que tem grau menor que n, contrariando a minimalidade do grau de $m(X)$. Sendo assim, β deve ser um conjunto linearmente independente. Portanto, $\beta = \{1, \alpha, \ldots, \alpha^{n-1}\}$ é, de fato, uma base de $F(\alpha)$ sobre F, o que conclui o resultado. □

Corolário 3.1.5. *Seja* $F \subseteq K$ *uma extensão de corpos. Então um elemento* $\alpha \in K$ *é transcendente sobre* F *se, e somente se,* $F(\alpha)$ *tem grau infinito sobre* F

Demonstração. Esse corolário é, precisamente, a contrapositiva da implicação $(i) \Rightarrow (ii)$, do teorema anterior. □

Proposição 3.1.6. *Sejam $F \subseteq L \subseteq K$ extensões de corpos. Então K é finito sobre F se, e somente se, K é finito sobre L e L é finito sobre F. Além disso,*

$$[K:F] = [K:L][L:F]$$

Demonstração. Por um lado, se K for finito sobre F, então K é um F-espaço vetorial de dimensão finita, donde existe um conjunto finito $\beta \subseteq K$ de geradores de K como F-espaço vetorial. Como $F \subseteq L$ teremos que β ainda gerará K como L-espaço vetorial, ou seja, K será finito sobre L. Além disso, como L é subespaço vetorial de K como F-espaço vetorial, segue, pela proposição (1.3.12), que L também é finito sobre F.

Por outro lado, considere que K seja finito sobre L e que L seja finito sobre F, com $[K:L] = n$ e $[L:F] = m$. Sendo assim, existem $\beta_1 = \{v_1, \ldots, v_n\}$ e $\beta_2 = \{w_1, \ldots, w_m\}$, bases de K sobre L e L sobre F, respectivamente. Vamos mostrar que o conjunto $\beta = \{v_i w_j;\ v_i \in \beta_1, w_j \in \beta_2\}$ é uma base de K sobre F, isto é, β gera k e é linearmente independente sobre F. Dado $k \in K$, como β_1 é base de K sobre L, existem escalares $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, tais que $k = \sum_{i=1}^{n} \alpha_i v_i$. Da mesma forma, como β_2 é uma base de L sobre F, para cada $i \in \{1, 2, \ldots, n\}$ existem $\gamma_{1i}, \gamma_{2i}, \ldots, \gamma_{mi} \in F$, tais que $\alpha_i = \sum_{j=1}^{m} \gamma_{ij} w_j$. Fazendo as substituições e manipulações convenientes, segue que para quaisquer $i \in \{1, \ldots, n\}$ e $j \in \{1, \ldots, m\}$ tem-se

$$\begin{aligned} k = \sum_{i=1}^{n} \alpha_i v_i &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \gamma_{ij} w_j \right) v_i \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \gamma_{ij} w_j v_i, \end{aligned}$$

onde $\gamma_{ij} \in F$. Segue que $k \in K$ é combinação linear de elementos em β e, sendo assim, este é um conjunto gerador de K sobre F.

Vejamos agora que β é um conjunto linearmente independente. Considere escalares $\gamma_{ij} \in F$, com $i \in \{1, \ldots, n\}$ e $j \in \{1, \ldots m\}$, tais que

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \gamma_{ij} w_j v_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \gamma_{ij} w_j \right) v_i = 0$$

Como o conjunto $\beta_1 = \{v_1, \ldots, v_n\}$ é linearmente independente, devemos ter que

$$\sum_{j=1}^{m} \gamma_{ij} w_j = 0$$

Da mesma forma, $\beta_2 = \{w_1, \ldots, w_m\}$ é um conjunto linearmente independente, segue então que $\gamma_{ij} = 0$, $\forall i \in \{1, \ldots, n\}$ e $\forall j \in \{1, \ldots, m\}$. Com isso, provamos que o conjunto β é linearmente

independente sobre F. Portanto, $\beta = \{v_i w_j;\ i = 1,\ldots,n \text{ e } j = 1,\ldots,m\}$ é uma base de K sobre F, com nm elementos, donde $[K:F] = nm = [K:L][L:F]$, o que conclui a demonstração. □

Sob certas condições dos graus envolvidos em uma extensão de corpos que possui um corpo intermediário, podemos concluir algumas igualdades entre esses corpos, como mostra o corolário a seguir.

Corolário 3.1.7. *Seja $F \subseteq L \subseteq K$ uma extensão finita de corpos. Então*

(a) Se $[K:F] = [L:F]$, então $K = L$.

(b) Se $[K:F] = [K:L]$, então $F = L$.

Demonstração. (a) Como $F \subseteq L \subseteq K$ é uma extensão finita, pela proposição anterior, temos que

$$[K:F] = [K:L][L:F]$$

Fazendo $[K:F] = [L:F]$ nessa igualdade, segue que $[K:F] = [K:L][K:F] \Rightarrow [K:L] = 1$. Pelo exemplo (3.1.2), concluímos que $K = L$.

(b) De maneira análoga, temos que $[K:F] = [K:L][L:F]$. Fazendo $[K:F] = [K:L]$ nessa igualdade, segue que $[K:L] = [K:L][L:F] \Rightarrow [L:F] = 1$. Pelo exemplo (3.1.2), concluímos que $L = F$. □

Corolário 3.1.8. *Seja $F \subseteq K$ uma extensão finita de corpos. Então todo elemento $\alpha \in K$ é algébrico sobre F e o seu grau sobre F divide $[K:F]$. Além disso, se $F \subseteq L \subseteq F(\alpha)$, então o grau de α sobre L divide o grau de α sobre F.*

Demonstração. Temos que $F \subseteq F(\alpha) \subseteq K$. Como $F \subseteq K$ é uma extensão finita, pela proposição (3.1.6), temos que K é finito sobre $F(\alpha)$ e $F(\alpha)$ é finito sobre F. Sendo assim, pela proposição (3.1.4), temos ainda que α é algébrico sobre F e $[F(\alpha):F]$ é o grau de α sobre F. Além disso, de acordo com a proposição (3.1.6), temos que

$$[K:F] = [K:F(\alpha)][F(\alpha):F]$$

Logo, o grau de α sobre F divide $[K:F]$.

Além disso, pela proposição (3.1.4), mostrar que o grau de α sobre L divide o grau de α sobre F equivale a mostrar que $[L(\alpha):L]$ divide $[F(\alpha):F]$. Considerando $F \subseteq L \subseteq F(\alpha)$,

temos que $F(\alpha) \subseteq L(\alpha)$. Como $L(\alpha)$ contém $F \cup \{\alpha\}$, pela minimalidade de $F(\alpha)$, segue que $L(\alpha) = F(\alpha)$. Sendo assim, pela proposição 3.1.6, segue que

$$[F(\alpha) : F] = [F(\alpha) : L][L : F]$$

Portanto, $[L(\alpha) : L] = [F(\alpha) : L]$ divide $[F(\alpha) : F]$, o que conclui a demonstração. □

O próximo corolário mostra que se K é uma extensão com grau primo sobre F, então o corpo K é uma extensão simples de F gerada por qualquer elemento $\alpha \in K \backslash F$.

Corolário 3.1.9. *Se $F \subseteq K$ é uma extensão de corpos e $[K : F] = p$ é um número primo, então $K = F(\alpha)$, para todo $\alpha \in K \backslash F$. Além disso, uma base de K sobre F é $\{1, \alpha, \ldots, \alpha^{p-1}\}$.*

Demonstração. Dado $\alpha \in K \backslash F$, temos que $F \subseteq F(\alpha) \subseteq K$. Como $F \subseteq K$ é uma extensão finita, pela proposição (3.1.6), segue que

$$p = [K : F] = [K : F(\alpha)][F(\alpha) : F]$$

ou seja, $[F(\alpha) : F]$ divide p. Como p é primo, temos que $[F(\alpha) : F] = 1$ ou $[F(\alpha) : F] = p$. Note que $\alpha \in K \backslash F$, donde $F(\alpha) \neq F$, sendo assim, do exemplo (2.3.3), temos que $[F(\alpha) : F] \neq 1$, portanto, $[F(\alpha) : F] = p$. Com isso, $p = [K : F] = [F(\alpha) : F]$, pelo corolário (3.1.7), segue que $K = F(\alpha)$, para todo $\alpha \in K \backslash F$. O fato de $\{1, \alpha, \ldots, \alpha^{p-1}\}$ ser uma base de K sobre F decorre de $[F(\alpha) : F] = p$ e da proposição (3.1.4). □

3.2 Extensões quadráticas

Uma extensão $F \subseteq K$, tal que $[K : F] = 2$, é chamada de extensão quadrática. Nesse caso, como dois é primo, segue, pelo corolário (3.1.9), que $K = F(\alpha)$, qualquer que seja $\alpha \in K \backslash F$. Além disso, α é raiz de um polinômio irredutível $m(X) = X^2 + bX + c$, com coeficientes em F, uma base de K sobre F é $\{1, \alpha\}$.

No decorrer do que faremos a seguir surgirá, naturalmente, uma divisão por dois, para que tal divisão seja possível, é necessário que estejamos sobre um corpo cuja característica não seja 2. Sendo assim, considere agora F um corpo de característica diferente de dois e $F(\alpha)$ uma extensão quadrática, com $\alpha^2 + b\alpha + c = 0$, onde $b, c \in F$. Posto $\Delta = b^2 - 4c$, temos

$$\begin{aligned} \alpha^2 + b\alpha + c = 0 &\Rightarrow \alpha^2 + b\alpha = -c \\ &\Rightarrow 4\alpha^2 + 4b\alpha = -4c \\ &\Rightarrow b^2 + 4\alpha^2 + 4b\alpha = b^2 - 4c \\ &\Rightarrow (b + 2\alpha)^2 = \Delta \end{aligned}$$

Portanto, em $F(\alpha)$ existe um elemento $\gamma := \pm(b+2\alpha)$, tal que $\gamma^2 = \Delta \in F$. Além disso, α pode ser expresso da seguinte forma: $\alpha = \dfrac{\gamma - b}{2}$. Com certo abuso de notação e pensando em uma analogia com o caso numérico, podemos definir $\gamma := \pm\sqrt{\Delta}$ e encontrar a fórmula usual para solução de equações quadráticas

$$\alpha = \frac{\gamma - b}{2} = \frac{-b \pm \sqrt{\Delta}}{2}$$

Note que $\alpha = \dfrac{\gamma}{2} - \dfrac{b}{2} \in F(\gamma)$, sendo assim, devemos ter que $\gamma \notin F$. Com efeito, se $\gamma \in F$, então, pelo exemplo (2.3.3), teríamos que $F(\gamma) = F$, donde $\alpha \in F(\gamma) = F$, o que não pode acontecer, pois $\alpha \in K \backslash F$. Além disso, γ anula o polinômio de grau dois $X^2 - \Delta \in F[X]$, o que nos possibilita concluir, de acordo com o exemplo (2.3.4), que γ tem grau dois sobre F, ou seja, $2 = [F(\alpha) : F] = [F(\gamma) : F]$. Observe também que, como $\alpha \in F(\gamma)$, então $F \subseteq F(\alpha) \subseteq F(\gamma)$. Sendo assim, pela proposição (3.1.7), segue que $F(\alpha) = F(\gamma)$.

Reciprocamente, se $\gamma \notin F$ e $\gamma^2 := c \in F$, então γ é raiz do polinômio $X^2 - c \in F[X]$. Disto, γ tem no máximo grau dois sobre F. Note que, pelo exemplo (2.3.3), γ não pode ter grau um sobre F, sendo assim, terá grau dois. Consequentemente, a extensão $F(\gamma)$ é quadrática sobre F.

A conclusão que podemos fazer é que todas, e apenas as extensões quadráticas de um corpo F com característica diferente de dois são do tipo $F(\gamma)$, com $\gamma \notin F$ e $\gamma^2 \in F$. Em corpos com característica igual a dois essa conclusão não é verdadeira. Para verificar essa afirmação, veja [2, Esempi 4.1.2, p. 136].

3.3 Extensões biquadráticas

Se F é um corpo e $F(\alpha)$ e $F(\beta)$ são duas extensões quadráticas distintas de F, então a extensão $F(\alpha,\beta) = F(\alpha)(\beta)$ é chamada de extensão biquadrática de F. Observe que $F(\alpha) \neq F(\beta)$ se, e somente se, $\beta \notin F(\alpha)$ (ou equivalentemente, $\alpha \notin F(\beta)$). Com efeito, considere $F(\alpha) \neq F(\beta)$ e suponha que $\beta \in F(\alpha)$. Assim, $F \subseteq F(\beta) \subseteq F(\alpha)$. Além disso, temos que $[F(\alpha) : F] = [F(\beta) : F] = 2$, o que implica, pelo corolário (3.1.7), que $F(\alpha) = F(\beta)$. Por outro lado, é claro que se $\beta \notin F(\alpha)$, então $F(\beta) \not\subseteq F(\alpha)$, logo, $F(\beta) \neq F(\alpha)$.

Vamos mostrar agora que β tem grau dois sobre $F(\alpha)$. Para isso, observe que β anula um polinômio de grau dois com coeficientes em F, pois $[F(\beta) : F] = 2$, sendo assim, também anula um polinômio de grau dois com coeficientes em $F(\alpha)$. Logo, como $\beta \notin F(\alpha)$, pelo exemplo (2.3.4)), segue que β tem grau dois sobre $F(\alpha)$, então, $[F(\alpha)(\beta) : F(\alpha)] = 2$.

Podemos agora verificar que a extensão $F(\alpha,\beta)$ tem grau quatro sobre F. Como $F \subseteq F(\alpha) \subseteq F(\alpha)(\beta)$, segue, da proposição (3.1.6), que

$$[F(\alpha,\beta):F] = [F(\alpha)(\beta),F] = \underbrace{[F(\alpha)(\beta):F(\alpha)]}_{2}\underbrace{[F(\alpha):F]}_{2} = 4$$

Ainda por essa proposição, temos que $\{1,\alpha\}$ e $\{1,\beta\}$ são bases de $F(\alpha)$ e $F(\beta)$ sobre F, respectivamente. Sendo assim, $\{1,\alpha,\beta,\alpha\beta\}$ é uma base de $F(\alpha,\beta)$ sobre F.

Mostraremos que $F(\alpha,\beta) = F(\gamma)$, onde $\gamma := \alpha+\beta$. Para isso, utilizaremos o corolário (3.1.7), sendo assim, é suficiente verificar que $F \subseteq F(\gamma) \subseteq F(\alpha,\beta)$ e $[F(\gamma):F] = [F(\alpha,\beta):F]$, ou seja, $[F(\gamma):F] = 4$. Note que $\gamma \in F(\alpha,\beta)$, donde obtemos a primeira condição: $F \subseteq F(\gamma) \subseteq F(\alpha,\beta)$. Pela proposição (3.1.6), temos que

$$4 = [F(\alpha,\beta):F] = [F(\alpha,\beta):F(\gamma)][F(\gamma):F].$$

Posto $d := [F(\gamma):F]$ temos que d divide 4 e, sendo assim, teremos três possibilidades:
(a) $d = 1$: Note que $\gamma \notin F$, caso contrário, teríamos $\beta = \gamma - \alpha \in F(\alpha)$, pois $\gamma \in F(\alpha)$ e $\alpha \in F(\alpha)$, o que não pode acontecer, pois queremos que $F(\beta)$ e $F(\alpha)$ sejam extensões distintas, e estas o serão se, e somente se $\beta \notin F(\alpha)$. Logo, pelo exemplo (2.3.3), $d \neq 1$ e, sendo assim, este item é falso.
(b) $d = 2$: Isto significa que $F \subseteq F(\gamma)$ é uma extensão quadrática, ou seja, γ anula um polinômio mônico de grau dois sobre F, seja $m(X) = X^2 + c_1X + c_0$ esse polinômio e considere $p(X) = X^2 + a_1X + a_0$ e $q(X) = X^2 + b_1X + b_0$ os polinômios minimais de α e β sobre F, respectivamente. Assim,

$$\begin{aligned} m(\gamma) = p(\alpha) = q(\beta) = 0 \quad &\Rightarrow \quad \gamma^2 + d_1\gamma + d_0 = \alpha^2 + a_1\alpha + a_0 = \beta^2 + b_1\beta + b_0 = 0 \\ &\Rightarrow \quad \gamma^2 + d_1\gamma + d_0 - \alpha^2 - a_1\alpha - a_0 - \beta^2 - b_1\beta - b_0 = 0 \end{aligned}$$

Fazendo $\gamma = \alpha + \beta$, segue que

$$\begin{aligned} (\alpha+\beta)^2 + d_1(\alpha+\beta) + d_0 - \alpha^2 - a_1\alpha - a_0 - \beta^2 - b_1\beta - b_0 = 0 \Rightarrow \\ \Rightarrow \alpha^2 + 2\alpha\beta + \beta^2 + d_1\alpha + d_1\beta + d_0 - \alpha^2 - a_1\alpha - a_0 - \beta^2 - b_1\beta - b_0 = 0. \end{aligned}$$

Cancelando α^2 e β^2 e colocando α e β em evidência em alguns termos, vem

$$(d_0 - a_0 - b_0) + (d_1 - a_1)\alpha + (d_1 - b_1)\beta + 2\alpha\beta = 0$$

O que é uma contradição, pois $\{1,\alpha,\beta,\alpha\beta\}$ é um conjunto linearmente independente sobre F, porque é uma base de $F(\alpha,\beta)$ sobre F, sendo assim, deveríamos ter todos os escalares nulos, o que não acontece. Portanto, este item também é falso.

(c) $d=4$: Nos resta então este item, ou seja, $d=[F(\gamma):F]=4$, como queríamos demonstrar.

Portanto, $F(\gamma)=F(\alpha+\beta)=F(\alpha,\beta)$, e uma outra base de $F(\gamma)$ sobre F é $\{1,\gamma,\gamma^2,\gamma^3\}$ (proposição (3.1.4)).

Vamos agora encontrar o polinômio minimal de γ sobre F. Suponhamos que F tenha característica diferente de dois, assim, como $F(\alpha)$ e $F(\beta)$ são extensões quadráticas, pela caracterização feita na seção anterior, temos que $a:=\alpha^2$ e $b:=\beta^2$ são elementos de F. Neste caso, o polinômio minimal $m(x)$ de γ sobre F será um polinômio mônico biquadrático. De fato,

$$\begin{aligned}
\gamma=\alpha+\beta &\Rightarrow \gamma^2=\alpha^2+2\alpha\beta+\beta^2\\
&\Rightarrow \gamma^2=a+2\alpha\beta+b\\
&\Rightarrow \gamma^2-a-b=2\alpha\beta\\
&\Rightarrow \gamma^4+a^2+b^2-2a\gamma^2-2b\gamma^2+2ab=4\alpha^2\beta^2\\
&\Rightarrow \gamma^4-2(a+b)\gamma^2+a^2+2ab+b^2=4ab\\
&\Rightarrow \gamma^4-2(a+b)\gamma^2+a^2-2ab+b^2=0\\
&\Rightarrow \gamma^4-2(a+b)\gamma^2+(a-b)^2=0
\end{aligned}$$

Logo, γ é raiz do polinômio biquadrático $X^4-(2a+b)X^2+(a-b)^2\in F[X]$.

A recíproca de tal fato não é, em geral, verdadeira, ou seja, se o polinômio minimal de γ sobre F é biquadrático, não necessariamente a extensão $F(\gamma)$ é biquadrática. Um exemplo de tal afirmação pode ser encontrado em [2, Sezione 3.5.2, p. 126].

3.4 Extensões do tipo $\mathbb{Q}(\sqrt[3]{a},\sqrt{b})$

Sejam $a,b\in\mathbb{Q}$, tais que X^3-a e X^2-b sejam polinômios irredutíveis sobre $\mathbb{Q}$ e considere $\alpha,\beta\in\mathbb{C}$, tais que $\alpha^3=a$ e $\beta^2=b$. Mostraremos que $\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\sqrt[3]{a},\sqrt{b})$ tem grau 6 sobre F e $\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\gamma)$, onde $\gamma:=\alpha+\beta$.

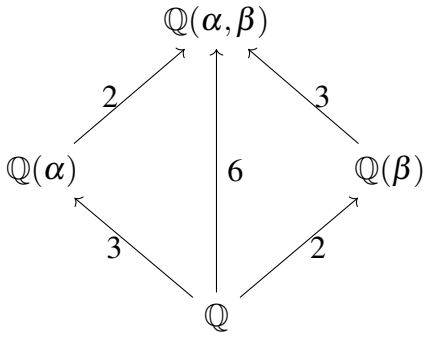
Note que α tem grau três sobre $\mathbb{Q}$, pois é raiz do polinômio irredutível $X^3-a\in\mathbb{Q}[X]$ e, de maneira análoga, β tem grau dois sobre $\mathbb{Q}$. Equivalentemente, pela proposição (3.1.4), temos que $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$ e $[\mathbb{Q}(\beta):\mathbb{Q}]=2$. Além disso, como $\alpha\in\mathbb{Q}(\alpha,\beta)$, segue que $\mathbb{Q}\subseteq\mathbb{Q}(\alpha)\subseteq\mathbb{Q}(\alpha,\beta)$. Sendo assim, pela proposição (3.1.6), vem

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha)(\beta):\mathbb{Q}(\alpha)]\underbrace{[\mathbb{Q}(\alpha):\mathbb{Q}]}_{3}=[\mathbb{Q}(\beta)(\alpha):\mathbb{Q}(\beta)]\underbrace{[\mathbb{Q}(\beta):\mathbb{Q}]}_{2} \tag{3.1}$$

Com isso, $d_1 := [\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$ é múltiplo de dois e de três, logo, é múltiplo de seis. Também sabemos que α anula um polinômio de grau três sobre $\mathbb{Q} \subseteq \mathbb{Q}(\beta)$, donde α tem no máximo grau três sobre $\mathbb{Q}(\beta)$, ou seja, $d_2 := [\mathbb{Q}(\beta)(\alpha):\mathbb{Q}(\beta)] \leq 3$. Portanto, da equação (3.1), segue que $d_1 = d_2 \cdot 2$

Como d_1 é múltiplo de seis, e $d_2 \leq 3$, devemos ter que $d_2 = 3$, o que nos possibilita concluir que $d_1 = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 6$, como queríamos.

Além disso, da proposição (3.1.4), temos que $\{1,\alpha,\alpha^2\}$ e $\{1,\beta\}$ são bases de $\mathbb{Q}(\alpha)$ e $\mathbb{Q}(\beta)$ sobre $\mathbb{Q}$, respectivamente. Sendo assim, $\{1,\alpha,\alpha^2,\beta,\alpha\beta,\alpha^2\beta\}$ é uma base de $\mathbb{Q}(\alpha,\beta)$ sobre $\mathbb{Q}$. Vamos visualizar um diagrama que representa essas extensões.



Vejamos agora que $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha,\beta)$, com $\gamma = \alpha+\beta$. Observe que $\gamma \in \mathbb{Q}(\alpha,\beta)$, logo, $\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha,\beta)$, para mostrar a igualdade, utilizaremos, novamente, o corolário (3.1.7), então basta verificar que $[\mathbb{Q}(\gamma):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 6$. Da proposição (3.1.6), temos que

$$6 = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\gamma)][\mathbb{Q}(\gamma):\mathbb{Q}]$$

Donde $d := [\mathbb{Q}(\gamma):\mathbb{Q}]$ divide seis, sendo assim, temos quatro possibilidades:

(a) $d = 1$. Analisando o diagrama, percebemos que a extensão $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha)(\beta)$ tem grau 2, logo, pelo exemplo (2.3.3), temos que $\beta \notin \mathbb{Q}(\alpha)$. Se $d = 1$, então, pelo mesmo exemplo, $\gamma \in \mathbb{Q}$, o que implicaria $\beta = \gamma - \alpha \in \mathbb{Q}(\alpha)$, que não pode ocorrer. Logo, este item é falso.

(b) $d = 2$. Se $d = 2$, então $\mathbb{Q}(\gamma)$ é uma extensão quadrática, ou seja, γ anula um polinômio $m(X) = X^2 + c_1X + c_0 \in \mathbb{Q}[X]$. Assim,

$$\begin{aligned} m(\gamma) = \gamma^2 + c_1\gamma + c_0 = 0 \quad &\Rightarrow \quad (\alpha+\beta)^2 + c_1(\alpha+\beta) + c_0 = 0 \\ &\Rightarrow \quad \alpha^2 + 2\alpha\beta + \beta^2 + b\alpha + c_1\beta + c_0 = 0 \end{aligned}$$

Como o conjunto $\{1,\alpha,\alpha^2,\beta,\alpha\beta,\alpha^2\beta\}$ é linearmente independente, pois é uma base de $\mathbb{Q}(\alpha,\beta)$ sobre $\mathbb{Q}$, a igualdade acima é uma contradição. Assim, este item também é falso.

(c) $d=3$. De maneira análoga, se $d=3$, então γ anula um polinômio $m(X)=X^3+c_2X^2+c_1X+c_0\in\mathbb{Q}[X]$. Assim,

$$\begin{aligned} m(\gamma)=\gamma^3+c_2\gamma^2+c_1\gamma+c_0 &= 0\\ (\alpha+\beta)^3+c_2(\alpha+\beta)^2+c_1(\alpha+\beta)+c_0 &= 0\\ \alpha^3+3\alpha^2\beta+3\alpha\beta^2+\beta^3+c_2(\alpha^2+2\alpha\beta+\beta^2)++c_1\alpha+c_1\beta+c_0 &= 0 \end{aligned}$$

Fazendo $\alpha^3=a$ e $\beta^2=b$, segue que

$$\begin{aligned} a+3\alpha^2\beta+3b\alpha+b\beta+c_2\alpha^2+2c_2\alpha\beta+c_2b+c_1\alpha+c_1\beta+c_0 &= 0\\ 3\alpha^2\beta+(3b+c_1)\alpha+(b+c_1)\beta+c_2\alpha^2+2c_2\alpha\beta+(a+c_2b+c_0) &= 0 \end{aligned}$$

Do mesmo modo, como o conjunto $\{1,\alpha,\alpha^2,\beta,\alpha\beta,\alpha^2\beta\}$ é linearmente independente, temos que a igualdade acima é uma contradição. O que implica que este item também é falso.

(d) $d=6$. Nos resta então este item, ou seja, $d=[\mathbb{Q}(\gamma):\mathbb{Q}]=6$, como queríamos demonstrar.

Portanto, $\mathbb{Q}(\gamma)=\mathbb{Q}(\alpha+\beta)=\mathbb{Q}(\alpha,\beta)$.

Vamos agora calcular o polinômio minimal de γ sobre $\mathbb{Q}(\beta),\mathbb{Q}(\alpha)$ e $\mathbb{Q}$.

(a) Sobre $\mathbb{Q}(\beta)$. Note que

$$\begin{aligned} \gamma=\alpha+\beta &\Rightarrow \gamma-\beta=\alpha\\ &\Rightarrow \gamma^3-3\gamma^2\beta+3\gamma\beta^2-\beta^3=\alpha^3\\ &\Rightarrow \gamma^3-3\beta\gamma^2+3b\gamma-b\beta-a=0 \end{aligned}$$

Donde o polinômio minimal de γ sobre $\mathbb{Q}(\beta)$ é $g(X)=X^3-3\beta X^2+3bX-(b\beta+a)$

(b) Sobre $\mathbb{Q}(\alpha)$. Observe que

$$\begin{aligned} \gamma=\alpha+\beta &\Rightarrow \gamma-\alpha=\beta\\ &\Rightarrow \gamma^2-2\gamma\alpha+\alpha^2=\beta^2\\ &\Rightarrow \gamma^2-2\alpha\gamma+(\alpha^2-b)=0 \end{aligned}$$

O que implica que $h(X)=X^2-2\alpha X+(\alpha^2-b)$ é o polinômio minimal de γ sobre $\mathbb{Q}(\alpha)$.

(c) Sobre $\mathbb{Q}$. Retornando ao item (a), temos que

$$\begin{aligned}
\gamma^3 - 3\beta\gamma^2 + 3b\gamma - b\beta - a &= 0 \\
\gamma^3 + 3b\gamma - a &= (3\gamma^2 + b)\beta \\
\gamma^6 + 9b^2\gamma^2 + a^2 + 6b\gamma^4 - 2\gamma^3 a - 6b\gamma a &= (9\gamma^4 + 6\gamma^2 b + b^2)\beta^2 \\
\gamma^6 + 6b\gamma^4 - 2a\gamma^3 + 9b^2\gamma^2 - 6ab\gamma + a^2 &= 9b\gamma^4 + 6b^2\gamma^2 + b^3 \\
\gamma^6 - 3b\gamma^4 - 2a\gamma^3 + 3b^2\gamma^2 - ab\gamma + (a^2 - b^3) &= 0
\end{aligned}$$

Portanto, o polinômio minimal de γ sobre $\mathbb{Q}$ é

$$f(X) = X^6 - 3bX^4 - 2aX^3 + 3b^2X^2 - 6abX + (a^2 - b^3)$$

Além disso, como γ tem grau seis sobre $\mathbb{Q}$, pela proposição (3.1.4), temos que outra base de $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\gamma)$ sobre $\mathbb{Q}$ é $\{1,\gamma,\gamma^2,\gamma^3,\gamma^4,\gamma^5\}$.

Para encerrar essa seção, observamos que γ anula os polinômios $f(X) \in \mathbb{Q}[X]$, $g(X) \in \mathbb{Q}(\beta)[X]$ e $h(X) \in \mathbb{Q}(\alpha)[X]$, além disso, temos que $f(X) \in \mathbb{Q}(\beta)[X]$ e $f(X) \in \mathbb{Q}(\alpha)[X]$. Dessa forma, como $g(X)$ e $h(X)$ são os polinômios minimais de γ sobre seus respectivos corpos, teremos, em concordância com os comentários feitos após a proposição (2.3.2), que $g(X)$ e $h(X)$ são fatores mônicos e irredutíveis de $f(X)$. Com efeito,

$$\begin{aligned}
f(X) &= g(X)(X^3 + 3\beta X^2 + 3bX + (b\beta - a)) \\
&= h(X)(X^4 + 2\alpha X^3 + (3\alpha^2 - 2b)X^2 - (2b\alpha - 2a)X + (b\alpha^2 + a\alpha + b^2))
\end{aligned}$$

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BOYER, Carl B.; MERZBACH, Uta C. **História da matemática**. Tradução de Helena Castro. Blucher, 2018.

[2] GABELLI, Stefania. **Teoria delle equazioni e teoria di Galois**. Springer Science & Business Media, 2008.

[3] GARBI, Gilberto Geraldo. **O romance das equações algébricas**. Editora Livraria da Física, 2009.

[4] HERSTEIN, Israel N. **Topics in algebra**. John Wiley & Sons, 1991.

[5] HOFFMAN, Kenneth; KUNZE, Ray. **Álgebra linear**. Prentice-Hall Hispanoamericana, 1973.

[6] LOURENÇO, Mary Lilian; COELHO, Flávio Ulhoa. **Um Curso de Álgebra Linear**. EDUSP, 2001.

[7] MARTINS, Sérgio T.; TENGAN Eduardo. **Álgebra Exemplar - Um estudo da álgebra através de exemplos**. IMPA, 2020.

[8] STILLWELL John. **Mathematics and Its History**. Springer, 2004.