UNIVERSIDADE FEDERAL DO AMAPÁ
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

EVERALDO DE ARAÚJO FERREIRA
EVERTON WILLIAN SOUZA MARTINS
HELIVALDO DA SILVA NUNES

INTRODUÇÃO À TEORIA DE GALOIS E EXTENSÃO DE CORPOS

MACAPÁ-AP
2012

EVERALDO DE ARAÚJO FERREIRA
EVERTON WILLIAN SOUZA MARTINS
HELIVALDO DA SILVA NUNES

INTRODUÇÃO À TEORIA DE GALOIS E EXTENSÃO DE CORPOS

Trabalho de Conclusão de Curso apresentado ao Colegiado de Matemática da Universidade Federal do Amapá, como parte das exigências para a obtenção do título de Licenciatura Plena em Matemática, sob orientação do Profº. Dr. Guzmán Isla Chamilco.

MACAPÁ-AP
2012

EVERALDO DE ARAÚJO FERREIRA
EVERTON WILLIAN SOUZA MARTINS
HELIVALDO DA SILVA NUNES

INTRODUÇÃO À TEORIA DE GALOIS E EXTENSÃO DE CORPOS

Trabalho de Conclusão de Curso apresentado à Comissão Examinadora do Colegiado de Matemática da Universidade Federal do Amapá, Campus Marco Zero, como requisito parcial para a obtenção do título de Graduação em Licenciatura Plena em Matemática.

Comissão Examinadora:

Profº. Dr. Guzmán Eulálio Isla Chamilco (Orientador).
Colegiado de Matemática, Unifap

Profº. Dr. José Walter Cárdenas Sotil
Colegiado de Matemática, Unifap

Profº. Josiane Oliveira dos Santos
Colegiado de Matemática, Unifap

MACAPÁ-AP
2012

Dedicamos a todos a contribuição que direta ou indiretamente nos ajudaram para realização do nosso trabalho, em particular ao nosso Professor Orientador: Guzmán Isla Chamilco, que em todo tempo esteve sempre disposto a nos auxiliar quando preciso. Desde já nossos sinceros agradecimentos.

AGRADECIMENTOS

A Deus por ter nos dados a vida, aos nossos pais que têm contribuído com a nossa formação, aos nossos irmãos, esposa, filhos, namorada e amigos pelo incentivo de continuar firme na labuta, aos meus colegas de curso pela amizade e companheirismo, aos professores, aos quais devemos parte de nossa formação, em particular o nosso Professor Orientador.

A Matemática como qualquer área do conhecimento humano, tem seu desenrolar evolutivo capaz de caracterizá-la como uma ciência que também se desenvolve a partir de sua própria história. Desse modo podemos buscar nessa história fatos, descobertas e revoluções que nos mostrem o caráter criativo do homem quando se dispõe a elaborar e disseminar a ciência matemática no seu meio sócio-cultural.

(MENDES, 2001, p.18)

Resumo

A Teoria de Galois é um ramo da álgebra abstrata. No nível mais básico, ela usa grupo de permutações para descrever como as várias raízes de uma certa equação polinomial estão relacionadas umas com as outras. Este foi o ponto-de-vista original de Évariste Galois.

A idéia central da teoria de Galois é considerar que permutações dessas raízes têm propriedades que qualquer equação algébrica satisfeita pelas raízes é ainda satisfeita depois dessas raízes terem sido permutadas. Um importante pré-requisito é restringir a equações algébricas cujos os coeficientes são números racionais.

Palavras-chave: Teoria de Galois, Normalidade, Solubilidade.

Lista de Figuras

Sumário

Capítulo 1

Introdução

1.1 A História da Teoria de Galois

Matemático francês (25/10/1811-31/5/1832). Autor da Teoria dos Grupos ou Conjuntos. Nascido em Bourg-la-Reine, é um estudante mediano até os 15 anos, quando se apaixona pela matemática. Em menos de cinco anos, domina quase todo o conhecimento disponível sobre o assunto em sua época.

Figura 1.1: Evariste Galois

Evariste Galois nasceu na França - 25 de outubro de 1811 e faleceu no dia 31 de maio de 1832. Seu primeiro Contato com a Matemática foi Com doze anos, Galois foi para a escola no Liceu de Louis-le-Grand. Lá ele não encontrou nenhum curso de matemática. Somente aos dezesseis anos pôde fazer seu primeiro curso de matemática e com dezessete anos, publicou seu primeiro trabalho nos Annales de Gergonne. Ele Foi reprovado duas vezes no exame de admissão para a Escola Polytechnique, os seus modos rudes e a falta de explicações na prova oral fizeram com que sua admissão fosse recusada. Com dezeseis anos, submeteu dois trabalhos de pesquisa Acadêmicas de Ciências. **Cauchy** ficou muito impressionado com o trabalho do jovem Evariste e o julgou capaz de participar na competição pelo Grande Prêmio de Matemática da Academia. Para isso, os dois trabalhos teriam que ser reapresentados na forma de uma única tese.

Em julho de 1829, um jesuíta, contrário as ideias republicanas do pai de Evariste, começou uma campanha para depô-lo. Escreveu uma série de versos vulgares ridicularizando membros da comunidade e os assinou com o nome do velho Galois que não pode suportar a vergonha e se suicidou.

Evariste Galois voltou a Paris e juntou seus dois trabalhos num só e os enviou para o secretário da Academia, Joseph Fourrier. O trabalho de Galois não apresentava uma solução para os problemas do quinto grau, mas oferecia uma visão tão brilhante que Cauchy, o considerava como o provável vencedor. Mas, o trabalho não ganhou o prêmio e nem foi oficialmente inscrito. Fourrier morreu algumas semanas antes da data da decisão dos juízes, e embora alguns trabalhos iniciais tivessem sido entregue ao comitê, o de Galois não estava entre eles. O trabalho nunca foi encontrado e a injustiça foi registrada por um jornalista francês. Em dezembro de 1830, o gênio contrariado tentou se tornar um rebelde profissional alistando-se na Artilharia da Guarda Nacional, acusado de conspiração Galois foi preso. Ficou na prisão durante um mês e mergulhou num estado de depressão, tentando suicídio. Em março de 1832, um mês antes do final da sentença, irrompeu uma epidemia de cólera em Paris e os prisioneiros foram libertados.

Galois envolveu-se com uma mulher misteriosa, chamada Stephanie-Felice Poterine du Motel. Stephanie já estava comprometida com um cidadão um dos melhores atiradores da França e que descobriu a infidelidade de sua noiva. Furioso, não hesitou em desafiar Galois para um duelo ao raiar do dia. Na noite anterior ao confronto, que ele acreditava ser a última oportunidade que teria para registrar suas ideias no papel, ele escreveu cartas para os amigos explicando as circunstância.

Um de seus maiores temores era de que sua pesquisa, rejeitada pela Academia, se perdesse para sempre. Em uma tentativa desesperada de conseguir reconhecimento, ele trabalhou a noite toda, escrevendo o teorema que, acreditava, explicaria o enigma da equação do quinto grau. No final da noite, quando seus cálculos estavam completos, ele escreveu uma carta explicativa ao seu amigo Auguste Chevalier, pedindo que, caso morresse, aquelas paginas fossem enviadas aos grandes Matemáticos da Europa.

A Teoria de Galois é um ramo da álgebra abstrata.No nível mais básico, ela usa grupo de permutações para descrever como as várias raízes de uma certa equação polinomial estão relacionadas umas com as outras. Este foi o ponto-de-vista original de Évariste Galois. A abordagem moderna da Teoria de Galois, desenvolvida por Richard Dedekind, Leopold Kronecker e Emil Artin, entre outros, envolve o estudo de automorfismos de extensões de corpos. Uma abstração além da Teoria de Galois é conseguida pela teoria das conexões de Galois. O nascimento da teoria foi originalmente motivado pela seguinte questão, que é conhecida como o teorema de Abel-Ruffini.

> "Porque não existe uma fórmula para as raizes de uma equação polinomial de quinta ordem (ou maior) em termos de coeficiente de polinômios, usando somente as operações algébricas usuais (adição, subtração, multiplicação, divisão) e aplicação de radicais (raiz quadrada, raiz cúbica, etc)?"

A teoria de Galois não é somente para dar um bela resposta para essa questão, mas também para explicar em detalhes porque é possível resolver equações de 4° grau ou menores da forma descrita acima e porque suas soluções assumem as formas que têm, ela dá uma clara explicação a questões referentes a problemas de construção com régua e compasso. Caracteriza de forma elegante as construções que podem ser executadas com este método. Usando esta teoria, torna-se relativamente fácil responder perguntas da geometria clássica tais como:

"Quais polígonos regulares são polígonos construtíveis ?"
"Por que não é possível a trissecção de um dado ângulo ?"
"Por que não é possível a quadratura do círculo?"
"Por que não é possível a duplicação do cubo?"

As últimas três perguntas referem-se aos problemas clássicos de construção com régua e compasso, que Galois conseguiu responder com sua teoria, utilizando as noções de números algébricos e transcendentes.

1.2 A abordagem de permutação de grupo na teoria Galois

- Se é dado um polinômio, pode acontecer que algumas de suas raízes estão concate -

nadas por várias equações algébricas.

Por exemplo:

Dado duas raízes α e β de um dado polinômio, a equação $\alpha^2+5\beta^3 = 7$ as conecta.

A idéia central da teoria de Galois é considerar que permutações (ou rearranjos) dessas raízes têm propriedades que qualquer equação algébrica satisfeita pelas raízes é ainda satisfeita depois destas raízes terem sido permutadas.

Um importante pré-requisito é restringir a equações algébricas cujos os coeficientes são números racionais. (Poderíamos ao invés disto especificar um certo corpo ao qual os coeficientes devem se restringir, mas no simples exemplo dado abaixo iremos nos restringir ao corpo dos números racionais.)

As permutações juntas formam um grupo de permutação, também conhecido como grupo Galois de polinômios (em relação aos números racionais). Isto pode ser melhor elucidado pela utilização de um exemplo.

Primeiro exemplo - uma equação quadrática

Considere a equação quadrática:

$$\alpha^2 - 4\alpha + 1 = 0$$

Pelo uso da equação quadrática, pode-se encontrar suas raízes:

$$\alpha^{'} = 2 + \sqrt{3} \text{ e } \alpha^{''} = 2 - \sqrt{3}$$

exemplos de equações algébricas por α e β incluem:

$$\alpha + \beta = 4 \text{ e } \alpha\beta = 1$$

Obviamente em ambas dessas equações, se nós trocarmos o α pelo β, obteremos outras expressões verdadeiras. Por exemplo, a equação $\alpha + \beta = 4$ torna-se simplesmente $\beta + \alpha = 4$. Além disso, é verdade, mas muito menos óbvio, que isso é válido também para cada possível equação algébrica satisfeita por α e β. A prova requer a teoria dos polinômios simétricos.

Exemplos de equações algébricas satisfeitas por α e β.

Conclui-se que os grupos de Galois do polinômio $x^2 - 4x + 1$ consistem das duas permutações: a permutação identidade, a qual deixa α e β inalterado, e a permutação de transposição, a qual alterna α e β. Como um grupo, ele é isomorfo ao grupo cíclico de ordem dois, representado por Z/Z_2.

Pode-se ainda levantar a objeção que α e β são relacionados ainda a outra equação algébrica

$$\alpha - \beta - 2\sqrt{3} = 0$$

a qual não é mais verdadeira quando α pelo β são trocados. Porém, esta equação não nos interessa, porque ela não possui coeficientes racionais; em particular, $2\sqrt{3}$ não é racional.

Uma discussão similar aplica-se a qualquer polinômio quadrático $ay^2 + by + c$, onde a, b e c são números racionais.

- Se o polinômio tem somente uma raiz, por exemplo $y^2 - 4y + 4 = (y^2)^2$, então o

grupo de Galois é trivial; isto é, ele contém unicamente uma permutação idêntica.

- Se ele tem duas raízes racionais, por exemplo $y^2 - 3y + 2 = (y - 2)(y - 1)$, então o

grupo de Galois é novamente racional.

- Se ele tem duas raízes *irracionais* (incluindo o caso onde as raízes são complexas),

então o grupo de Galois contém novamente duas permutações, justamente como no exemplo acima.

Segundo exemplo - um pouco mais elaborado:

Considere o polinômio $X^4 - 10X^2 + 1$, que pode também ser escrito como

$$(X^2 - 5)^2 - 24$$

. Desejamos descrever o grupo de Galois desse polinômio, novamente em relação ao corpo dos números racionais. O polinômio tem quatro raízes:

$$K = \sqrt{2} + \sqrt{3}$$

$$W = \sqrt{2} - \sqrt{3}$$

$$Y = -\sqrt{2} + \sqrt{3}$$

$$Z = -\sqrt{2} - \sqrt{3}$$

Haverá 24 possibilidades para permutar essas 4 raízes, mas nem todas essas permutaçôes são membros do grupo de Galois. Os membros dos grupos de Galois devem preservar qualquer equação algébrica com coeficiente racionais envolvendo K, W, Y e Z. Uma dessas equações é

$$K + Z = 0$$

Porém a permutação

$$(K, W, Y, Z) \longrightarrow (K, W, Z, Y)$$

não é permitida, porque isso transforma a equação válida $K+Z = 0$ na equação $K+Y = 0$, a qual é inválida, visto que $K + Y = 2\sqrt{3} \neq 0$.

Outra equação que as raízes da equação satisfazem é

$$(K + W)^2 = 8$$

Esta excluirá outras permutações, tais como:

$$(K, W, Y, Z) \longrightarrow (K, Y, W, Z)$$

Continuando nesse processo, descobrimos que as únicas permutações remanescentes (satisfazendo ambas equações simultâneas) são:

$$(K, W, Y, Z) \longrightarrow (K, W, Y, Z)$$

$$(K, W, Y, Z) \longrightarrow (Y, Z, K, W)$$

$$(K, W, Y, Z) \longrightarrow (W, K, Z, Y)$$

$$(K, W, Y, Z) \longrightarrow (Z, Y, W, K)$$

e o grupo de Galois é isomórfico.

Capítulo 2

Grupos

2.1 Definição de Grupo

Definição 2.1. Um grupo G é um conjunto não vázio, munido de uma regra (chamada lei de composição) que, a cada par de elementos x e y de G, associa um elemento de G, denotado por xy, e que satisfaz às seguintes condições:

GR 1. Para todos x, y e z de G vale a associatividade, ou seja, $(x * y) * z = x * (y * z)$.

GR 2. Existe um elemento e de G tal que $e * x = x * e = x$ para todo x de G.

GR 3. Se x é um elemento de G, então existe um elemento y em G tal que $x * y = y * x = e$.

Estritamente falando, chamamos G um grupo multiplicativo. Se o elemento de G que está associado ao par (x, y) é denotado por $x \oplus y$, escrevemos **GR 1** na forma

$$(x \oplus y) \oplus z = x \oplus (y \oplus z)$$

GR 2 na forma existe um elemento 0 em G tal que

$$0 \oplus x = x \oplus 0 = x$$

para todo x de G e **GR 3** na forma dado $x \in G$, existe um elemento y em G tal que

$$x \oplus y = y \oplus x = 0$$

com essa notação, G é chamado grupo aditivo. Usaremos a anotação $\oplus$ somente quando o grupo em questão satisfizer a condição adicional

$$x \oplus y = y \oplus x$$

para todos x e y de G. Na notação multiplicativa, isso é $xy = yx$ para todos x e y de G; se G tem essa propriedade, então ele é chamado grupo comutativo, ou abeliano.

Provaremos, agora, vários fatos simples que se verificam em todos os grupos.

- Seja G um grupo. O elemento e de G cuja existência é assegurada por **GR 2** é determinado de modo único.

Demonstração 2.1. Se e e e' satisfazem, ambos, a essa condição, então

$$e' = ee' = e$$

a esse elemento damos o nome de elemento unidade de G. No caso aditivo, ele é chamado elemento zero.

- Seja $x \in G$. O elemento y tal que $xy = yx = e$ é determinado de modo único.

Demonstração 2.2. Se z satisfaz $xz = zx = e$, temos

$$z = ez = (yx)z = y(xz) = ye = y$$

chamamos y o inverso de x, e o denotamos por x^{-1}. Na notação aditiva escrevemos $y = -x$.

Daremos agora exemplos de grupos.

Exemplo 2.1. Seja $\mathbb{Q}$ o conjunto dos números racionais, ou seja, o conjunto de todas as frações m/n, onde m e n são inteiros e $n \neq 0$. $\mathbb{Q}$ é um grupo em relação à adição. Além disso, os elementos não nulos de $\mathbb{Q}$ formam um grupo em relação à multiplicação, denotado por $\mathbb{Q}^*$.

Exemplo 2.2. Os números reais e os números complexos formam grupos em relação à adição. Os números reais não nulos e os números complexos não nulos formam grupos em relação à multiplicação. Daqui para frente, passaremos a denotar os números reais e complexos por $\mathbb{R}$ e $\mathbb{C}$, e o grupo dos elementos não-nulos por $\mathbb{R}^*$ e $\mathbb{C}^*$, respectivamente.

Exemplo 2.3. Os números complexos cujo valor absoluto é 1 formam um grupo em relação à multiplicação.

Exemplo 2.4. O conjunto que consiste dos números 1, -1 é um grupo em relação à multiplicação, formado por dois elementos.

Exemplo 2.5. O conjunto que consiste dos números $1, -1,\ i, -i$ é um grupo em relação à multiplicação. Esse grupo tem quatro elementos.

Exemplo 2.6 (**O corpo direto**)**.** Sejam G e G' grupos. Seja $G \times G$' o conjunto formado por todos os pares $(x,\ x')$ com $x \in G$ e $x' \in G$'. Se $(x,\ x')$ e $(y,\ y')$ são dois pares, defina seu produto como $(xy,\ x'y')$. Então $G \times G'$ é um grupo.

É simples verificar que as condições **GR 1, 2, 3** são satisfeitas. Chamamos $G \times G'$ de produto direto de G e G'.

Seja G um grupo, e H um subgrupo de G. Dizemos que H é um subgrupo se ele contiver o elemento unidade, e se, dados x e $y \in H$, então xy e x^{-1} também forem elementos de H. (No caso aditivo, escrevemos $x + y \in H$ e $-x \in H$). Desta forma, H é um grupo, e sua lei de composição é a mesma de G. O elemento unidade de G constitui um subgrupo, o qual é chamado subgrupo trivial. Todo grupo G é um subgrupo dele mesmo.

Exemplo 2.7. O grupo aditivo dos números racionais é um subgrupo do grupo aditivo dos números reais. O grupo dos números complexos de valor absoluto igual a 1 é um subgrupo do grupo multiplicativo dos números complexos não nulos. O grupo $\{1, -1\}$ é um subgrupo de $\{1, -1,\ i, -i\}$.

Definição 2.2. Sejam G um grupo e $a \in G$. Tomemos H como o subconjunto de elementos de G constituído de todas as potências a^n com $n \in \mathbf{Z}$. Dessa forma, H é um subgrupo gerado por a. De fato, H contém o elemento unidade $e = a^0$. Sejam $a^n,\ a^m \in H$. Assim,

$$a^m a^n = a^{m+n} \in H$$

para finalizar, temos $(a^n)^{-1} = a^{-n} \in H$. Assim H satisfaz as condições de um subgrupo e H é gerado por a.

Definição 2.3. Seja G um grupo. Diremos que G é cíclico se existe um elemento a de G tal que todo elemento x de G pode ser escrito na forma a^n para algum inteiro n. O subgrupo H acima é o subgrupo cíclico gerado por a.

Exemplo 2.8. Consideremos o grupo aditivo dos inteiros. Dessa forma é cíclico gerado por 1.

2.2 Aplicações

Definição 2.4. Sejam S, S' conjuntos. Uma aplicação de S em S' é uma regra que a cada elemento de S associa um elemento de S'. Em vez de dizer que f é uma aplicação de S em S', escrevemos frequentemente os símbolos $f : S \longrightarrow S$'.

Se $f : S \longrightarrow S$' é uma aplicação, e x é um elemento de S, denotamos por $f(x)$ o elemento de S' associado a x por f. Chamamos $f(x)$ o valor de f em x, ou, também,

a imagem de x por f. O conjunto de todos os elementos $f(x)$, com $x \in S$, é chamado imagem de f. Se T é um subconjunto de S, o conjunto dos elementos $f(x)$ com $x \in T$ é chamado imagem de T, sendo denotado por $f(T)$.

Se f é como anteriormente descrito, escrevemos $x \longmapsto f(x)$ para denotar a imagem de x por f. Note que distinguimos dois tipos de setas, ou seja, $\longrightarrow$ e $\longmapsto$.

Exemplo 2.9. Sejam S e S' ambos iguais a $\mathbb{R}$. Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$ a aplicação $f(x) = x^2$, isto é, a aplicação cujo valor em x é x^2. Podemos expressar a mesma coisa dizendo que f é a aplicação tal que $x \longmapsto x^2$. A imagem de f é o conjunto de números reais ≥ 0.

Seja $f : S \longrightarrow S$' uma aplicação, e seja T um subconjunto de S. Podemos definir uma aplicação $T \longrightarrow S$' pela mesma regra $x \longmapsto f(x)$, para $x \in T$. Em outras palavras, podemos ver f como se estivesse definida somente em T. Essa aplicação é chamada restrição de f a T e é denotada por $f|T : T \longrightarrow S$'.

Sejam S e S' dois conjuntos. Uma aplicação $f : S \longrightarrow S$' é dita injetiva se, dados x e $y \in S$, o fato de $x \neq y$ implicar $f(x) \neq f(y)$. Podemos também escrever essa condição da seguinte forma: se f(x) = f(y), então x = y.

Exemplo 2.10. A aplicação f do exemplo 1 não é injetiva. De fato, temos $f(1) = f(-1)$. Seja $g : R \longrightarrow R$ a aplicação $x \longmapsto x + 1$. Vemos que g é injetiva, pois se $x \neq y$, $x + 1 \neq y + 1$, ou seja, $g(x) \neq g(y)$.

Sejam S e S' conjuntos. Uma aplicação $f : S \longrightarrow S$' é dita sobrejetiva se a imagem $f(S)$ de S é igual a S'. Isso significa que, dado qualquer elemento $x' \in S$', existe um elemento $x \in S$ tal que $f(x) = x$'. Pode-se também dizer que f é sobre S'.

Exemplo 2.11. Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$ a aplicação $f(x) = x^2$. Então f não é sobrejetiva, pois sua imagem não contém números negativos.

Seja $g : R \longrightarrow R$ a aplicação $x \longmapsto x+1$. Dado um número y, temos $y = g(y-1)$. Logo, g é sobrejetiva.

Sejam S e S' conjuntos, e $f : S \longrightarrow S$' uma aplicação. Dizemos que f é bijetiva se f for ao mesmo tempo injetiva e sobrejetiva. Isso significa que, dado um elemento $x' \in S$', existe um único elemento $x \in S$ tal que $f(x) = x$'. (A existência vem do fato de f ser sobrejetiva, e a unicidade vem de f ser injetiva).

Exemplo 2.12. Seja J_n o conjunto dos inteiros $\{1, 2, \cdots, n\}$. Uma aplicação bijetiva $\sigma : J_n \longrightarrow J_n$ é chamada permutação dos inteiros de 1 a n. Assim, em particular, uma permutação σ como anteriormente é uma aplicação $i \longmapsto \sigma(i)$.

Exemplo 2.13. Seja S um conjunto não-vazio, e seja $I : S \longrightarrow S$ a aplicação tal que $I(x) = x$ para todo $x \in S$. I é chamada aplicação identidade, sendo também denotada

por id; ela é, obviamente, bijetiva. Muitas vezes precisamos explicitar o conjunto S na notação e escrevemos I_s ou ids para denotar a aplicação identidade de S. Seja T um subconjunto de S. A aplicação identidade $t \longmapsto t$, vista como a aplicação $T \longrightarrow S$ é chamada inclusão, e é muitas vezes denotada por $T \hookrightarrow S$.

Sejam S, T, U, e sejam

$$f : S \longrightarrow T \text{ e } g : T \longrightarrow U$$

aplicações. Podemos formar a aplicação composta

$$g \circ f : S \longrightarrow U$$

definida pela regra

$$(g \circ f)(x) = g(f(x))$$

para todo $x \in S$.

Exemplo 2.14. Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$ a aplicação $f(x) = x^2$, e $g : \mathbb{R} \longrightarrow \mathbb{R}$ a aplicação $g(x) = x + 1$. Então, $g(f(x)) = x^2 + 1$. Note que, neste caso, podemos também formar $f(g(x)) = f(x + 1) = (x + 1)^2$, e que

$$f \circ g \neq g \circ f$$

Seja $f : S \longrightarrow S$' uma aplicação. Uma aplicação inversa para f é uma aplicação

$$g : S' \longrightarrow S$$

tal que

$$g \circ f = id_s \text{ e } f \circ g = id_{s'}$$

assim, denotamos a aplicação inversa g por f^{-1}. Logo, por definição, a aplicação inversa f^{-1} é caracterizada pela seguinte propriedade: para todo $x \in S$ e $x' \in S$', temos

$$f^{-1}(f(x)) = x \text{ e } f(f^{-1}(x')) = x'$$

Exemplo 2.15. Seja $\mathbb{R}^+$ o conjunto dos números reais positivos (isto é, números reais > 0). Seja $h : R^+ \longrightarrow R^+$ a aplicação $h(x) = x^2$. Então, h é bijetiva e sua inversa é a aplicação raiz quadrada, isto é,

$$h^{-1}(x) = \sqrt{x}$$

para todo $x \in \mathbb{R}$, $x > 0$.

2.3 Homomorfismos

Definição 2.5. Sejam G e G' grupos. Um homomorfismo

$$f : G \longrightarrow G'$$

de G em G' é uma aplicação dotada da seguinte propriedade: para todos x, $y \in G$, temos

$$f(xy) = f(x)f(y)$$

e na notação aditiva, $f(x + y) = f(x) + f(y)$.

Exemplo 2.16. Seja G um grupo comutativo. A aplicação $x \longmapsto x^{-1}$ de G em si mesmo é um homomorfismo. Em notação aditiva, isso corresponde à aplicação $x \longmapsto -x$. A verificação de que essa aplicação possui a propriedade que define um homomorfismo é imediata.

Exemplo 2.17. A aplicação

$$z \longmapsto |z|$$

é um homomorfismo do grupo multiplicativo dos números complexos não-nulos no grupo multiplicativo dos números complexos não-nulos (na verdade, no grupo multiplicativo dos números reais positivos).

Exemplo 2.18. A aplicação

$$x \longmapsto e^x$$

é um homomorfismo do grupo aditivo dos números reais no grupo multiplicativo dos números reais positivos. Sua aplicação inversa, o logaritmo, é também um homomorfismo. Seja $f : G \longrightarrow G$' um homomorfismo de grupos. Definimos o núcleo de f como o conjunto de todos os elementos $x \in G$ tais que $f(x) = e'$.

O núcleo contém o elemento unidade e, pois $f(e)$ é o elemento unidade de G'. E assim por diante.

Exemplo 2.19. Seja G um grupo, e $a \in G$. A aplicação

$$n \longmapsto a^n$$

é um homomorfismo de $\mathbb{Z}$ em G. O núcleo desse homomorfismo é formado por todos os inteiros n tais que $a^n = e$.

Definição 2.6. Seja $f : G \to G$' um homomorfismo de grupos. Dizemos que f é um isomorfismo (ou um isomorfismo de grupos) se existe um homomorfismo $g : G' \to G$ tal

que $f \circ g$ e $g \circ f$ são as aplicações identidades de G' e G, respectivamente. Indicamos um isomorfismo pela notação

$$G \approx G'$$

Exemplo 2.20. A função *exp* é um isomorfismo do grupo aditivo dos números reais no grupo multiplicativo dos números reais positivos. Sua inversa é o logaritmo.

Exemplo 2.21. Seja G um grupo comutativo. A aplicação

$$f : x \longmapsto x^{-1}$$

é um isomorfismo de G em si mesmo.

- Um homomorfismo de grupos $f : G \longrightarrow G$' que é injetivo e sobrejetivo é um isomorfismo.

Demonstração 2.3. Seja $f^{-1} : G' \longrightarrow G$ a aplicação inversa. Tudo que precisamos provar é que f^{-1} é um homomorfismo de grupos. Sejam $x', y' \in G$', e tomemos $x, y \in G$ de modo que $f(x) = x$' e $f(y) = y$'. Então, $f(xy) = x'y$'. Segue-se, por definição,

$$f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$$

isso prova que f^{-1} é um homomorfismo, como queríamos.

Por automorfismo de um grupo indicamos um isomorfismo desse grupo em si mesmo. A aplicação do exemplo 6 é um automorfismo do grupo comutativo G. Denotamos o conjunto dos automorfismos de G por $Aut(G)$.

2.4 Classes Laterais e Subgrupos Normais

Sejam S e S' subconjuntos de um grupo G. Definimos o produto desses subconjuntos por SS'= o conjunto de todos os elementos xx' com $x \in S$ e $x' \in S$'. É fácil verificar que se S_1, S_2 e S_3 são três subconjuntos de G, então

$$(S_1S_2)S_3 = S_1(S_2S_3)$$

esse produto consiste, simplesmente, de todos os elementos xyz, com $x \in S_1$, $y \in S_2$ e $z \in S_3$. Assim, o produto de subconjuntos é associativo.

Seja G um grupo, e H um subgrupo. Seja a um elemento de G. O conjunto de todos os elementos ax com $x \in H$ é chamado uma classe lateral de H em G. Denotamos essa classe por aH, seguindo a notação acima. Na notação aditiva, uma classe lateral de H será escrita $a + H$.

Como o grupo G pode não ser comutativo, o conjunto aH deveria ser chamado classe lateral à esquerda de H. De modo semelhante, podemos definir classes laterais à direita, mas, no que se segue, classe lateral, significará classe lateral à esquerda, a menos que se especifique o contrário.

Seja G um grupo, e H um subgrupo. Um subgrupo H é dito normal se ele satisfaz uma das seguintes condições equivalentes:

NOR 1. Para todo $x \in G$ temos $xH = Hx$, isto é, $xHx^{-1} = H$.

NOR 2. H é o núcleo de algum homomorfismo de G em algum grupo.

Vamos mostrar que essas duas condições são equivalentes. Suponhamos primeiro que H é o núcleo de um homomorfismo f. Então,

$$f(xHx^{-1}) = f(x)f(H)f(x)^{-1} = 1$$

assim $xHx^{-1} \subset H$ para todo $x \in G$, ou seja, $x^{-1}Hx \subset H$, o que implica em $H \subset xHx^{-1}$. Portanto $xHx^{-1} = H$. Com isso fica demonstrado que NOR 2 implica em NOR 1.

Comentário 2.1. A condição que se encontra em NOR 1 não significa o mesmo que $xhx^{-1} = h$ para todos os elementos $h \in H$, quando G não é comutativo. Entretanto, devemos observar que um subgrupo de um grupo comutativo é sempre normal e, portanto, satisfaz a condição que é mais forte do que NOR 1, ou seja, $xhx^{-1} = h$ para todo $h \in H$.

2.5 Aplicações para Grupos Cíclicos

Seja G um grupo cíclico, e a um gerador. Indiquemos por $d\mathbb{Z}$ o núcleo do homomorfismo

$$\mathbb{Z} \longrightarrow G \ \text{ tal que } \ n \longmapsto a^n$$

Quando o núcleo desse homomorfismo só possui o 0, temos um isomorfismo entre $\mathbb{Z}$ e G. No segundo caso, quando o núcleo não é zero, temos um isomorfismo

$$\mathbb{Z}/d\mathbb{Z} \xrightarrow{\approx} G$$

Teorema 2.1. Um homomorfismo é determinado, de forma única, pelos seus valores no conjunto de geradores.

Estendemos este resultado. Sejam G e G' grupos. Suponha que G é gerado por um subconjunto de elementos de S. Em outras palavras, todo elemento de G pode ser escrito como um produto

$$x = x_1 \cdots x_r \ \text{ com } \ x_i \in S \ \text{ ou } \ x_i^{-1} \in S$$

sejam $b_1, \cdots, b_r$ elementos de G'. Se existe um homomorfismo

$$f : G \longrightarrow G'$$

tal que $f(x_i) = b_i$, para $i = 1, \cdots, r$, então este homomorfismo é determinado de forma única. Em outras palavras, se

$$g : G \longrightarrow G'$$

é um homomorfismo tal que $g(x_i) = b_i$, para $i = 1, \cdots, r$, então $g = f$. A demonstração é imediata, pois para qualquer elemento x escrito como acima, isto é, $x = x_1 \cdots x_r$, com $x_i \in S$ ou $x_i^{-1} \in S$, temos

$$g(x) = g(x_1) \cdots g(x_r) = f(x_1) \cdots f(x_r) = f(x)$$

de forma clara, dados elementos arbitrários $b_1, \cdots, b_r \in G$' não existe necessariamente um homomorfismo $f : G \longrightarrow G$' tal que $f(x_i) = b_i$. Por vezes tal homomorfismo f existe, e em outras não.

2.6 Grupos de Permutações

Nesta seção, investigaremos mais de perto o grupo S_n das permutações de n elementos $\{1, \cdots, n\} = J_n$. Esse grupo é chamado grupo simétrico.

Se $\sigma \in S_n$, recordamos que $\sigma^{-1} : J_n \longrightarrow J_n$ é a permutação tal que $\sigma^{-1}(k) =$ único inteiro $j \in J_n$ tal que $\sigma(j) = k$. Uma transposição τ é uma permutação que troca as posições de dois números e que deixa os outros fixos, isto é, existem inteiros $i, j \in J_n$, $i \neq j$, tais que $\tau(i) = j, \tau(j) = i$, e $\tau(k) = k$ se $k \neq i$ e $k \neq j$. Percebe-se imediatamente que se τ é uma transposição, então $\tau^{-1} = \tau$ e $\tau^2 = I$. Em particular, a inversa de uma transposição é uma transposição. Vamos demonstrar que as transposições geram S_n.

Teorema 2.2. Toda permutação de J_n pode ser expressa como um produto de transposições.

Demonstração 2.4. Vamos demonstrar nossa proposição por indução sobre n. Para $n = 1$, não há nada a demonstrar. Suponhamos $n > 1$ e admitamos que a proposição seja verdadeira para $n - 1$. Seja σ uma permutação de J_n. Seja $\sigma(n) = k$. Seja τ a transposição de J_n tal que $\tau(k) = n$ e $\sigma(n) = k$. Então $\tau\sigma$ é uma permutação tal que

$$\tau\sigma(n) = \tau(k) = n$$

em outras palavras, $\tau\sigma$ deixa n fixo. Assim, podemos considerar $\tau\sigma$ como uma permutação de J_{n-1}, e por indução existem as transposições $\tau_1, \cdots, \tau_s$ de J_{n-1}, que deixam n fixo, de

modo que

$$\tau\sigma = \tau_1 \cdots \tau_s$$

podemos agora escrever

$$\tau = \tau^{-1}\tau_1 \cdots \tau_s$$

demonstrando assim nossa proposição.

Uma permutação σ de $\{1, \cdots, n\}$ algumas vezes é indicada por

$$\begin{bmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{bmatrix}$$

logo

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

denota a permutação σ tal que $\sigma(1) = 2$, $\sigma(2) = 1$, e $\sigma(3) = 3$. Essa permutação é de fato uma transposição.

Sejam $i_1, \cdots, i_r$ inteiros distintos em J_n. Com o símbolo

$$\begin{bmatrix} i_1 & \cdots & i_r \end{bmatrix}$$

representaremos a permutação σ tal que

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3\ \cdots,\ \sigma(i_r) = i_1$$

e que σ deixa todos os outros inteiros fixos. Por exemplo [132] denota a permutação σ tal que $\sigma(1) = 3$, $\sigma(3) = 2$, e $\sigma(2) = 1$, e sigma deixa fixados todos os outros inteiros. Tal permutação é chamada ciclo, ou, mais precisamente, r-ciclo.

Se $\sigma = [i_1 \cdots i_r]$ é um ciclo, verifica-se facilmente que σ^{-1} é também um ciclo, e que

$$\sigma^{-1} = [i_r \cdots i_1]$$

assim, se [132], então

$$\sigma^{-1} = [231]$$

note que um 2-ciclo [ij] nada mais é que uma transposição. Mais especificamente, uma transposição tal que $i \longrightarrow j$ e $j \longrightarrow i$.

Um produto de ciclos é determinado facilmente. Por exemplo,

$$[132][34] = [2134]$$

percebe-se isso se usando a definição: se $\sigma = [132]$ e $\tau = [34]$, então, por exemplo,

$$\sigma(\tau(3)) = \sigma(4) = 4$$

$$\sigma(\tau(4)) = \sigma(3) = 2$$

$$\sigma(\tau(2)) = \sigma(2) = 1$$

$$\sigma(\tau(1)) = \sigma(1) = 3$$

Seja G um grupo. Diremos que G é solúvel se existir uma sequencia de subgrupos

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_m = \{e\}$$

tal que H_i é normal em H_{i-1} e tal que o grupo quociente H_{i-1}/H_i é abeliano para $i = 1, \cdots, m$.

Capítulo 3

Anéis

Nesta seção, vamos axiomatizar as noções de adição e multiplicação.

Definição 3.1. Um anel $\mathbb{R}$ é um conjunto, cujos objetos podem ser adicionados e multiplicados, (isto é, são dadas as correspondências $(x, y) \longmapsto x + y$ e $(x, y) \longrightarrow xy$ de pares de $\mathbb{R}$, em $\mathbb{R}$) satisfazendo às seguintes condições:

AN 1. Sob a adição, $\mathbb{R}$ é um grupo aditivo (abeliano).

AN 2. Para todos os x, y e $z \in \mathbb{R}$ temos

$$(y + z) = xy + xz \text{ e } (y + z)x = yx + zx$$

AN 3. Para todos x, y e $z \in \mathbb{R}$ temos $(xy)z = x(yz)$.

AN 4. Existe um elemento $e \in \mathbb{R}$ tal que $ex = xe = x$ para todo $x \in R$.

Exemplo 3.1. Seja $\mathbb{R}$ o conjunto $\mathbb{N}$ dos inteiros; $\mathbb{R}$ é um anel.

Exemplo 3.2. Os conjuntos dos números racionais, reais e complexos são anéis.

Exemplo 3.3. Seja $\mathbb{R}$ o conjunto das funções contínuas com valores reais, definidas no intervalo [0, 1]. A soma e o produto de duas funções f e g são definidos da maneira usual, ou seja, $(f + g)(t) = f(t) + g(t)$ e $(fg)(t) = f(t)g(t)$. Com isso, $\mathbb{R}$ é um anel.

No caso geral, consideremos um conjunto não-vazio S e $\mathbb{R}$ um anel. Seja $M(S, \mathbb{R})$ o conjunto das aplicações de S em $\mathbb{R}$. Então, $M(S, \mathbb{R})$ é um anel se definirmos a soma e o produto de aplicações f, g pelas regras

$$(f + g)(x) = f(x) + g(x) \text{ e } (fg)(x) = f(x)g(x)$$

Exemplo 3.4 (O anel dos endomorfismos). Seja A um grupo abeliano. Denotemos por $Hom(A, A)$ o conjunto dos homomorfismos de A em si mesmo. Chamamos de $End(A)$

de conjunto dos endomorfismos de A. Assim, seguindo a notação do item 2.3, temos que $End(A) = Hom(A, A)$. Sabemos que $End(A)$ é um grupo aditivo.

- Se definirmos a lei de composição multiplicativa em $End(A)$ como sendo a composição de aplicações, $End(A)$ passa a ser um anel.

  Demonstração 3.1. Já sabemos que **AN 1** está satisfeita. Quanto a **AN 2**, sejam f, g e $h \in End(A)$. Então, para todo $x \in A$,

  $$(f \circ (g+h))(x) = f((g+h)(x)) = f(g(x)+h(x)) = f(g(x))+f(h(x)) = f \circ g(x)+f \circ h(x)$$

assim, $f \circ (g + h) = f \circ g + f \circ h$. De modo semelhante, demonstra-se que $(f + g) \circ h = f \circ h + g \circ h$. observamos que, neste caso, **AN 3** é nada menos que a associatividade de aplicações, um resultado já conhecido. O elemento unidade de **AN 4** é a aplicação identidade I. Vimos, assim, que $End(A)$ é um anel.

Um anel $\mathbb{R}$ é dito comutativo se $xy = yx$ para todos os x e $y \in \mathbb{R}$.

Os anéis dos exemplos 1, 2 e 3 são comutativos. Em geral, o anel do exemplo 4 não é comutativo.

Assim como ocorre com os grupos, o elemento e de um anel $\mathbb{R}$ que satisfaz **AN 4** é único, e é chamado elemento unidade do anel. Ele é normalmente indicado por 1. Notemos que, se $1 = 0$, então o anel $\mathbb{R}$ consiste unicamente do 0; neste caso, ele é chamado anel zero.

Podemos deduzir várias regras de aritmética a partir dos axiomas que definem um anel $\mathbb{R}$; passamos, em seguida, a listá-las:

- Temos $0x = 0$ para todo $x \in \mathbb{R}$.

  Demonstração 3.2. Escrevendo

  $$0x + x = 0x + ex = (0 + e)x = ex = x$$

  portanto, $0x = 0$.

- Temos ainda $(-e)x = -x$ para todo $x \in \mathbb{R}$.

  Demonstração 3.3.

  $$(-e)x + x = (-e)x + ex = (-e + e)x = 0x = 0$$

- Prova-se que $(-e)(-e) = e$.

Demonstração 3.4.

Multiplicamos a equação

$$e + (-e) = o$$

por $-e$, e obtemos

$$-e + (-e)(-e) = 0$$

somando e a ambos os membros, obtemos $(-e)(-e) = e$, como queríamos provar.

Também valem as relações

$$(-x)y = -xy \text{ e } (-x)(-y) = xy$$

para todos x e $y \in \mathbb{R}$.

Da condição **AN 2**, que é chamada distributividade, podemos deduzir regras semelhantes, envolvendo vários elementos; de fato, se x e $y_1, \cdots, y_n$ são elementos do anel $\mathbb{R}$, então

$$x(y_1 + \cdots + y_n = xy_1 + \cdots + xy_n)$$

da mesma forma, se $x_1, \cdots, x_m$ são elementos de $\mathbb{R}$, então

$$(x_1 + \cdots + x_m)(y_1 + \cdots + y_n) = x_1y_1 + \cdots + x_my_n = \sum_{i=1}^{m}\sum_{j=1}^{n} x_iy_i$$

a soma indicada no membro direito deve ser tomada sobre todos os índices i e j. Estas regras mais gerais podem ser demonstradas por indução.

Seja $\mathbb{R}$ um anel. Um subanel $\mathbb{R}$' de $\mathbb{R}$ é um subconjunto de $\mathbb{R}$ tal que o elemento unidade de $\mathbb{R}$ pertence a $\mathbb{R}$', e, se x e $y \in \mathbb{R}$', então $-x, x + y$ e xy também estão em $\mathbb{R}$'. Assim, de forma óbvia, $\mathbb{R}$' é um anel no qual as operações de adição e multiplicação são as mesmas de $\mathbb{R}$.

Exemplo 3.5. Os inteiros formam um subanel do conjunto dos números racionais, que, por sua vez, é um subanel do conjunto dos reais.

Exemplo 3.6. As funções reais diferenciáveis definidas sobre $\mathbb{R}$ formam um subanel do anel das funções contínuas.

Seja $\mathbb{R}$ um anel. Pode ocorrer a existência de elementos $x, y \in \mathbb{R}$ tais que $x \neq 0$ e $y \neq 0$, mas xy = 0. Tais elementos são chamados divisores de zero. Um anel comutativo sem divisores de zero, tal que $1 \neq 0$, é chamado anel de integridade. Um anel comutativo tal que o subconjunto de elementos não-nulos é um grupo sob a multiplicação é chamado corpo. Observe que, em um corpo, temos necessariamente $1 \neq 0$, e que este corpo não possui divisores de zero.

Exemplo 3.7. O conjunto $\mathbb{Z}$ dos inteiros é um anel de integridade. Todo corpo é um anel de integridade.

Seja $\mathbb{R}$ um anel. Denotamos por $\mathbb{R}^*$ o conjunto dos elementos $x \in \mathbb{R}$ para os quais existe $y \in \mathbb{R}$ tal que $xy = yx = e$. Em outras palavras, $\mathbb{R}^*$ é o conjunto formado pelos elementos de $\mathbb{R}$ que têm inverso multiplicativo. Os elementos de $\mathbb{R}^*$ são chamados unidades de $\mathbb{R}$. Por exemplo, as unidades de um corpo formam o grupo de elementos diferentes de zero do corpo.

Sejam $\mathbb{R}$ um anel e $x \in \mathbb{R}$. Se n é um inteiro positivo, definimos

$$x^n = x \cdots x$$

o produto tomado n vezes. Dessa forma, para inteiros positivos m e n temos

$$x^{n+m} = x^n x^m \quad \text{e} \quad (x^m)^n = x^{mn}$$

3.1 Ideais

Definição 3.2. Seja $\mathbb{R}$ um anel. Um ideal à esquerda de $\mathbb{R}$ é um subconjunto J de $\mathbb{R}$, dotado das seguintes propriedades: Se x e $y \in J$, então $x + y \in J$; o elemento zero está em J; e se $x \in J$ e $a \in R$, então $ax \in J$.

Utilizando o negativo $-e$, vemos que, se J é um ideal à esquerda, e $x \in J$, então também, $-x \in J$, pois $-x = (-e)x$. Assim, os elementos de um ideal à esquerda formam um subgrupo aditivo de R; podemos também dizer que um ideal à esquerda é um subgrupo aditivo J de $\mathbb{R}$ tal que, se $x \in J$ e $a \in \mathbb{R}$, então $ax \in J$.

Notemos que $\mathbb{R}$ é um ideal à esquerda, chamado ideal unitário e o mesmo acontecendo com o subconjunto de $\mathbb{R}$ formado unicamente pelo 0. Temos $J = \mathbb{R}$ se, e somente se $1 \in J$.

De modo semelhante, podemos definir um ideal à direita e um ideal bilateral. Desta forma, um ideal bilateral J é, por definição, um subgrupo aditivo de $\mathbb{R}$ tal que, se $x \in J$ e $a \in \mathbb{R}$, então ax e xa pertencem a J.

Exemplo 3.8. Seja $\mathbb{R}$ o anel das funções reais contínuas definidas no intervalo $[0, 1]$. Seja J o subconjunto das funções f tais que $f\dfrac{1}{2} = 0$. Então J é um ideal (bilateral, pois $\mathbb{R}$ é comutativo).

Exemplo 3.9. Seja $\mathbb{R}$ o anel $\mathbb{RZ}$ dos inteiros. Os inteiros pares, isto é, os do tipo $2n$, com $n \in \mathbb{Z}$, formam um ideal.

Exemplo 3.10. Sejam $\mathbb{R}$ um anel e a um elemento de $\mathbb{R}$. O conjunto dos elementos xa, com $x \in \mathbb{R}$, é um ideal à esquerda, chamado ideal à esquerda principal gerado por a. (Verifique, detalhadamente, que se trata de um ideal à esquerda). Esse ideal é denotado por (a). Mais geralmente, sejam $a_1, \cdots, a_n$ elementos de $\mathbb{R}$. O conjunto de todos os elementos

$$x_1a_1 + \cdots + x_na_n$$

com $x_i \in \mathbb{R}$, é um ideal à esquerda, denotado por $a_1, \cdots, a_n$. Chamamos $a_1, \cdots, a_n$ de **geradores** desse ideal.

Daremos uma demonstração completa desse fato, para mostrar o quanto ela é simples; $y_1, \cdots, y_n, x_1, \cdots, x_n \in \mathbb{R}$, então

$$(x_1a_1+\cdots+x_na_n)+(y_1a_1+\cdots+y_na_n) = x_1a_1+y_1a_1+\cdots+x_na_n+y_na_n = (x_1+y_1)a_1+\cdots+(x_n+y_n)a_n$$

se $z \in \mathbb{Z}$, então

$$z(x_1a_1 + \cdots + x_na_n) = zx_1a_1 + \cdots + zx_na_n$$

finalmente,

$$0 = 0a_1 + \cdots + 0a_n$$

isto prova que o conjunto de todos os elementos $x_1a_1 + \cdots + x_na_n$ com $x_i \in \mathbb{R}$, é um ideal à esquerda.

Exemplo 3.11. Seja $\mathbb{R}$ um anel, e sejam L e M ideais à esquerda. Denotamos por LM o conjunto de todos os elementos $x_1y_1 + \cdots + x_ny_n$ com $x_i \in L$ e $y_i \in M$. LM é também um ideal à esquerda. Se, L, M e N são ideais à esquerda, então $(LM)N = L(MN)$.

Exemplo 3.12. Sejam L e M ideais à esquerda. Definimos $L + M$ como sendo o subconjunto constituído por todos os elementos $x + y$, com $x \in L$ e $y \in M$. $L + M$ também é um ideal à esquerda. Se L, M e N são ideais à esquerda, então

$$L(M + N) = LM + LN$$

Exemplo 3.13. Seja L um ideal à esquerda. Denotemos por $L\mathbb{R}$ o conjunto de todos os elementos $x_1y_1 + \cdots + x_ny_n$ com $x_i \in L$ e $y_i \in \mathbb{R}$. Assim, $L\mathbb{R}$ é um ideal bilateral.

3.2 Homomorfismos

Sejam $\mathbb{R}$ e $\mathbb{R}$' dois anéis. Por um homomorfismo de anéis entendemos a aplicação dotada das seguintes propriedades: para todos x e $y \in \mathbb{R}$,

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(e) = e'$$

(se e e e' são, respectivamente, os elementos unidade de $\mathbb{R}$ e $\mathbb{R}$').

Entendemos por núcleo de um homomorfismo de anéis $f : \mathbb{R} \longrightarrow \mathbb{R}'$ o núcleo desse homomorfismo, quando é encarado como um homomorfismo de grupos aditivos; isto é, o conjunto de todos os elementos $x \in \mathbb{R}$ tais e $f(x) = 0$.

Exemplo 3.14. Seja $\mathbb{R}$ o anel das funções definidas no intervalo [0, 1], com valores complexos. A aplicação que a cada função $f \in \mathbb{R}$ associa o valor $f(1/2)$ é um homomorfismo de $\mathbb{R}$ em $\mathbb{C}$.

Exemplo 3.15. Seja $\mathbb{R}$ o anel das funções reais definidas no intervalo [0, 1]. Seja $\mathbb{R}$' o anel das funções reais definidas no intervalo [0, 1/2]. Cada função $f \in \mathbb{R}$ pode ser vista como uma função definida em [0, 1/2]; quando encarada dessa forma, damos-lhe o nome de restrição de f a [0, 1/2]. Mais geralmente, seja S um conjunto, e S' um subconjunto de S. Seja $\mathbb{R}$ o anel das funções reais definidas em S. Para cada $f \in \mathbb{R}$, denotamos por $f|S$' a função definida em S' cujo valor em um elemento $x \in S$' é $f(x)$. $f|S$' é chamada restrição de f a S'. Seja $\mathbb{R}$' o anel das funções reais definidas em S'. A aplicação

$$f \longmapsto f|S'$$

é um homomorfismo de anéis de $\mathbb{R}$ em $\mathbb{R}$'. Como o núcleo de um homomorfismo de anéis é definido somente em termos dos grupos aditivos envolvidos, fica-se sabendo que é injetor um homomorfismo de anéis cujo núcleo é trivial.

Seja $f : \mathbb{R} \longrightarrow \mathbb{R}$' um homomorfismo de anéis. Se existe um homomorfismo de anéis $g : \mathbb{R}' \longrightarrow \mathbb{R}$ tal que $g \circ f$ e $f \circ g$ são, respectivamente, as aplicações identidades de $\mathbb{R}$ e $\mathbb{R}$', dizemos que f é um isomorfismo de anéis. Um isomorfismo de um anel nele mesmo é chamado automorfismo.

Observação 3.1. Até aqui, fomos apresentados aos homomorfismos de grupo e homomorfismos de anéis, e demos a definição de isomorfismo de forma similar em cada uma dessas categorias de objetos. Nossas definições têm sido apresentadas num padrão completamente generalizável, isto é, podem ser aplicadas a outros objetos e categorias. Em geral, sem prejuízo para o objeto matemático com o qual se trabalha, pode-se usar a palavra morfismo no lugar de homomorfismo. Assim, um isomorfismo (em qualquer categoria) é um morfismo f para o qual existe um morfismo g que satisfaz

$$f \circ g = id \quad \text{e} \quad g \circ f = id$$

em outras palavras, é um morfismo que tem uma inversa.

O símbolo id representa a aplicação identidade. Para que essa definição geral faça sentido, duas propriedades precisam ser satisfeitas: a associatividade e a existência

de uma identidade para cada objeto. Dessa forma, um automorfismo é definido como um isomorfismo de um objeto em si mesmo. Assim, de forma completa, geral e direta, segue da definição que os automorfismos de um objeto formam um grupo. Um dos tópicos básicos de estudo da matemática é a estrutura de grupos de automorfismos de vários objetos.

Exemplo 3.16. Se $\mathbb{R} = \mathbb{Z}$, e n é um inteiro não-nulo, então $\mathbb{R}/(n) = \mathbb{Z}/(n)$ é chamado anel dos inteiros módulo n. Observamos que este anel é finito, contendo exatamente n elementos. Podemos também escrever $\mathbb{Z}/n\mathbb{Z}$ em vez de $\mathbb{Z}/(n)$.

Exemplo 3.17. Seja $\mathbb{R}$ um anel qualquer, com elemento unidade e.

Seja $a \in \mathbb{R}$. Desde que $\mathbb{R}$ também é um grupo abeliano aditivo, sabemos como definir na para qualquer inteiro n. Se n é positivo, então

$$na = a + a + \cdots + a$$

a soma sendo tomada n vezes. Se n é negativo, isto é, $n = -k$ com k positivo, então

$$na = -(ka)$$

em particular, podemos tomar $a = e$ e definir a aplicação

$$f : \mathbb{Z} \longrightarrow \mathbb{R} \text{ tal que } n \longmapsto ne$$

sabemos que essa aplicação f é um homomorfismo de grupos aditivos abelianos. Além disso, f é também um homomorfismo de anéis. De fato, inicialmente, notemos que para todo inteiro positivo n, vale a propriedade

$$(ne)a = (e + \cdots + e)a = ea + \cdots + ea = n(ea) = \underbrace{(a + \cdots + a)}_{\text{n vezes}} = na$$

se m e n são inteiros positivos, então assim, colocando $a = e$, obtemos

$$f(mn) = (mn)e = m(ne) = (me)(ne) = f(m)f(n)$$

a propriedade também é válida quando m ou n é negativo. Na demonstração usa-se m, n positivos, e a propriedade dos homomorfismos, dada por $f(-n) = -f(n)$.

Seja $f : \mathbb{Z} \longrightarrow \mathbb{R}$ um homomorfismo de anéis. Por definição, devemos ter $f(1) = e$. Assim, necessariamente, para todo inteiro positivo n devemos ter

$$f(n) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = ne$$

e para um inteiro negativo $m = k$,

$$f(-k) = -f(k) = -ke$$

portanto, existe um, e somente um homomorfismo de anéis de $\mathbb{Z}$ em um anel $\mathbb{R}$, do tipo definido anteriormente.

Teorema 3.1. Suponhamos que $\mathbb{R}$ seja um anel de integridade e, portanto, sem divisores de 0. Logo, o inteiro n tal que $\mathbb{Z}/n\mathbb{Z}$ está contido em $\mathbb{R}$, deve ser 0 ou um número primo.

Demonstração 3.5. Suponhamos que n não seja primo e não seja 0. Desta forma, $n = mk$ com inteiros m e $k \geq 2$ e não existe a possibilidade de m e k pertencerem ao núcleo do homomorfismo $f : \mathbb{Z} \longrightarrow \mathbb{R}$. Assim, $me \neq 0$ e $ke \neq 0$. Mas $(me)(ke) = mke = 0$ contradiz a hipótese de que $\mathbb{R}$ não tem divisores de 0. Portanto, n é primo.

Seja K um corpo, e $f : \mathbb{Z} \longrightarrow K$ o homomorfismo de inteiros em K. Se o núcleo de f é $\{0\}$, então K contém $\mathbb{Z}$ como um subanel e dizemos que K tem característica 0. Se o núcleo de f é gerado por um número primo, então dizemos que K tem característica p. O corpo $\mathbb{Z}/p\mathbb{Z}$, algumas vezes denotado por F_p, é chamado corpo primo de característica p. Esse corpo primo, F_p, está contido em todo corpo característica p.

Seja $\mathbb{R}$ um anel. Recordemos que uma unidade em $\mathbb{R}$ é um elemento $u \in \mathbb{R}$ que possui um inverso multiplicativo, isto é, existe um elemento $v \in \mathbb{R}$ tal que $uv = e$. O conjunto das unidades é denotado por $\mathbb{R}^*$. Esse conjunto de unidades é um grupo. De fato, se u_1 e u_2 são unidades, então o produto u_1u_2 é uma unidade, pois tem $u_2^{-1}u_1^{-1}$ como elemento inverso. Os outros axiomas relacionados com o grupo são imediatamente verificados a partir dos axiomas de anel concernentes à multiplicação.

Exemplo 3.18. Seja n um inteiro ≥ 2, e $\mathbb{R} = \mathbb{Z}/n\mathbb{Z}$. Então as unidades de $\mathbb{R}$ são os elementos de $\mathbb{R}$ que têm um representante $a \in \mathbb{Z}$, com a e n primos entre si. Este grupo de unidades é especialmente importante, e agora vamos descrever como ele ocorre na forma de grupo de automorfismos.

Teorema 3.2. Seja G um grupo multiplicativo e cíclico de ordem $\mathbb{Z}$. Considere $m \in \mathbb{Z}$ e $\mathbb{Z}$ primos entre si, e construa a aplicação

$$\sigma_m : G \longrightarrow G$$

tal que $\sigma_m(x) = x^m$. Então σ_m é um automorfismo de G, e a associação

$$m \longmapsto \sigma_m$$

induz um isomorfismo $(\mathbb{Z}/\mathbb{N}\mathbb{Z})^* \xrightarrow{\approx} Aut(G)$.

Demonstração 3.6. Desde que $\sigma_m(xy) = x^m y^m$ (pois G é comutativo) segue-se que σ_m é um homomorfismo de G em si mesmo. Como $(m, \mathbb{N}) = 1$ concluímos que $x^m = e \Longrightarrow x = e$. Logo, $nuc(\sigma_m)$ é trivial e como G é finito, segue-se que σ_m é bijetiva. Assim σ_m é um automorfismo. Se $m \equiv n \ \mathrm{mod}\mathbb{N}$, então $\sigma_m = \sigma_n$ e assim σ_n depende apenas da classe lateral de $mmod\sigma_{\mathbb{N}}\sigma_{\mathbb{Z}}$. Temos

$$\sigma mn(x) = x^{mn} = (x^n)^m = \sigma_n \sigma_m(x)$$

logo $m \longmapsto \sigma_m$ induz um homomorfismo de $(\mathbb{Z}/\mathbb{N}\mathbb{Z})^*$ em $Aut(G)$. Seja a um gerador de G. Se $\sigma_m = id$, então $a^m = a$. Daí $a^{m-1} = e$ e $\mathbb{N}|m-1$, ou seja, $m?1modN$. Dessa forma, o núcleo de $m \longmapsto \sigma_m$ em $(\mathbb{Z}/\mathbb{Z}\mathbb{Z})^*$ é trivial. Para finalizar, seja $f : G \longrightarrow G$ um automorfismo. Então $f(a) = a^k$, para algum $k \in \mathbb{Z}$, pois a é um gerador; além disso, como f é um automorfismo, devemos ter $(k, \mathbb{N}) = 1$, pois em caso contrário a^k não é gerador de G. Sendo assim, para todo $x \in G$, $x = a^i$ (i depende de x), obtemos

$$f(a^i) = f(a)^i = a^{ki} = (a^i)^k$$

e $f = \sigma_k$. Assim, o homomorfismo injetivo $(\mathbb{N}/\mathbb{N}\mathbb{Z})^* \longrightarrow Aut(G)$, dado por $m \longmapsto \sigma_m$, é sobrejetivo e, portanto, é um isomorfismo. CQD.

Seja $\mathbb{R}$ um anel comutativo e seja P um ideal. Definimos P como um ideal primo se $P \neq \mathbb{R}$, e, sempre que a e $b \in R$ e $ab \in P$, então $a \in P$ ou $b \in P$.

Seja $\mathbb{R}$ um anel comutativo e seja M um ideal. Definimos M como um ideal maximal se $M \neq \mathbb{R}$, e se não existe um ideal J tal que $\mathbb{R} \supset J \subset M$, com $\mathbb{R} \neq J$ e $J \neq M$.

3.3 Corpos quocientes

Nas seções precedentes, com o objetivo de darmos exemplos para conceitos mais abstratos, assumimos que o leitor já estava familiarizado com os números racionais. Estudaremos agora como se podem definir os números racionais a partir dos inteiros.

Antes de entrarmos na discussão abstrata, analisaremos de perto o caso dos números racionais. No ensino fundamental, o que se faz (ou o que se deveria fazer) é dar regras para se determinar quando dois quocientes de números racionais são iguais. Isso é necessário porque, por exemplo, $\frac{3}{4} = \frac{6}{8}$. O importante é que uma fração pode ser determinada por um par de números; neste exemplo, o par (3,4), mas também por outros pares, como por exemplo, (6,8). Se consideramos como equivalentes todos os pares que dão origem ao mesmo quociente, estamos dando um método para definir as frações, como sendo classes de equivalência. Em seguida, é necessário estabelecer regras para adicionar frações; as que daremos serão essencialmente as mesmas que são (ou deveriam ser) dadas

no ensino fundamental. Nossa discussão aplicar-se-á para um anel de integridade $\mathbb{R}$ arbitrário. (Lembre-se de que se um anel for de integridade, então $1 \neq 0$, R será comutativo e não terá divisores de zero).

Sejam (a, b) e (c, d) pares de elementos em $\mathbb{R}$, com $b \neq 0$ e $d \neq 0$. Diremos que esses pares são equivalentes se $ad = bc$. Afirmamos que essa é uma relação de equivalência.

Denotamos a classe de equivalência de (a, b) por a/b. Precisamos, agora, definir como somar e multiplicar tais classes.

Se a/b e c/d são classes de equivalência, definimos sua soma como

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

e seu produto como

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Naturalmente, devemos mostrar que, definindo a soma e o produto como foi feito, o resultado independe da escolha dos pares (a, b) e (c, d) que representam as classes dadas. Faremos isso para a soma. Suponhamos que

$$a/b = a'/b' \text{ e } c/d = c'/d'$$

devemos mostrar que

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$$

isso é verdadeiro se, e somente se,

$$b'd'(ad + bc) = bd(a'd' + b'c')$$

ou, em outras palavras,

(a) $b'd'ad + b'd'bc = bda'd' + bdb'c'$.

Mas, por hipótese, $ab' = a'b$ e $cd' = c'd$. Utilizando esse fato, vemos que a igualdade (a) se verifica.

Afirmamos, agora, que o conjunto de todos os quocientes a/b, com $b \neq 0$, é um anel, em que as operações de adição e multiplicação são definidas acima. Note, inicialmente, que existe um elemento unidade, a classe $1/1$, em que 1 é o elemento unidade de $\mathbb{R}$. É necessário, agora demonstrar a validade de todos os outros axiomas que definem um anel. Isso é cansativo, mas cada passo se apresenta de forma óbvia. Como exemplo, verificaremos a associatividade da adição. Para três quocientes

$a/b, c/d$ e e/f, temos

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{fad+fbc+bde}{bdf}$$

por outro lado

$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{cf+de}{df}=\frac{adf+bcf+bde}{bdf}$$

É claro que as expressões dos membros direitos são iguais em ambos os casos, o que prova a associatividade da adição. Os demais axiomas são de demonstração igualmente fácil, por isso omitiremos essa rotina tediosa. Vimos assim que nosso anel de quocientes é comutativo.

Denotemos o anel de todos os quocientes a/b por K. Afirmamos que K é um corpo. Para perceber isso, tudo que precisamos fazer é demonstrar que todo elemento não-nulo admite um inverso multiplicativo. Mas, o elemento zero de K é 0/1, e se a/b = 0/1 então a = 0. Desta forma, todo elemento não-nulo pode ser escrito na forma a/b, com b $\neq 0$ e a $\neq 0$. Seu inverso é então, b/a, como se pode perceber diretamente a partir da definição de multiplicação de quocientes.

Finalmente, note que temos uma aplicação

$$a \longmapsto a/1$$

Novamente, é rotineiro verificar que essa aplicação é um homomorfismo de anéis injetor. Todo homomorfismo de anéis injetor será chamado imersão. Vemos que $\mathbb{R}$ é imerso em K de uma maneira natural.

Chamamos K o corpo quociente de $\mathbb{R}$. Quando $\mathbb{R} = \mathbb{Z}$, então K é, por definição, o corpo dos números racionais.

Suponhamos que $\mathbb{R}$ seja um subanel de um corpo F. O conjunto de todos os elementos ab^{-1}, com $a, b \in \mathbb{R}$ e $b \in 0$ é evidentemente um corpo, que é um subcorpo de F. Chamamos esse corpo também de corpo quociente de $\mathbb{R}$ em F. Esta terminologia não pode dar origem a confusões, pois o corpo quociente de $\mathbb{R}$, como foi definido previamente, é isomorfo a este corpo, sob a aplicação

$$a/b \longmapsto ab^{-1}$$

a verificação é trivial, e, em vista disso, o elemento ab^{-1} de F é também denotado por a/b.

Exemplo 3.19. Seja K um corpo e seja $\mathbb{Q}$, como é usual, o conjunto dos números racionais. Não existe necessariamente uma imersão de $\mathbb{Q}$ em K (K pode, por exemplo, ser finito). Mas, por outro lado, se existe uma imersão de $\mathbb{Q}$ em K, ela é única. Isso pode ser visto facilmente, pois todo homomorfismo

$$f : Q \longrightarrow K$$

deve ser tal que $f(1) = e$ (o elemento unidade de K). Logo, para qualquer inteiro $n > 0$, percebe-se, por indução, que $f(n) = ne$, e, consequentemente,

$$f(-n) = -ne$$

além disso,

$$e = f(1) = f(nn^{-1}) = f(n)f(n^{-1})$$

e assim $f(n^{-1}) = f(n)^{-1} = (ne)^{-1}$. Como consequência, para todo quociente $m/n = mn^{-1}$, onde m e n são inteiros e $n > 0$, devemos ter

$$f(m/n) = (me)/(ne)^{-1}$$

mostrando, assim, que f é determinada de modo único. Logo, costuma-se considerar $\mathbb{Q}$ imerso em K, e enxergar todo número racional como um elemento de K.

Finalmente, passamos a fazer algumas observações sobre a extensão de uma imersão de um anel em um corpo.

Seja $\mathbb{R}$ um anel de integridade, e

$$f : \mathbb{R} \longrightarrow E$$

uma imersão de $\mathbb{R}$ em algum corpo E. Seja K o corpo quociente de $\mathbb{R}$. Então, f admite uma única extensão a uma imersão de K em E, ou seja, uma imersão $f* : K \longrightarrow E$ cuja restrição a $\mathbb{R}$ é igual a f.

Para ver a unicidade, observe que, se f^* é uma extensão de f, e

$$f* : K \longrightarrow E$$

é uma imersão, então para todos a e $b \in \mathbb{R}$ devemos ter

$$f^*(a/b) = f^*(a)/f^*(b) = f(a)/f(b)$$

e assim o efeito de f^* sobre K é determinado pelo efeito de f sobre $\mathbb{R}$. Reciprocamente,

pode-se definir f^* pela fórmula

$$f * (a/b) = f(a)/f(b)$$

e percebe-se imediatamente que o valor de f^* independe da escolha de representação do quociente a/b; isto é, se $a/b = c/d$ com

$$a, b, c \text{ e } d \in \mathbb{R} \text{ e } bd \neq 0$$

então

$$f(a)/f(b) = f(c)/f(d)$$

verifica-se também facilmente que f^*, definida desta forma, é um homomorfismo, provando, assim, a sua existência.

Capítulo 4

Espaços vetoriais

4.1 Espaços vetoriais e bases

Definição 4.1. Seja K um corpo. Um espaço vetorial V sobre o corpo K é um grupo aditivo (abeliano), mais a operação de multiplicação de elementos de V por elementos de K, isto é, uma associação

$$(x, y) \longmapsto xv$$

de KxV em V, que satisfaz às seguintes condições:

EV 1. Se 1 é o elemento unidade de K, então $1v = v$ para todo $v \in V$.

EV 2. Se $c \in K$ e $v, w \in V$, então $c(v + w) = cv + cw$.

EV 3. Se $x, y \in K$ e $v \in V$, então $(x + y)v = xv + yv$.

EV 4. Se $x, y \in K$ e $v \in V$, então $(xy)v = x(yv)$.

Exemplo 4.1. Seja V o conjunto das funções contínuas no intervalo [0,1] com valores reais. V é um espaço vetorial sobre $\mathbb{R}$. A adição de funções é definida da maneira usual: se f, g são funções, definimos

$$(f + g)(t) = f(t) + g(t)$$

Se $c \in \mathbb{R}$ definimos (cf)(t) = cf(t). Logo, é uma simples questão de rotina verificar que todas as quatro condições serão atendidas.

Exemplo 4.2. Seja S um conjunto não-vazio, e seja V o conjunto de todas as aplicações de S em K. Então V é um espaço vetorial sobre K, em que a adição de aplicações e a multiplicação por elementos de K são definidas como para as funções do exemplo precedente.

Exemplo 4.3. Denotemos por K^n o produto $K \times \cdots \times K$, isto é, o conjunto das n-uplas de elementos de K. (Se K=R, tem-se o espaço euclidiano usual). Definimos a adição de n-uplas componente a componente, isto é, se

$$X = x_1, cdots, x_n \text{ e } Y = y_1, cdots, y_n$$

são elementos de K^n com $x_i, y_i \in K$, então definimos

$$X + Y = (x_1 + y_1, \cdots, x_n + y_n)$$

Se $c \in K$, definimos

$$cX = (cx_1, \cdots, cx_n)$$

verifica-se facilmente que estas operações satisfazem todas as condições de um espaço vetorial.

Exemplo 4.4. Tomando-se $n = 1$ no exemplo 3, vê-se que K é um espaço vetorial sobre si mesmo.

- Seja V um espaço vetorial sobre o corpo K. Seja $v \in V$. Então, $0v = 0$.

  Demonstração 4.1. $0v + v = 0v + 1v = (0 + 1)v = 1v = v$. Logo, adicionando-se $-v$ a ambos os membros, mostra-se que $0v = 0$.

  Se $c \in K$ e cv = 0, mas $c \neq 0$, então $v = 0$.

  Para ver isto, multiplique por c^{-1} para obter $c^{-1}cv = 0$, e, portanto $v = 0$.

- Temos $(-1)v = -v$.

  Demonstração 4.2. $(-1)v + v = (-1)v + 1v = (-1 + 1)v = 0v = 0$. Logo, $(-1)v = -v$.

  Sejam V um espaço vetorial e W um subconjunto de V. Diremos que W é um subespaço de V se for um subgrupo (do grupo aditivo de V), e se, dados $c \in K$ e $v \in W$, cv for também um elemento de W. Em outras palavras, um subespaço W de V é um subconjunto que satisfaz às seguintes condições:

  i Se v, w são elementos de W, então sua soma $v + w$ é também um elemento de W.

  i O elemento 0 de V é também um elemento de W.

  i Se $v \in W$ e $c \in K$, então $cv \in W$.

Portanto, W é, por sua vez, um espaço vetorial. De fato, como as propriedades **EV 1** a **EV 4**, são satisfeitas por todos os elementos de V, são satisfeitas a fortiori pelos elementos de W.

Seja V um espaço vetorial, e $w_1, \cdots, w_n$ elementos de V. Seja W o conjunto de todos os elementos

$$x_1 w_1 + \cdots + x_n w_n$$

com $x_i \in K$. Então W é um subespaço de V, como se pode verificar sem dificuldades. Ele é chamado subespaço gerado por $w_1, \cdots, w_n$, e dizemos que $w_1, \cdots, w_n$ são geradores desse subespaço.

Seja V um espaço vetorial sobre um corpo K, e sejam $v_1, \cdots, v_n$ elementos de V. Diremos que $v_1, \cdots, v_n$ são linearmente dependentes sobre K se existirem elementos $a_1, \cdots, a_n$ em K, nem todos iguais a 0, tais que

$$a_1 v_1 + \cdots + a_n v_n = 0$$

Se não existirem tais elementos, então diremos que $v_1, \cdots, v_n$ são linearmente independentes sobre K. Frequentemente omitimos as palavras "sobre K".

Exemplo 4.5. Seja $V = K^n$ e consideremos os vetores

$$v_1 = (1,\ 0,\ \cdots,\ 0)$$

$$\vdots$$

$$v_n = (0,\ 0,\ \cdots,\ 1)$$

Então $v_1, \cdots, v_n$ são linearmente independentes. De fato, sejam $a_1, \cdots, a_n$ elementos de K tais que $a_1 v_1 + \cdots + a_n v_n = O$ como

$$a_1 v_1 + \cdots + a_n v_n = (a_1, \cdots, a_n)$$

segue-se que todos os $a_i = 0$.

Exemplo 4.6. Seja V o espaço vetorial de todas as funções de uma variável t. Sejam $f_1(t), \cdots, f_n(t)n$ funções. Dizer que elas são linearmente dependentes é dizer que existem n números $a_1, \cdots, a_n$, não todos iguais a 0, tais que

$$a_1 f_1(t) + \cdots + a_n f_n(t) = O$$

para todos os valores de t.

As duas funções e^t e e^{2t} são linearmente independentes. Para prová-lo suponhamos que existam números a e b tais que

$$ae^t + be^{2t} = 0$$

(para todos os valores de t). Diferenciando esta relação, obtemos

$$ae^t + 2be^{2t} = 0$$

Subtraiamos a primeira relação da segunda. Resulta que $be^{2t} = 0$, e, portanto $b = 0$. Da primeira expressão, segue-se que $ae^t = 0$, e assim a = 0. Logo, e^t e e^{2t} são linearmente independentes.

Consideremos, outra vez, um espaço vetorial V arbitrário sobre o corpo K. Sejam $v_1, \cdots, v_n$ elementos linearmente independentes de V. Sejam $x_1, \cdots, x_n$ e $y_1, \cdots, y_n$ números. Suponhamos que temos

$$x_1v_1 + \cdots x_nv_n = y_1v_1 + \cdots y_nv_n$$

Em outras palavras, que duas combinações lineares de $v_1, \cdots, v_n$ sejam iguais. Então, deve-se ter $x_i = y_i$ para cada $i = 1, \cdots, n$. Com efeito, subtraindo o segundo membro do primeiro, obtemos

$$x_1v_1 - y_1v_1 + \cdots + x_nv_n - y_nv_n = 0$$

podemos escrever essa relação na forma

$$(x_1 - y_1)v_1 + \cdots + (x_n - y_n)v_n = 0$$

por definição, devemos ter $x_i - y_i = 0$ para todo $i = 1, \cdots, n$, demonstrando, assim, a nossa afirmação.

Definição 4.2 (**Definição de Base**)**.** Definimos uma base de V sobre K como uma sequência de elementos $\{v_1, \cdots, v_n\}$ de V que geram V, e que são linearmente independentes.

Os vetores $v_1, \cdots, v_n$ do exemplo 5 formam uma base de K^n sobre K.

Seja W o espaço vetorial gerado, sobre $\mathbb{R}$, pelas duas funções e^t e e^{2t}. Então $\{e^t, e^{2t}\}$ é uma base de W sobre $\mathbb{R}$.

Seja V um espaço vetorial, e seja $v_1, \cdots, v_n$ uma base de V. Os elementos de V podem ser representados por n-uplas relativas a essa base, da seguinte maneira: se um

elemento v de V é escrito como uma combinação linear

$$v = x_1 v_1 + \cdots + x_n v_n$$

dos elementos da base, chamamos $(x_1, \cdots, x_n)$ as coordenadas de v com respeito à nossa base, e dizemos que x_i é a i-ésima coordenada. Dizemos também que a n-upla $X = (x_1, \cdots, x_n)$ é o vetor-coordenada de v com respeito à base $\{v_1, \cdots, v_n\}$. Seja V, por exemplo, o espaço vetorial gerado pelas duas funções e^t, e^{2t}. Então, as coordenadas da função

$$3e^t + 5e^{2t}$$

com respeito à base $\{e^t, e^{2t}\}$ são (3,5).

Exemplo 4.7. Mostre que os vetores (1, 1) e (-3, 2) são linearmente independentes sobre $\mathbb{R}$.

Sejam a e b dois números tais que

$$a(1,1) + b(-3,2) = O$$

Escrevendo esta equação em termos de suas componentes, encontramos

$$a - 3b = 0$$

$$a + 2b = 0$$

esse é um sistema de duas equações que resolvemos para a e b. Subtraindo a segunda da primeira, obtemos $-5b = 0$, e assim $b = 0$. Substituindo em qualquer das duas equações, resulta $a = 0$. Portanto a e b são ambos iguais a 0, e nossos vetores são linearmente independentes.

Exemplo 4.8. Encontre as coordenadas de (1, 0) com respeito aos dois vetores (1, 1) e (-1, 2).

Devemos achar números a e b tais que

$$(1,1) + b(-1,2) = (1,0)$$

Escrevendo esta equação em termos de suas coordenadas, obtemos

$$a - b = 1$$

$$a + 2b = 0$$

resolvendo para a e b da maneira usual, resulta $b = -\frac{1}{3}$ e $a = \frac{2}{3}$. Logo, as coordenadas

de (1, 0) com respeito a (1, 1) e (-1, 2) são $(\frac{2}{3}, -\frac{1}{3})$.

Seja $\{v_1, \cdots, v_n\}$ um conjunto de elementos de um espaço vetorial V sobre um corpo K. Seja r um inteiro positivo $\leq n$. Diremos que $\{v_1, \cdots, v_r\}$ é um subconjunto maximal de elementos linearmente independentes, se $v_1, \cdots, v_r$ forem linearmente independentes, e se, além disto, dado qualquer v_i com $i > r$, os elementos $v_1, \cdots, v_r, v_i$ serão linearmente dependentes.

O próximo teorema fornece um critério prático para decidir se um conjunto de elementos de um espaço vetorial é uma base.

Teorema 4.1. Seja $\{v_1, \cdots, v_n\}$ o conjunto de geradores de um espaço vetorial V. Seja $\{v_1, \cdots, v_r\}$ um subconjunto maximal de elementos linearmente independentes. Então $\{v_1, \cdots, v_r\}$ é uma base de V.

Demonstração 4.3. Devemos provar que $v_1, \cdots, v_r$ geram V. Provaremos inicialmente que cada v_i (para $i > r$) é uma combinação linear de $v_1, \cdots, v_r$· Por hipótese, dado v_i, existem números $x_1, \cdots, x_r, y \in K$, não todos nulos, tais que

$$x_1 v_1 + \cdots + x_r v_r + y v_i = 0$$

além disso, $y \neq 0$, pois de outra forma, obteríamos uma relação de dependência linear para $v_1, \cdots, v_r$. Portanto, podemos resolver para v_i, ou seja,

$$v_i = \frac{x_1}{-y} v_1 + \cdots + \frac{x_r}{-y} v_{r'}$$

mostrando, assim, que v_i é uma combinação linear de $v_1, \cdots, v_r$.

Em seguida, seja v um elemento qualquer de V. Existem $c_1, \cdots, c_n \in K$ tais que

$$v = c_1 v_1 + \cdots + c_n v_n$$

Nesta relação, podemos substituir cada $v_i (i > r)$ por uma combinação linear de $v_1, \cdots, v_r$. Fazendo isto, e depois agrupando os termos semelhantes, conseguimos expressar v como uma combinação linear de $v_1, \cdots, v_r$. Isto prova que $v_1, \cdots, v_r$ geram V, formando, assim uma base de V.

Sejam V, W espaços vetoriais sobre K. Uma aplicação

$$f : v \longrightarrow W$$

é chamada aplicação K-linear, ou homomorfismo de espaços vetoriais, se f satisfizer às

seguintes condições: Para todos $x \in K$ e $v, v' \in V$ temos

$$f(v+v') = f(v) + f(v'), f(xv) = xf(v)$$

assim, f é um homomorfismo de V em W se estes conjuntos forem vistos como grupos aditivos, e satisfizerem à condição adicional de que $f(xv) = xf(v)$. Dizemos, usualmente, "aplicação linear" em vez de "aplicação K-linear".

Teorema 4.2. Sejam V e W dois espaços vetoriais, e $v_1, \cdots, v_n$ uma base de V. Sejam $w_1, \cdots, w_n$ elementos de W. Então, existe uma única aplicação linear $f : V \longrightarrow W$ tal que $f(v_i) = w_i$ para todo i.

Demonstração 4.4. A aplicação K-linear é determinada de modo único,

$$v = x_1v_1 + \cdots + x_nv_n$$

é um elemento de V, com $x_i \in K$, então devemos ter necessariamente pois se

$$f(v) = x_1f(v_1) + \cdots + x_nf(v_n) = x_1w_1 + \cdots + x_nw_n$$

aplicação f existe, pois, dado um elemento v como acima, definimos $f(v)$ como $x_1w_1 + \cdots + x_nw_n$. Devemos assim verificar se f é uma aplicação linear. Seja

$$v' = y_1v_1 + \cdots + y_nv_n$$

um elemento de V com $y_i \in K$. Então

$$v + v' = (x_1 + y_1)v_1 + \cdots + (x_n + y_n)v_n$$

portanto,

$$f(v+v') = (x_1+y_1)w_1+\cdots+(x_n+y_n)w_n = x_1w_1+y_1w_1+\cdots+x_nw_n+y_nw_n = f(v)+f(v')$$

se $c \in K$, então $cv = cx_1v_1 + \cdots + cx_nv_n$, e assim

$$f(cv) = cx_1w_1 + \cdots + cx_nw_n = cf(v)$$

isto prova que f é linear, e concluindo a demonstração do teorema.

O núcleo de uma aplicação linear é definido como o núcleo dessa aplicação quando é vista como um homomorfismo de grupos aditivos. Logo, $Nucf$ é o conjunto dos $v \in V$ tais que $f(v) = 0$.

Como foi feito para os grupos, dizemos que uma aplicação linear $f : V \longrightarrow W$ é

um isomorfismo (isto é, um isomorfismo de espaços vetoriais) se existir uma aplicação linear $g : W \longrightarrow V$ tal que $g \circ f$ seja a aplicação identidade de V, e $f \circ g$ seja a aplicação identidade de W. A observação precedente mostra que uma aplicação linear é um isomorfismo se, e somente se, ela for bijetiva.

Sejam V e W espaços vetoriais sobre o corpo K. Indicamos por $Hom_K(V, W) =$ conjunto de todas as aplicações lineares de V em W. Sejam $f, g : V \longrightarrow W$ aplicações lineares. Assim, podemos definir a soma $f + g$ da mesma forma como foi definida a soma de aplicações de um conjunto em W. Logo, por definição

$$(f + g)(v) = f(v) + g(v)$$

se $c \in K$, então definimos cf como sendo a aplicação tal que

$$(cf)(v) = cf(v)$$

mom estas definições, é fácil verificar que $Hom_K(V, W)$ é um espaço vetorial sobre K. caso $V = W$, chamamos os homomorfismos (ou K-aplicações lineares) de V em si mesmo de endomorfismos de V, e os indicamos por

$$End_K(V) = Hom_K(V, V)$$

4.2 Dimensão de um Espaço Vetorial

O resultado principal desta seção é que duas bases quaisquer de um espaço vetorial têm o mesmo número de elementos. Para provar isso, teremos antes que obter um resultado intermediário.

Teorema 4.3. Seja V um espaço vetorial sobre um campo K e considere $\{v_1, \cdots, v_m\}$ uma base de V sobre $\mathbb{K}$. Sejam $w_1, \cdots, w_n$ elementos de V, e suponha que $n > m$. Então $w_1, \cdots, w_n$ são linearmente dependentes.

Demonstração 4.5. Suponhamos que $w_1, \cdots, w_n$ sejam linearmente independentes. Sendo $\{v_1, \cdots, w_m\}$ uma base, existem elementos $a_1, \cdots, a_m \in \mathbb{K}$ tais que

$$w_1 = a_1 v_1 + \cdots + a_m v_m$$

por hipótese, sabemos que $w_1 \neq 0$, e portanto existe algum $a_i \neq 0$. Após renumerar $v_1, \cdots, v_m$, se necessário for, podemos supor. sem perda de generalidade que $a_1 \neq 0$. Podemos então resolver para v_1, e chegar a

$$a_1 v_1 = w_1 - a_2 v_2 - \cdots - a_m v_m$$

$$v_1 = a_1^{-1}w_1 - a_1^{-1}a_2v_2 - \cdots - a_1^{-1}a_mv_m$$

o subespaço de V gerado por $w_1, v_2, \cdots, v_m$ contém v_1 e, portanto deve coincidir com V, pois $v_1, \cdots, v_m$ geram V. A ideia agora é continuar neste processo passo a passo, e substituir sucessivamente $v_2, v_3, \cdots$ por $w_2, w_3, \cdots$ até que se esgotem todos os elementos $v_1, \cdots, v_m$, e $w_1, \cdots, w_m$ gerem V. Suponhamos agora por indução que exista um número inteiro r, $1 \leq r < m$, tal que, após uma adequada reordenação de $v_1, \cdots, v_m$, os elementos $w_1, \cdots, w_r, v_{r+1}, \cdots, v_m$ gerem V. Por outro lado, existem elementos

$$b_1, \cdots, b_r, c_{r+1}, \cdots, c_m$$

em $\mathbb{K}$, tais que

$$w_{r+1} = b_1v_1 + \cdots + b_rw_r + c_{r+1}v_{r+1} + \cdots + c_mv_m$$

Não podemos ter $c_j = 0$ para $j = r+1, \cdots, m$, pois neste caso encontraríamos uma relação de dependência linear entre $w_1, \cdots, w_{r+1}$, contradizendo nossa afirmação. Após reordenarmos $v_{r+1}, \cdots, v_m$ se necessário for, podemos supor, sem perda de generalidade, que $c_{r+1} \neq 0$. Obtemos então

$$c_{r+1}v_{r+1} = w_{r+1} - b_1w_1 - \cdots - b_rw_r - c_{r+2}v_{r+2} - \cdots - c_mv_m$$

dividindo por c_{r+1}, concluímos que v_{r+1} está no subespaço gerado por

$$w_1, \cdots, w_{r+1}, v_{r+2}, \cdots, v_m$$

pela nossa hipótese de indução, segue-se que $w_1, \cdots, w_{r+1}, v_{r+2}, \cdots, v_m$ geram V. Assim, por indução, provamos que $w_1, \cdots, w_m$ geram V. Se escrevermos

$$w_{m+1} = x_1w_1 + \cdots + x_mw_m$$

com $x_i \in K$, obtemos uma relação de dependência linear

$$w_{m+1} - x_{1w_1} - \cdots - x_mw_m = 0$$

como era para ser mostrado.

Teorema 4.4. Seja V um espaço vetorial e suponhamos que uma base tenha n elementos, e outra m elementos. Então $m = n$.

Demonstração 4.6. Aplicamos o teorema 12.3 e encontramos $n \leq m$ e $m \leq n$ e, portanto $m = n$.

Se um espaço tem uma base, então qualquer outra base tem o mesmo número de elementos. Este número é a dimensão de V (sobre $\mathbb{K}$), ou que V é n-dimensional. Se V é

constituído apenas pelo elemento O, então dizemos que V tem dimensão 0.

Corolário 4.1. Seja V um espaço vetorial e seja W um subespaço contendo n elementos linearmente independentes. Então $W = V$.

Demonstração 4.7. Sejam $v \in V$ e $w_1, \cdots, w_n$ elementos linearmente independentes de W. Então $w_1, \cdots, w_n, v$ são linearmente dependentes, e assim existem $a, b_1, \cdots, b_n \in K$ nem todos nulos, tais que

$$av + a_1v_1 + \cdots + b_nw_n = 0$$

Não podemos ter $a = 0$, pois se assim fosse, $w_1, \cdots, w_n$ seriam linearmente dependentes. Logo,

$$v = -a^{-1}b_1w_1 - \cdots - a^{-1}b_nw_n$$

é um elemento de W. Isto prova que $V \subset W$ e, portanto $V = W$.

Teorema 4.5. Seja $f : V \longrightarrow W$ um homomorfismo de espaços vetoriais sobre $\mathbb{K}$. Suponhamos que V e W tenham dimensão finita e que $dimV = dimW$. Se $Nucf = 0$ ou se $Imf = W$, então f é um isomorfismo.

Demonstração 4.8. Supondo-se que $Nucf = 0$. Seja $\{v_1, \cdots, v_n\}$ uma base de V. Então $f(v_1), \cdots, f(v_n)$ são linearmente independentes, pois considerando $c_1, \cdots, c_n \in \mathbb{K}$, tais que

$$c_1f(v_1) + \cdots + c_nf(v_n) = 0$$

ou

$$f(c_1v_1 + \cdots + c_nv_n) = 0$$

e como f é injetiva, temos $c_1v_1 + \cdots + c_nv_n = 0$. Logo, como $\{v_1, \cdots, v_n\}$ é uma base de V, $c_i = 0$ para $i = 1, \cdots, n$. Portanto Imf é um subespaço de W de dimensão n, e pelo corolário 12.1 $Imf = W$. Logo, f é também sobrejetiva e, portanto um isomorfismo.

Seja V um espaço vetorial. Definimos um automorfismo de V como sendo uma aplicação linear invertível

$$f : V \longrightarrow V$$

de V em si mesmo. Denotamos o conjunto de automorfismo de V por

$$Aut(V) \text{ ou } LG(V)$$

as letras LG representam "Linear Geral".

Teorema 4.6. O conjunto $Aut(V)$ é um grupo.

Demonstração 4.9. A multiplicação é a composição de aplicações. Esta composição é associativa; além disso, já vimos que a inversa de uma aplicação é linear, e a identidade também. Logo, todos os axiomas de grupo se verificam.

Capítulo 5

Extensão de Corpos

5.1 Extensão de Corpos

Definição 5.1. Um corpo L é uma extensão de um corpo K se $L \supset K$ e se as operações de L restritas a K coincidem com as operações de K.

Noutros termos, $(K, +, \cdot)$ é subcorpo de $(L, \oplus, \odot)$, isto é, $L \supset K$ e para todo $a, b \in K$ vale

$$a \oplus b = a + b \in K \quad \text{e} \quad a \odot b = a \cdot b \in K$$

Seja $L \in K$ uma extensão de corpos. Dados $a, b \in K$ e $u, v, w \in L$ temos que

1. $u + v = v + u$
2. $(u + v) + w = u + (v + w)$
3. $0_L + u = u$
4. $\exists - u \in L$ tal que $-u + u = 0_L$
5. $(a \cdot b) \cdot u = a \cdot (b \cdot u)$
6. $(a + b) \cdot u = a \cdot u + b \cdot u$
7. $a \cdot (u + v) = a \cdot (u + v)$
8. $1_K \cdot u = u$.

Essas oito propriedades decorrem do fato de L ser um corpo e K um subcorpo de L e fazem da estrutura $(L, K, +, \cdot)$ um espaço vetorial, onde L é o conjunto de vetores, K é o conjunto de escalares, $+$ é soma de L e $\cdot$ representa o produto de L, que na estrutura vetorial só faz sentido se feito entre escalares de K e vetores de L. Do ponto de vista vetorial, questões sobre dependência linear, geradores, base e dimensão ganham pertinência.

Definição 5.2. Dizemos que $L \supset K$ é uma extensão finita se L tem dimensão finita como espaço vetorial sobre K e definimos o grau da extensão com sendo

$$[L : K] = \dim_K L$$

Caso contrário diremos que $L \supset K$ é uma extensão infinita.

Exemplo 5.1. $\mathbb{C} \supset \mathbb{R}$ é uma extensão finita pois $[\mathbb{C} : \mathbb{R}] = 2$. Com efeito, basta notar que $\{1, i\}$ é uma base de $\mathbb{C}$ sobre $\mathbb{R}$.

Exemplo 5.2. Seja $\mathbb{Q}\sqrt{2} = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\}$. É fácil ver que $\mathbb{Q}\sqrt{2}$ é uma extensão finita de $\mathbb{Q}$ e que $[\mathbb{Q}\sqrt{2} : \mathbb{Q}] = 2$.

Exemplo 5.3. $\mathbb{R} \supset \mathbb{Q}$ é uma extensão infinita. Com efeito, considere o conjunto das potências de π

$$S = \{\pi^n/n \in \mathbb{Z} \text{ e } n \geq 0$$

uma vez que π não é raiz de nenhum polinômio com coeficientes racionais (Lindemann, 1882), temos que qualquer subconjunto finito de S é LI. Portanto, $\mathbb{R} \supset \mathbb{Q}$ é uma extensão infinita.

Teorema 5.1. Se $L \supset F$ e $K \supset F$ são extensões finitas então $L \supset F$ é extensão finita e vale a equação

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

Demonstração 5.1. Ponha $[L : K] = n$ e $[K : F] = m$ e sejam $\{u_1, \cdots, u_n\}$ uma base de L sobre K e $\{a_1, \cdots, a_m\}$ uma base de K sobre F. Vamos provar que o conjunto

$$\beta = \{a_i u_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

possui $n \cdot m$ elementos e constitui uma base de L sobre F. Primeiramente, se $a_i u_j = a_k u_l$ então os vetores u_j e u_l são LD, donde segue que $j = l$. Temos assim que $(a_i - a_k)u_j = 0$ e como $u_j \neq 0$, resta que $a_i = a_k$. Isso prova que β tem $n \cdot m$ elementos.

Seja $v \in L$. Então existem $y_1, \cdots, y_n \in K$ tais que

$$v = \sum_{i=1}^{n} y_i u_i$$

por sua vez cada y_i é uma combinação linear de $a_1, \cdots, a_m$, isto é, existem escalares $x_1, \cdots, x_n \in F$ de modo que

$$y_i = \sum_{j=1}^{n} x_{ij} a_j$$

assim,

$$v = \sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij}a_j u_i$$

o que prova ser β um conjunto de geradores para L.

Finalmente, suponha que $x_{ij} \in F$ são escalares tais que

$$\sum_{i,j} x_{ij}a_i u_j = 0$$

eearranjando as parcelas convenientemente, obtem-se

$$\sum_{j}^{n}\left(\sum_{i}^{m}\right) u_j = 0 \Longrightarrow \forall j, \sum_{i}^{m} x_{ij}a_i = 0$$

pois o conjunto $\{u_1, \cdots, u_n\}$ é LI. Da mesma forma

$$\forall\ j, \sum_{i}^{m} x_{ij}a_i = 0 \Longrightarrow \forall\ i, j, x_{ij} = 0$$

Teorema 5.2. Sejam L e K duas extensões finitas do corpo F. Se $f : L \longrightarrow K$ é um isomorfismo de corpos tal que $f(c) = c$ para todo $c \in F$, então $[L : F] = [K : F]$.

Demonstração 5.2. Seja $\{u_1, \cdots, u_n\}$ uma base de L. Vamos mostrar que o conjunto $\{f_{(u_1)}, \cdots, f_{(u_n)}\}$ é uma base de K. Com efeito, sejam $c_1, \cdots, c_n \in F$ tais que $c_1 \cdot f(u_1) + \cdots + c_n \cdot f(u_n) = 0_K$. Por hipótese, $c_i = f(c_i)$ para todo i e o fato de f ser um isomorfismo nos permite deduzir

$$f(c_1)\cdot f(u_1) + \cdots + f(c_n)\cdot f(u_n) = f(0_K) \Longrightarrow f(c_1 \cdot u_1 + \cdots + c_n \cdot u_n) = f(0_K) \Longrightarrow$$

$$\Longrightarrow c_1 \cdot u_1 + \cdots + c_n \cdot u_n = 0_L$$

da independência linear do conjunto $\{u_1, \cdots, u_n\}$, segue que $c_1 = \cdots = c_n = 0_F$

Deixamos como exercício, a prova de que $\{f(u_1), \cdots, f(u_n)\}$ gera os elementos de K.

Teorema 5.3 (**Kronecker, 1887**)**.** Seja K um corpo e $f \in K[X]$ um polinômio não constante. Então existe uma extensão $L \supset K$ na qual f tem uma raiz.

Demonstração 5.3. Uma vez que todo polinômio de grau positivo em $K[X]$ é produto de irredutíveis, é suficiente provarmos o teorema para este tipo de polinômio. Com efeito, suponha que $f(X) = a_0 + a_1X + \cdots + a_nX_n$ é irredutível sobre K e considere o corpo

$L = K[X]/\langle f \rangle$. É fácil ver que a aplicação

$$\begin{array}{rccc} \psi: & K & \longrightarrow & L \\ & a & \longmapsto & \overline{a} \end{array}$$

é um homomorfismo injetivo cuja imagem é isomorfa a K e portanto constitui um subcorpo de L isomorfo a K. Podemos então encarar o corpo L como sendo uma extensão de K. Além disso, tomando o polinômio f e o elemento $\alpha = \overline{X} \in L$ temos que

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = \overline{a_0} + \overline{a_1}\overline{X} + \cdots + \overline{a_n}\overline{X}^n = \overline{f} = 0 \in L$$

o mesmo teorema é verdade se $K = D$ for apenas um domínio de integridade. Isto porque todo domínio de integridade está imerso em seu corpo de frações D'. Agora se K é simplesmente um anel comutativo com unidade, o teorema de Kronecker pode não ter validade.

Exemplo 5.4. Seja $f(X) = \overline{2}X + 1 \in \mathbb{Z}_4[X]$. Se α fosse uma raiz de f pertencente a algum extensão de $\mathbb{Z}_4$, teríamos $\overline{0} = \overline{2} \cdot (\overline{2} \cdot \alpha + \overline{1}) = \overline{4} \cdot \alpha + \overline{2} = \overline{2}$, absurdo.

5.2 Elementos Algébricos e Transcendentes

No que segue, K é um corpo e $L \supset K$ é uma extensão de K.

Definição 5.3. Dizemos que um elemento $\alpha \in L$ é algébrico sobre K se ele for raiz de algum polinômio não-nulo em $K[X]$. Caso contrário, dizemos que $\alpha \in L$ é transcendente sobre K.

Naturalmente todo elemento de K é algébrico sobre K pois se $\alpha \in K$ então basta tomar $f(X) = X - \alpha \in K[X]$ e teremos $f(\alpha) = 0$.

Exemplo 5.5. $\mathbb{R} \supset \mathbb{Q}$ e $\alpha = \sqrt{2} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$ pois para $f(X) = X^2 - 2 \in \mathbb{Q}[X]$ temos $f(\alpha) = 0$.

Exemplo 5.6. $\pi, e \in \mathbb{R}$ são transcendentes sobre $\mathbb{Q}$. (Lindemann em 1882 & Hermite em 1873, respec.)

Exemplo 5.7. $\mathbb{C} \supset \mathbb{R}$ e $i \in \mathbb{C}$ é algébrico sobre $\mathbb{R}$ pois para $f(X) = X^2 + 1 \in R[X]$ tem-se $f(i) = 0$ em $\mathbb{C}$.

Definição 5.4. Seja $\alpha \in L \supset K$. Dado $\alpha \in L$, definimos o conjunto dos polinômios anuladores de *alpha* em $K[X]$ como sendo

$$\mathrm{Ann}_K(\alpha) = \{f \in K[X]/f(\alpha) = 0\} \tag{5.1}$$

Proposição 5.1. $\text{Ann}_K(\alpha)$ é um ideal de $K[X]$ e $\alpha \in L$ é transcendente sobre K se, e somente se, $\text{Ann}_K(\alpha) = \{0\}$.

Demonstração 5.4. Basta comparar os conceitos de anulador e elemento transcendente sobre um corpo.

Admita então que α é algébrico sobre K. Nesse caso, $\text{Ann}_K(\alpha) \neq \{0\}$. Mas $K[X]$ é um domínio de ideais principais e portanto existe um único polinômio mônico $p \in \text{Ann}_K(\alpha)$ tal que

$$\partial(p) \leq \partial(f) \text{ para todo } f \in \text{Ann}_K(\alpha) \text{ e } \text{Ann}_K(\alpha) = \langle p(X) \rangle$$

Definição 5.5. O gerador mônico do ideal $\text{Ann}_K(\alpha)$ é chamado polinômio minimal de α sobre K e é denotado por $irr(\alpha, K) := p(X)$.

Proposição 5.2. Se α é algébrico sobre K então $\text{Ann}_K(\alpha)$ é um ideal maximal de $K[X]$.

Demonstração 5.5. Basta mostrar que o gerador p é irredutível sobre K. Com efeito, se escrevermos $p(X) = f(X) \cdot g(X)$ em $K[X]$ então $0 = f(\alpha) \cdot g(\alpha)$ em L. Logo $f(\alpha) = 0$ ou $g(\alpha) = 0$. Supondo $f(\alpha) = 0$ temos que $f \in \text{Ann}_K(\alpha)$ donde $\partial(f) \geq \partial(p) = \partial(f) + \partial(g)$ e portanto $\partial(g) = 0$.

Definição 5.6. Dado $\alpha \in L \supset K$ definimos

$$K[\alpha] = \{f(\alpha) : f \in K[X]\} \tag{5.2}$$

Vale a pena observar que $K \subseteq K[\alpha] \subseteq L$. Com efeito, se $a \in K$ tomamos o polinômio de grau zero $f(X) = a$ e assim $a = f(\alpha) \in K[\alpha]$.

O próximo teorema estabelece a estrutura de $K[\alpha]$ quando α é algébrico ou transcendente.

Teorema 5.4. Seja $\alpha \in L \supset K$ e considere a função

$$\begin{array}{rccc} \psi: & K[X] & \longrightarrow & L \\ & f(X) & \longmapsto & f(\alpha) \end{array}$$

temos então que

a) ψ é um homomorfismo de anéis

b) $ker\{\psi\} = \text{Ann}_K(\alpha)$ e $Im\{\psi\} = K[\alpha]$

c) $K[X]/\text{Ann}_K(\alpha) \approx K[\alpha]$.

Demonstração 5.6.

a) Dados $f, g \in K[X]$ temos

$$\psi(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \psi(f) + \psi(g)$$

$$\psi(f \cdot g) = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha) = \psi(f) \cdot \psi(g)$$

b) De acordo com (3.1) e (3.2) temos

$$\mathrm{Ann}_K(\alpha) = \{f \in K[X]/f(\alpha) = 0\} = \{f \in K[X]/\psi(f) = 0\} = ker\{\psi\}$$

$$K[\alpha] = \{f(\alpha) : f \in K[X]\} = \psi(f) : f \in K[X] = Im\{\psi\}$$

em particular, segue que $K[\alpha]$ é subdomínio de L.

c) Pelo teorema do homomorfismo de anéis segue a fórmula

$$K[X]/\mathrm{Ann}_K(\alpha) \approx K[\alpha]$$

na notação da definição (3.5), a fórmula acima fica

$$K[X]/\langle irr(\alpha; K)\rangle \approx K[\alpha]$$

Exemplo 5.8. Construção de $\mathbb{Q}[\sqrt[3]{2}]$. Seja $\alpha = \sqrt[3]{2} \in \mathbb{R} \supset \mathbb{Q}$ raiz do irredutível $X^3 - 2$. Pelo algoritmo da divisão euclidiana para todo $f \in \mathbb{Q}[X]$ existem $q, r \in Q[X]$ tais que

$$f(X) = q(X)(X^3 - 2) + r(X) \;\; \mathrm{com} r(X) = a + bX + cX^2$$

daí, $f(\alpha) = r(\alpha)$ e por definição

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

Corolário 5.1. Se $\alpha \in L$ é algébrico sobre K então $K[\alpha]$ é um subcorpo de L que contém K.

Demonstração 5.7. Uma vez que $\mathrm{Ann}_K(\alpha)$ é maximal, o anel quociente $K[X]/\mathrm{Ann}_K(\alpha)$ tem a estrutura de corpo que, por isomorfismo, é passada a $K[\alpha]$ conforme o item c) do teorema acima.

Corolário 5.2. Se $\alpha \in L$ é transcendente sobre K então $K[X] \approx K[\alpha]$.

Demonstração 5.8. Pela proposição (3.1) tem-se $ker\{\psi\} = \{0\}$. Isso garante que, $\psi : K[X] \longrightarrow K[\alpha]$ é bijetiva e portanto um isomorfismo.

Corolário 5.3. Se $\alpha, \beta \in L$ são raízes do mesmo polinômio irredutível sobre K então $K[\alpha]$ e $K(\beta)$ são corpos isomorfos.

Demonstração 5.9. Seja $q \in K[X]$ irredutível sobre K tal que $q(\alpha) = q(\beta) = 0$ em L. Então, q é um múltiplo escalar não-nulo de $irr(\alpha, K)$ e de $irr(\beta, K)$ e uma vez que estes últimos são mônicos devemos ter $irr(\alpha, K) = irr(\beta, K)$. Assim, $\mathrm{Ann}_K(\alpha) = \mathrm{Ann}_K(\beta)$ e por c) $K[\alpha] \approx K(\beta)$.

Exemplo 5.9. $\alpha = \sqrt[3]{2}$ e $\beta = \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ são raízes do polinômio irredutível $p(X) = X^3 - 2$. Portanto, $\mathbb{Q}[\alpha] \approx \mathbb{Q}[\beta]$.

Corolário 5.4. Se $\alpha \in L \supset K$ é algébrico sobre K e o grau do $irr(\alpha; K)$ é n então

a $[K[\alpha] : K] = n$

b $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $K[\alpha]$ sobre K.

Exemplo 5.10. Seja $\alpha = \sqrt{3} + \sqrt{5} \in \mathbb{R}$. Fazendo $\alpha^2 = 8 + 2\alpha\sqrt{15}$ temos que $(\alpha^2 - 8)^2 = 60$ donde α é raiz do polinômio $p(X) = X^4 - 16X^2 + 4 \in Q[X]$ o qual é irredutível sobre $\mathbb{Q}$ (Exercício!). Assim, α é algébrico sobre $\mathbb{Q}$ com $irr(\alpha; \mathbb{Q}) = p(X)$. Pelo corolário acima temos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ e $\{1, \alpha, \alpha^2, \alpha^3\}$ é uma base para $\mathbb{Q}(\alpha)$.

Capítulo 6

Separabilidade e Normalidade

Vamos iniciar esta seção com um exemplo de corpo infinito de característica $p \neq 0$. E assumiremos que o leitor já tenha conhecimento sobre o teorema da unicidade da fatoração.

Seja $F = \mathbb{F}_p(t)$ o corpo das funções racionais na indeterminada t com coeficientes em $\mathbb{F}_p$ (F é o corpo de frações do anel de polinômios $\mathbb{F}p[t]$ na variável t). Esse corpo é claramente infinito com característica p. Observe que o polinômio $x^p - t \in F[x]$ (x é a indeterminada) é irredutível em $F[x]$.

Podemos usar o critério de Eisenstein com $D = Fp[t]$ que é domínio fatorial e tem F como corpo de frações. Tomamos o irredutível $t \in D$ e aplicamos o critério em $x^p - t$, com o irredutível t. Logo $x^p - t$ é irredutível em $F[x]$ e como é primitivo, também é irredutível em $D[x]$.

Observe agora que esse polinômio só tem uma raiz que aparece repetida p vezes (dizemos que tem multiplicidade p). De fato, seja α uma raiz desse polinômio em alguma extensão K de F. Então $x^p = t$ e podemos reescreve o polinômio na forma $\mathrm{x}^p - a^p = (x-a)^p$ (Lembrar de que num corpo de característica p vale a relação $(\alpha + \beta)^p = x^p + \beta^p$. Logo α é a única raiz desse polinômio repetindo-se p vezes (com multiplicidade p).

Vamos formalizar o que vimos neste exemplo e definir raiz múltipla.

Definição 6.1. Dado um polinômio não constante $f(x) \in F[x]$, seja α uma raiz de $f(x)$ em alguma extensão K de F. Dizemos que α é uma raiz múltipla, de $f(x)$ com multiplicidade n, se $(x-\alpha)^n$ divide $f(x)$ e $(x-\alpha)^{(n+1)}$ não divide $f(x)$, em $K[x]$. Quando $n > 1$ dizemos que α é uma raiz múltipla.

No caso n = 1 dizemos que α é uma raiz simples.

Vamos a seguir estabelecer um critério para decidir se uma raiz é simples ou não e também para decidir se um corpo F pode ter algum polinômio com raiz múltipla.

Definição 6.2. Dado um polinômio $f(x) = a_o + a_1x + \cdots a_nx^n \in F[x]$, definimos a derivada formal de $f(x)$ como sendo o polinômio $f^{'}(x) = a_1 + 2a_2x + \cdots + na_nx^{(n-1)}$.

Analogamente definimos derivadas de ordem superior: $f^{(n+1)}(x) = (f^n(x))^{'}$, para todo $f(x) \in F[x]$.

Vamos também definir que $f^0(x) = f(x)$, para todo $f(x) \in F[x]$.

Definição 6.3. Um corpo F é chamado de perfeito se todo polinômio irredutível $f(x) \in F[x]$ só tem raízes simples.

Juntando as observações acima podemos dizer que um corpo F é perfeito se e somente se $c(F) = 0$ ou $F = F_p$.

Definição 6.4. Seja F um corpo, E uma extensão algébrica de F e $\alpha \in E$.

1. Dizemos que α é separável sobre F se um polinômio mínimo de α sobre F for separável. Caso contrário dizemos que α é inseparável.

2. Dizemos que E é uma extensão separável de F se todo elemento de E for separável sobre F.

3. Dizemos que E é puramente inseparável sobre F se existir $n \geq 1$ tal que $\alpha^{p^n} \in F$, onde $0 \neq p = c(F)$.

4. Dizemos que E é uma extensão puramente inseparável de F se todo elemento de $E \setminus F$ for puramente inseparável sobre F.

Observação 6.1. Em alguns textos é dito que $\alpha \in F$ é separável e puramente inseparável ao mesmo tempo. Nesse caso defini-se que α é puramente inseparável se existir $n \geq 0$ tal que $x^n \in F$.

Observemos que, conforme a definição dada acima, todo elemento $\alpha \in F$ é separável sobre F pois nesse caso o polinômio mínimo é $x - \alpha$ de grau 1 que tem raiz simples. Observe também que se F for perfeito, então toda extensão algébrica E de F é separável sobre F.

Observe também que o exemplo inicial onde $K = F(\alpha)$, com α uma raiz do polinômio $x^p - t \in F[x]$ e $F = F_p(t)$, é um exemplo de uma extensão puramente inseparável, pois como vimos todo $z \in K \setminus F$ satisfaz a condição $z^p \in F$.

Seja F com $c(F) = p \neq 0$ tal que $[F : F^p] > p$ (Lembrar que F^p é um subcorpo de F e podemos considerar, como estamos fazendo há muito tempo neste curso, F como espaço vetorial sobre F^p.)

Tomemos $a, b \in F$ de forma que $b \notin F^p(a)$, ou equivalentemente, de forma que $1, a, a_2, \cdots, a^{(p-1)}, b$ sejam linearmente independentes sobre F^p. Existem $a, b \in F$ assim porque $[F : F^p] > p$.

Sejam agora α, β raízes de $x^p - a$ e $x^p - b$, respectivamente, em alguma extensão K de F.

Proposição 6.1. $[F(\alpha, \beta) : F] = p^2$ e existem infinitas extensões intermediárias entre F e $F(\alpha, \beta)$.

Demonstração 6.1. Como $a, b \notin F^p$ os polinômios $x^p - a$ e $x^p - b$ são irredutíveis. Realmente, lembre-se que esses polinômios têm, cada um deles, raiz única com multiplicidade p. Consideremos o caso $x^p - a$ que tem α como raiz. Seja $f(x) \in F[x]$ um polinômio mínimo de α sobre F. Sabemos que $f(x)$ divide $x^p - a$. Logo também $f(x)$ só tem α como raiz com multiplicidade $m = grf(x) \leq p$. Se $m = p$, então $x^p - a$ é irredutível como afirmado. Suponhamos que $m < p$. Em $F(\alpha, \beta)[x]$ vamos ter $f(x) = (x - \alpha)^m$. Logo $(-\alpha)^m = f(0) \in F$. Como $m < p$, m e p são relativamente primos e podemos escrever $1 = sm + tp$, com $s, t \in Z$. Assim $\alpha = \alpha^{(sm+tp)} = \alpha(\alpha^{m^s})(\alpha^{p^t}) \in F$, contra a escolha de $a \notin F^p$. Logo o polinômio $x^p - a$ é irredutível e analogamente $x^p - b$ também é.

Veremos agora que $\beta \notin F(\alpha)$ e assim $b \notin F(\alpha)^p$. Resulta disso que usando os argumentos acima com $F(\alpha)$ no lugar de F vamos obter $x^p - b$ irredutível em $F(\alpha)[x]$. Portanto $[F(\alpha) : F] = p = [F(\alpha, \beta) : F(\alpha))]$ e assim $[F(\alpha, \beta) : F] = p^2$, como afirmado. Vejamos então que $\beta \in F(\alpha)$. Procurando por um absurdo vamos supor que acontece o contrário. Logo, existem $a_o, \cdots, a_{p-1} \in F$ tais que $\beta = a_o + a_1\alpha + \cdots + a_{p-1}\alpha^{(p-1)}$. Elevando-se os dois lados a potência p obtemos $b = \alpha_0^p + \alpha_1^p\alpha + \cdots + \alpha_{(p-1)}^p\alpha^(p-1)$. Como essa igualdade implica que $b \in F^p(a)$ obtemos a contradição procurada.

Vejamos agora que existem infinitas extensões intermediárias. Consideremos o conjunto de todos os $yc = \alpha + c\beta$ com $c \in F$. Observe que se $c_1 \neq c_2$, então $\alpha + c_1\beta \neq \alpha + c_2\beta$. Como F tem que ser infinito, porque não é perfeito, vamos concluir que existem infinitos yc desse tipo. Vejamos agora que para $c_1 \neq c_2$ temos $F(yc_1) \neq F(yc_2)$. De fato, $F(yc_1) = F(yc_2)$ implicaria em $\alpha + c_2\beta \in F(\alpha + c1\beta)$ do que resulta $\alpha, \beta \in F(yc_1).AssimF(yc_1) = F(\alpha, \beta)$. Observe, porém, que $y_{c_1}^p = a + c_1^p b \in F$. Logo $[F(yc_1) : F] \leq p$, contradizendo o fato de $[F(\alpha, \beta) : F] = p^2$.

Proposição 6.2. Seja K uma extensão de um corpo F. Existe $\alpha \in K$ tal que $K = F(\alpha)$ se e somente se o número de extensões intermediárias entre F e K for finito.

Demonstração 6.2. Seja $K = F(\alpha)$ e $f(x) \in F[x]$ um polinômio mínimo de α. Dado $F \subset L \subset K$, um corpo intermediário, seja $g(x) = a_o + a_1x + \cdots + a_nx^n \in L[x]$ um polinômio mínimo de α sobre L. Logo $[K : L] = n$.

Tomemos agora $E = F(a_o, a_1, \cdots, a_n) \subset L$. Temos que $g(x) \in E[x]$ e como $g(x)$ é irredutível sobre L, uma extensão de E, também é irredutível sobre E. Logo $[K : E] = n$, também. Resulta então que $[L : E] = 1$, ou melhor $L = E = F(a_o, a_1, \cdots, a_n)$. Conclusão: cada extensão intermediária $F \subset L \subset K$ fica determinada pelo polinômio mínimo de α sobre L.

Observe agora que $g(x)|f(x)$ e que o número de todos os divisores de $f(x)$ em $K[x]$ é finito. Logo existe um número finito de extensões intermediárias, conforme afirmado.

Vejamos agora a recíproca. Se F for finito, o resultado vale. Vamos então assumir que F é infinito e que o número de extensões intermediárias entre F e K é finito.

Uma primeira conclusão é que K é uma extensão finita de F. Sejam $\alpha_1, \alpha_2, \cdots, \alpha_m \in K$ tais que $K = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$. Vamos fazer a demonstração recursivamente sobre m. Para $m = 1$ a afirmação já está demonstrada. Para $m = 2$ sejam, $yc = \alpha_1 + c\alpha_2$, com $c \in F$. Como F não é finito temos infinitos yc em K. Como o número de extensões intermediárias é finito, existem $c1 \neq c2$ tais que $F(yc1) = F(yc2)$. Como os mesmos argumentos da proposição de página 6 resulta dessa igualdade que $F(yc1) = F(\alpha_1, \alpha_2)$ e o resultado vale para $m = 2$. Supondo-se que vale para $m = k$ e tomando-se $K = F(\alpha_1, \alpha_2, \cdots, \alpha k + 1) = F(\alpha_1, \alpha_2, \cdots, \alpha k)(\alpha_{k+1})$, temos que existe $\delta \in F(\alpha_1, \alpha_2, \cdots, \alpha k)$ tal que $F(\alpha_1, \alpha_2, \cdots, \alpha m) = F(\delta)$ e assim $K = F(\delta, \alpha_{k+1})$. Usando o caso $m = 2$ concluímos a demonstração.

Uma extensão do tipo $K = F(\alpha)$ é chamada de extensão simples e o elemento α é chamado de elemento primitivo. Mostramos que dada uma extensão finita K de F existe elemento primitivo se e somente se o número de extensões intermediárias entre F e K é finito. Mais para frente, como aplicação do Teorema de Galois vamos mostrar que toda extensão finita e separável tem elemento primitivo. Vamos a seguir examinar a importância da propriedade dada no item (4) da Questão 7, página 7.

Proposição 6.3. Dado um corpo F seja K uma extensão finita de F. São equivalentes:

1. todo polinômio irredutível $f(x) \in F[x]$ sobre F que tem uma raiz em K tem todas as suas raízes em K;

2. existe $f(x) \in F[x]$ não constante tal que K é o corpo de raízes de $f(x)$;

3. dada uma extensão intermediária $F \subset L \subset K$ e um F-homomorfismo $\widetilde{\sigma} : L \to \Omega$ onde Ω é uma extensão qualquer de F contendo K, existe uma extensão $\sigma : K \to K$.

Demonstração 6.3. (1) $\to$ (2) Seja $\alpha_1, \cdots, \alpha_n$ uma base de K sobre F. Para cada $i = 1, ..., n$ seja $P_i(x) \in F[x]$ um polinômio mínimo de α_i. Tomemos $f(x) = p_x p + 2(x)\Delta\Delta\Delta p_n(x) \in F[x]$. Por (1) cada um dos $p_i(x)$ tem todas as suas raízes em K, logo $f(x)$ também tem todas as suas raízes em K. Por outro lado, se $F \subset E \subset K$ for uma

extensão intermediária onde $f(x)$ tem todas as suas raízes, em particular $\alpha_i \in E$, para todo i. Logo $K \subset E$, ou $E = K$. Assim K é o corpo de raízes de $f(x)$ como queríamos.

(2) $\rightarrow$ (3) Por (2), K é o corpo de raízes de $f(x) \in F[x] \subset L[x]$. Portanto K também é o corpo de raízes de $f(x) \in L[x]$. Seja C o conjunto de todas as raízes de $f(x)$ (que estão em K). Temos que $K = L(C)$. Seja agora $\sigma L_1 = \sigma(L) \subset \Omega$ a imagem de L por Σ dentro de Ω. Como Σ é homomorfismo (de anel) e o L é corpo, σ é injetiva, do que resulta que L_1 é corpo.

Observe a seguir C está contido em Ω e portanto podemos tomar a extensão $L_1(C) \subset \Omega$. Como $F \subset L_1$, pois Σ é um F-homomorfismo, temos $f(x) \in L1[x]$ também. Mais ainda, por construção $L_1(C)$ é um corpo de raízes de $f(x) \in L1[x]$

Aplicamos agora o teorema da unicidade ao isomorfismo $\sigma \ : L \rightarrow L_1$ e aos polinômios $f(x)$ e $\sigma(f(x)) = f(x)$. Logo existe e $\widetilde{\sigma} : K \longrightarrow L_1(C)$, um isomorfismo que estende σ.

Para terminarmos a demonstração do item observe que $K = F(C) \subset F1(C)$. Como a restrição de Σ a F é a identidade, obtemos que $\widetilde{\sigma} : K \longrightarrow L_1(C)$ é uma F transformação linear. Como é um isomorfismo, vai preservar as dimensões sobre F, isto é, $[K : F] = [F_1(C) : F]$. Mas então a inclusão acima tem que ser uma igualdade: $L1(C) = K$ e obtemos o isomorfismo e $\widetilde{\sigma} : K \longrightarrow K$ que estende σ.

(3) $\longrightarrow$ (1) Seja $f(x) \in F[x]$ irredutível com uma raiz $\alpha \in K$. Seja Ω um corpo de raízes de $f(x) \longrightarrow K[x]$. Denotemos por $\alpha = \alpha_1, \cdots, \alpha_r$ as raízes de $f(x)$ em Ω.Pelo teorema da Unicidade para cada raiz α_i existe um isomorfismo $\sigma_i : F(\alpha) \longrightarrow F(\alpha_i)$ que estende a $id : F \longrightarrow F$ tal que $\sigma_i(\alpha) = \alpha_i$. Aplicamos agora a condição (3) ao corpo intermediário $F(\alpha)$ e ao F-homomorfismo σ_i. Logo existe e $\sigma_i : K \longrightarrow K$, F-isomorfismo que estende σ_i. Resulta então que $\alpha_i = \sigma_i(\alpha) = \sigma_i(\alpha) \in K$, para todo $i = 1, \cdots, r$. Logo $f(x)$ tem todas as suas raízes em K, como afirmado.

Uma extensão K de um corpo F para a qual vale a propriedade (1) desta última proposição (e portanto qualquer um dos outros itens, já que são equivalentes) é chamada de extensão normal. A Proposição está nos dizendo que uma extensão K de F é normal se e somente se for o corpo de raízes de um polinômio.

Proposição 6.4. Seja F um corpo e Ω uma extensão qualquer de F.

1. Sejam K e L duas extensões normais de F contidas em Ω. Então $K \cap L$ também é uma extensão normal de L.

2. Assumimos neste item que Ω é um fecho algébrico de F. Para toda extensão finita L de F, dentro de Ω existe uma extensão normal e finita, K, de F contendo L dentro de Ω que é mínima com a propriedade de conter L. Algumas vezes K é chamado de fecho normal de L em Ω.

3. Assumimos agora que Ω é uma extensão normal e finita de $FeF \subset K \subset \Omega$ é uma extensão intermediária. Se para todo $\Omega \in G(\Omega; F)$ tivermos $\sigma(K) = K$, então K é uma extensão normal de F.

4. Assumimos novamente que Ω é uma extensão normal e finita de F e que $F \subset K \subset \Omega$ é uma extensão intermediária.

(a) Então Ω é uma extensão normal (e finita) de K.

(b) Assumimos agora que K é uma extensão normal de F. Seja $\sigma \in G(\sigma; F)$ um F-automorfismo de Ω. Então $\sigma(K) = K$, ou então, a restrição de σ a K está em $G(K; F)$. Mais ainda, a função $G(\sigma; F) \longrightarrow G(K; F)$ dada por $\sigma \longmapsto \sigma|K$ (restrição de σ a K) é um homomorfismo sobrejetivo de grupos cujo núcleo é $G(\Omega; K)$. Logo $G(K; F) \simeq G(\Omega; F)/G(\Omega; K)$.

Demonstração 6.4. Seja $f(x) \in F[x]$ irredutível com uma raiz em $K \cap L$. Logo $f(x)$ terá todas as suas raízes em K e também em L já que são extensões normais de F. Portanto todas as raízes de $f(x)$ estão em $K \cap L$.

Seja $\alpha_1, \cdots, \alpha_n$ uma F-base de L e sejam $f_1(x), \cdots, f_n(x)$ os polinômios minimais de $\alpha_1, \cdots, \alpha_n$, respectivamente. Tome K o corpo de decomposição de $f(x) = f_1(x) \cdots f_n(x)$ sobre F. Como K contem $\alpha_1, \cdots, \alpha_n$, raízes de $f(x)$, K conterá L. K é uma extensão normal e finita de F. Finalmente, qualquer extensão normal de F, contida em que contenha K tem uma raiz de cada um dos polinômios irredutíveis $f_1(x), \cdots, f_n(x) \in F[x]$. Devido a normalidade conterá todas as raízes desses polinômios. Logo conterá todas as raízes de $f(x)$ e portanto, pela propriedade do corpo de raízes, conterá K.

De fato, seja $f(x) \in F[x]$ irredutível com uma raiz em $\alpha \in K$. Sejam $\alpha_2, \cdots, \alpha n$ as outras raízes de $f(x)$ que estão em Ω, e façamos $\alpha_1 = \alpha$ (Ω é uma extensão normal de F). Pelo teorema da unicidade para cada α_i existe, $\alpha_i : F(\alpha_1) \longrightarrow F(\alpha_i)$ uma extensão de id tal que $\sigma_i(\alpha_1) = \alpha_i$. Existe uma extensão e $\widetilde{\sigma}_i : \Omega \longrightarrow \Omega$. Isto é, existe e $\sigma_i \in G(\Omega; F)$ tal que $\widetilde{\sigma}_i(\alpha_1) = \alpha_i$. Como por hipótese e $\widetilde{\sigma}_i(K) = K$, resulta que $\alpha_i \in K$. Isso vale para todo $1 \leq i \leq n$. Assim $\alpha_1, \cdots, \alpha_n \in K$ e K é uma extensão normal de F como afirmado.

Seja $f(x) \in K[x]$ irredutível com uma raiz $\alpha \in \Omega$. Seja $g(x) \in F[x]$ um polinômio mínimo de α em relação a F. Logo $f(x)|g(x)$ em $K[x]$. Como Ω é normal sobre F, $g(x)$ tem todas as suas raízes em Ω. Como as raízes de $f(x)$ estão entre as raízes de $g(x)$, também $f(x)$ terá todas as suas raízes em Ω. Assim Ω é uma extensão normal de K.

K é o corpo de raízes de polinômio não constante $f(x) \in F[x]$. Logo $K = F(\alpha_1, \cdots, \alpha_n)$, onde $\alpha_1, \cdots, \alpha_n$ são as raízes de $f(x)$. Observe que para todo $1 \leq i \leq$

n, $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0$. Portanto $\sigma(\alpha_i) = \alpha_j$ para algum j. Resulta disso que $\sigma(F(\alpha_1, \cdots, \alpha_n)) = F(\sigma(\alpha_1), \cdots, \sigma(\alpha_n)) \subset F(\alpha_1, \cdots, \alpha_n)$.

Aplicando-se o mesmo argumento a $\sigma^{(-1)}$ vamos obter $\sigma^{(-1)}(F(\alpha_1, \cdots, \alpha_n)) \subset F(\alpha_1, \cdots, \alpha_n)$. Logo $F(\alpha_1, \cdots, \alpha_n) \subset \sigma(F(\alpha_1, \cdots, \alpha_n))$. Portanto $\sigma(K) = K$, como queríamos.

Que a aplicação $\sigma \longmapsto \sigma|K$ é um homomorfismo com núcleo $G(\Omega; K)$ é claro. O ponto interessante é mostrar que essa aplicação é sobrejetiva. Para isso tome $\tau \in G(K; F)$. Logo $\tau : K \longmapsto K \subset \Omega$ é um F-isomorfismo de uma extensão intermediária $F \subset K \subset \Omega$ em Ω. Existe extensão $(\widetilde{\tau}) : \Omega \longmapsto \Omega$ de τ. Isto é, existe $(\widetilde{\tau}) \in G(\Omega; F)$ cuja restrição a K é τ, demonstrando a sobrejetividade do homomorfismo.

Proposição 6.5. Para todo inteiro $n \geq 1$ e todo irredutível $p \in \mathbb{Z}$, existe um corpo K com p^n elementos.

Demonstração 6.5. Observemos que o polinômio $x^{p^n} - x \in \mathbb{F}_p(x)$ tem derivada $-1 \neq 0$ constante. Logo, tem raízes distintas. Seja K o corpo de raízes desse polinômio sobre $\mathbb{F}_p$. Temos que K tem pelo menos p^m elementos. Suponhamos que K tem p^m elementos, com $m \geq n$.

Seja agora $L = \alpha \in K \mid \varphi^n(\alpha) = \alpha$. Verifica-se diretamente que L é um subcorpo de K. Por outro lado, pela própria definição de L, vamos ter que L é o conjunto das raízes de $x^{p^n} - x$.

Mas então L contém o corpo de raízes de $x^{p^n} - x$ sobre $\mathbb{F}_p$. Portanto $L = K$, de onde obtemos que $\varphi^n = id$. Como φ tem ordem m temos que $m \mid n$ e assim $m \leq n$. Logo $n = m$ e K tem p^n elementos, conforme esperado.

Capítulo 7

Teorema de Galois

Apresentamos abaixo um diagrama mostrando todos os subgrupos do grupo de Galois do corpo de raízes de $x^3 - 2$ sobre $\mathbb{Q}$ e os correspondentes corpos fixos.

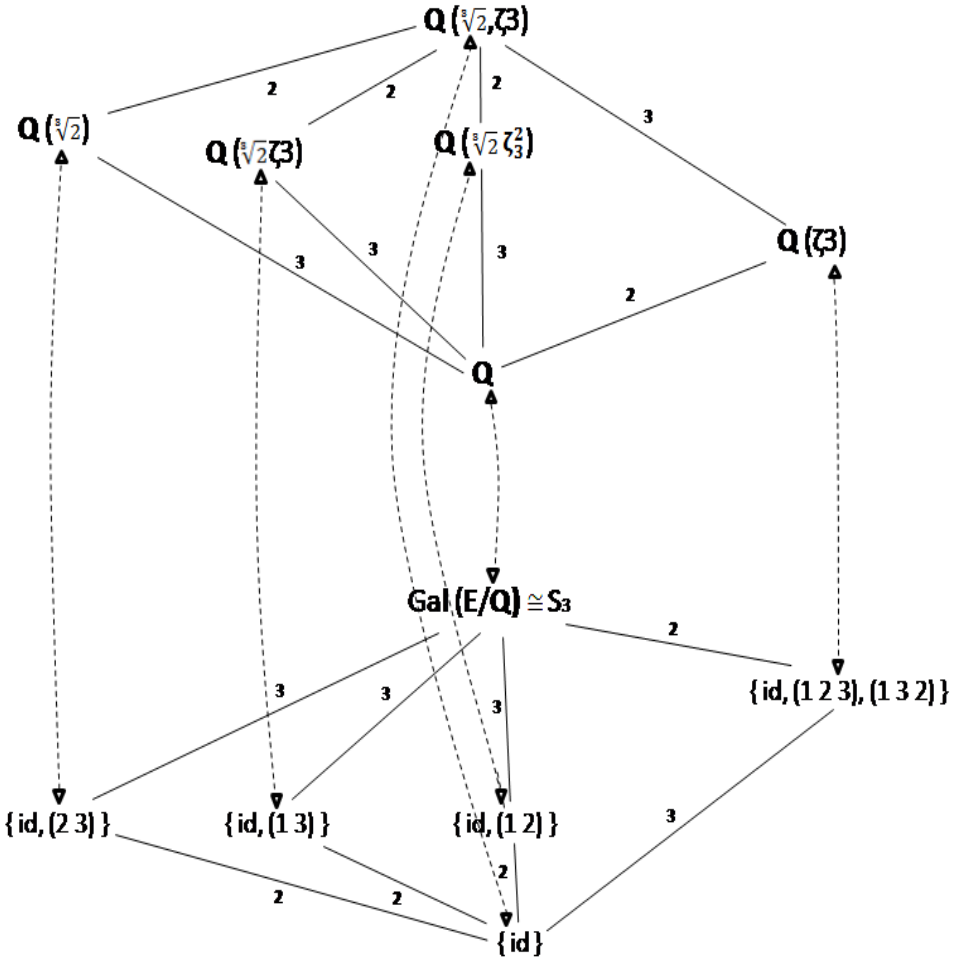

Figura 7.1: The Galois Correspondence for $\mathbb{Q}(\sqrt[3]{2}, \varsigma_3)/\mathbb{Q}$

7.1 Resolução de Equações Por Radicais

Esse exemplo (assim como muito outros semelhantes) são a motivação para a próxima definição. **Daqui em diante sempre assumir $c(F) = 0$ para evitar a necessidade de muitas restrições que assegurem a separabilidade dos polinômios**.

Definição 7.1. Seja F um corpo com $c(F) = 0$.

(a) Dizemos que uma extensão finita K de F é uma extensão radical se existir uma cadeia de corpos intermediários

$$F = F_o \subset F_1 = F_o(\alpha_1) \subset F_2 = F_1(\alpha_2) \subset \cdots F_{i-1} \subset F_i = F_{i-1}(\alpha_i) \subset F_t = K \quad (7.1)$$

onde para todo $1 \leq i \leq t$, $\alpha_i^{n_i} \in F_{i-1}$, para algum $n_i \geq 1$.

(b) Dizemos que uma equação $f(x) = 0$, com $f(x) \in F[x]$, é resolúvel por radicais se existir uma extensão radical K de F que contém um corpo de raízes de $f(x)$.

O Teorema de Galois sugere definirmos o equivalente a resolúvel para grupos:

Definição 7.2. Dizemos que um grupo finito G é resolúvel se existir uma cadeia de subgrupos

$$1 = H_o \subset H1 \subset \cdots \subset H_t = G,$$

onde para todo $1 \leq i \leq t, H_{i-1} \lhd H_i$ é o grupo quociente H_i/H_{i-1} é abeliano.

Vamos agora juntar esses dois objetos:

Teorema 7.1. Seja $f(x) \in F[x]$ um polinômio não constante e seja E um corpo de raízes de $f(x)$ sobre F $(c(F) = 0)$. Então a equação $f(x) = 0$ é resolúvel por radicais se e somente se $G(E; F)$ for um grupo resolúvel.

Antes de prosseguirmos com o estudo de extensões radicais vamos mostrar que a equação $f(x) = 0$, com $grf(x) = 2$, 3, e 4 são resolúveis por radicais. Com esse objetivo vamos estabelecer um critério que torne mais fácil decidir quando um grupo é solúvel. Inicialmente introduzimos alguns novos elementos.

Definição 7.3. Seja G um grupo qualquer.

(a) Dados $a, b \in G$ definimos o comutador de a e b como sendo o elemento $[a, b] = aba^{-1}b^{-1} \in G$.

(b) Seja G' o subgrupo de G gerado por todos os comutadores $[a,b]$ com $a,b \in G$. Isto é, G'= interseção de todos os subgrupos de G que contém o conjunto $[a,b]|a,b \in G$. G' é chamado de derivada de G. (Às vezes o grupo derivado também é denotado por $[G,G]$.)

O grupo G/G' é chamado de abelianizado de G. As questões acima mostram que G/G' é o "maior" grupo quociente de G que é abeliano. Em particular se G é abeliano se e somente se $G' = 1$. O critério para decidir se um grupo é resolúvel é, em certo sentido, uma generalização desse último fato.

Inicialmente definimos grupos derivados superiores : seja $G^1 = G'$ o grupo derivado de G. $G^2 = (G^{(1)})'$ o derivado do derivado e vamos repetindo o processo pondo $G^{n+1} = (G^{(n)})'$.

Critério. Um grupo finito G é resolúvel se e somente se existe $n \geq 1$ tal que $G^{(n)} = 1$.

Demonstração 7.1. Seja G um grupo resolúvel e a cadeia de subgrupos

$$1 = H_o \subset H_1 \subset \cdots \subset H_t = G,$$

onde para todo $1 \geq i \geq t$, $H_{i-1} \lhd H_i$ e o grupo quociente H_i/H_{i-1} é abeliano. Como G/H_{t-1} é abeliano, $G^{(1)} = G' \subset H_{t-1}$.

Igualmente H_{t-1}/H_{t-2} abeliano implica $H'_{t-1} \subset H_{t-2}$. Como $G^{(1)} \subset H_{t-1}$ vale que $G^{(1)} = (G^{(1)})' \subset H'_{t-1} \subset H_{t-2}$. Suponhamos que verificamos que $G^{(1)} \subset H_{t-i}$ para todo $1 \leq i \leq r$. Novamente de $H_{t-r}/H_{t-(r+1)}$ abeliano vai resultar $G^{(r+1)} = (G^r)' \subset H'_{t-r} \subset H_{t-(r+1)}$. Concluímos assim que $G^{(1)} \subset H_{t-i} para todo 1 \leq i \leq t$. Logo $G^{(t)} \subset H_o = 1$.

Reciprocamente, suponhamos que exite $n \geq 1$ tal que $G^{(n)} = 1$. Tomamos então a cadeia $H_i = G^{(n-i)}$ e vamos obter

$$1 = H_o \subset H_1 \subset \cdots \subset H_n = G^{(0)} = G'$$

onde H_{i-1} é o derivado de H_i. Portanto $H_{i-1} \lhd H_i$ e o grupo quociente H_i/H_{i-1} é abeliano. Isso termina a demonstração do critério.

Resolubilidade de S_n. Para $n = 2, 3, 4$ temos que S_n é resolúvel.

Demonstração 7.2. S_2 é abeliano e portanto resolúvel. Em S_3 temos a cadeia $1 \subset A_3 \subset S_3$, onde A_3 é abeliano, $A_3 \lhd S_3$ e como S_3/A_3 tem ordem 2 também é abeliano.

Em S_4 tomamos a cadeia $1 \subset V \subset A_4 \subset S_4$, onde V é o grupo de Klein. Temos que V é abeliano e $V \lhd S_4$. Logo, a fortiori, $V \lhd A_4$. Como A_4/V tem ordem 3, que é um número primo, A_4/V é abeliano. Quanto ao A_4 já sabemos $A_4 \lhd S_4$ e S_4/A_4 abeliano.

Seja agora um polinômio $f(x)$ de grau $m = 2, 3, 4$. Se K for o corpo de raízes de $f(x)$, então $G(K; F)$ é um subgrupo de S_m. Vimos acima que para esses valores de m, S_m é resolúvel. Logo, $G(K; F)$ é resolúvel.

Observe que isso não impede de Sn ter algum subgrupo resolúvel.

Vamos a seguir construir um polinômio $f(x)$ de grau 5 para o qual $G(K; Q) = S_5$, onde K é o corpo de raízes de $f(x)$. Logo a equação $f(x) = 0$ não pode ser sempre resolúvel por radicais.

Seja $f(x) = x^5 - 4x + 2 \in Q[x]$. Esse polinômio é irredutível pelo critério de Eisenstein. Por outro lado temos $f(-2) = -22 < 0$ e $f(-1) = 5 > 0$, mostrando que $f(x)$ tem uma raiz real $-2 < \alpha_3 < -1$. Analogamente, $f(1) = -2 < 0$ e $f(2) = 25 > 0$. Logo temos mais duas raízes reais $-1 < \alpha_4 < 2$ e $1 < \alpha_5 < 2$. Examinando-se em seguida a derivada de $f(x)$ obtemos $f'(x) = 5x^4 - 3 = (\sqrt{(5x^2)} - 2)(\sqrt{(5x^2)} + 2)$. Logo $f(x)$ só tem dois pontos críticos

$$\sqrt{\frac{2}{\sqrt{5}}},\ -\sqrt{\frac{2}{\sqrt{5}}}$$

sendo um deles um mínimo relativo e o outro um máximo relativo. Concluímos assim que o gráfico de $f(x)$ no plano $\mathbb{R}^2$ só corta o eixo X três vezes, em α_3, α_4, e α_5. As outras duas raízes, α_1 e α_2 são complexas e conjugadas. Seja $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ o corpo de raízes de $f(x)$ sobre $\mathbb{Q}$ e $G = G(K; \mathbb{Q})$ o grupo de Galois. Veja no diagrama abaixo a posição dos corpos $\mathbb{Q}$, $\mathbb{C}(\alpha_3, \alpha_4, \alpha_5)$ e K,

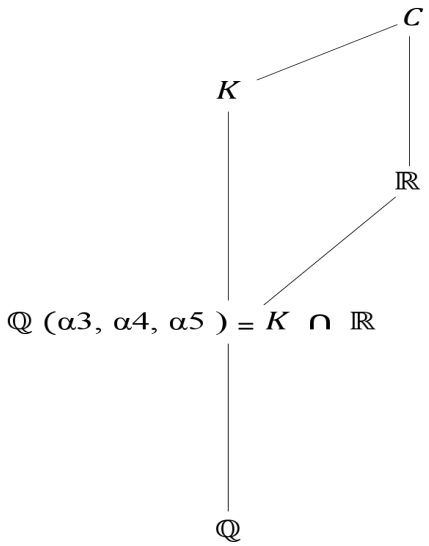

Figura 7.2: Posição dos corpos $\mathbb{Q}$, $\mathbb{C}(\alpha_3, \alpha_4, \alpha_3)$ e K

Proposição 7.1. Seja $f(x) \in Q[x]$ um polinômio irredutível de grau primo p com 2 raízes complexas conjugadas e $p - 2$ raízes reais. Seja K o corpo de raízes de $f(x)$ sobre $\mathbb{Q}$.

Então $G(K;\mathbb{Q}) \cong S_p$. Voltando ao estudo de equações resolúveis por radicais mostraremos inicialmente que podemos apresentar o item (a) da definição de forma mais forte.

Proposição 7.2. Seja K uma extensão radical de um corpo $F(c(F) = 0)$. Então existe uma extensão N de F com as seguintes propriedades:

(i) $K \subset N$;

(ii) N é uma extensão galoisiana de F;

(iii) N é uma extensão radical de F.

Demonstração 7.3. Fixemos uma cadeia $F = F_o \subset F_1 \subset \cdots \subset F_t = K$ satisfazendo as condições do item (a) da definição acima: $F_i = F_{i-1(\alpha_i)}$ onde $\alpha_i = \alpha_i^{n_i} \in F_{i-1}$, para todo $i = 1, \cdots, t$.

Para cada $0 \leq i \leq t$ mostraremos que existe uma extensão N_i de F tal que $F_i \subset N_i$, Ni é uma extensão galoisiana de F e N_i é uma extensão radical de F.

Vamos fazer a construção recursivamente. Para $i = 0$, tomamos $N_o = F$. Suponhamos que já temos construídas as extensões N_i para todo $i = 0, \cdots, s < t$ e vamos construir N_{s+1}. Recordar que $F_s = F_{s-1(\alpha_s)}$ com $\alpha_s = \alpha_s^{n_i} \in F_{s-1}$ e N_s é uma extensão galoisiana de F contendo F_s e também uma extensão radical de F.

Vamos fazer um diagrama com os elementos do problema,

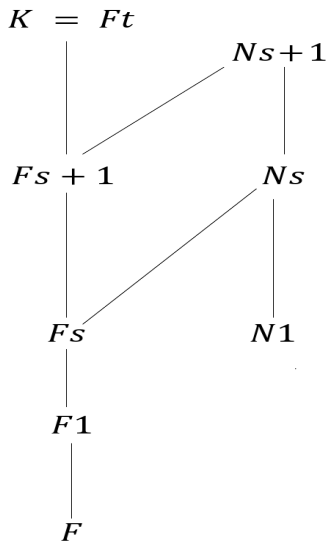

Figura 7.3: Extensão galoisiana de F.

Seja $G(N_s; F) = \sigma_1, \cdots, \sigma k$ e tomemos o polinômio

$$g(x) = \prod_{j=1}^{k} (x^{n_s} - \sigma_j(a_s))$$

onde escolhemos $\sigma_1 = id$. Observe que para todo $1 \leq l \leq k$

$$\sigma^{'}(g(x)) = \prod_{j=1}^{k}(x^{n_s} - \sigma^{'}\sigma_j(a_s)) = g(x),$$

pois $\sigma^{'}\sigma^1, \cdots, \sigma^{'}\sigma^k = \sigma_1, \cdots, \sigma_k$. Dessa forma $g(x) \in F[x]$, pois F é o corpo fixo de $G(N_s; F)$.

Tomemos agora N_{s+1} como o corpo de raízes de $g(x)$ sobre N_s. Sejam $\beta_1, \beta_2, \cdots, \beta_S$ as raízes de $g(x)$ em $Ns + 1$. Logo $N_{s+1} = N_s(\beta_1, \beta_2, \cdots, \beta_S)$.

Vamos verificar que N_{s+1} têm as propriedades requeridas. Observe em primeiro lugar que como $\sigma_1 = id$, $x^{ns} - \alpha s$ as é um dos fatores de $g(x)$. Logo alguma das raízes $\beta_1, \beta_2, \cdots, \beta_S$ é igual a α_s.

Para simplificar, suponhamos que $\beta_S = \alpha_s$. Logo

$$F_{s+1} = F_s(\alpha_s) \subset N_s(\alpha_s) \subset N_{s+1}$$

Por hipótese, N_s é uma extensão galoisiana de F, logo N_s é o corpo de raízes de um polinômio não constante $f(x) \in F[x]$. Se $\gamma_1, \cdots, \gamma_r$ são as raízes de $f(x)$ em N_s, então $N_s = F(\gamma_1, \cdots, \gamma_r)$.

Tomando-se agora o polinômio $f(x)g(x)$ vemos que suas raízes em N_{s+1} são $\gamma_1, \cdots, \gamma_r, \beta_1, \beta_2, \cdots, \beta_S$. Logo o corpo de raízes de $f(x)g(x)$ sobre $F[x]$ será

$$F(\gamma_1, \cdots, \gamma_r, \beta_1, \beta_2, \cdots, \beta_S) = N_s(\beta_1, \beta_2, \cdots, \beta_S) = N_{s+1}$$

Portanto N_{s+1} é uma extensão galoisiana de F e contém F_{s+1}. Por outro lado, cada β_h por ser raiz de $g(x)$ tem que anular algum dos fatores $x^{ns} - \sigma_j(\alpha_s)$ de $g(x)$. Mas então $\beta_h^{ns} = \sigma_j(\alpha_s) \in N_s$ (observe que $\alpha_s \in F_s \subset N_s$ e $\sigma_j(N_s) = N_s$, para $\sigma_j \in G(N_s; F)$) Temos então uma cadeia

$$N_s \subset N_s(\beta_1) \subset N_s(\beta_1, \beta_2) \subset \cdots N_s(\beta_1, \beta_2, \cdots, \beta_S) = N_{s+1}$$

que mostra que N_{s+1} é uma extensão radical de N_s. Como N_s é uma extensão radical de F, podemos emendar a cadeia que vai de F para N_s com a cadeia acima e obter uma cadeia que vai de F à N_{s+1} (ver Questão abaixo). Mas então N_{s+1} é uma extensão radical de F e obtivemos o N_{s+1} procurado.

Repetindo o processo acima quantas vezes for necessário vamos obter uma extensão $N = N_t$ de F que tem as propriedades exigidas na proposição.

Observação 7.1. Convém destacar que pela proposição acima sempre podemos tomar uma extensão radical K de F com K galoisiana sobre F. Nesse caso se $F = F_o \subset F_1 \subset \cdots \subset F_t = K$ for a cadeia dos subcorpos, a cada corpo intermediário F_{t-i} corresponde um subgrupo $H_i = G(K; Ft - i)$ de $G(K; F)$. Mas ainda temos que trabalhar um pouco mais para podermos ter $H_i \lhd H_{i+1}$ e obter que $G(K; F)$ é resolúvel.

Proposição 7.3. Seja F um corpo e assumimos que $c(F) = 0$ e $n > 1$ (bastava assumir que n não é divisível por $c(F)$). Dado a F^x temos que o corpo de raízes de $x^n - a$ sobre F é igual ao corpo de raízes de $(x^n - 1)(x^n - a)$ sobre F.

Demonstração 7.4. Observe inicialmente que o polinômio $x^n - a$ e seu derivado nx^{n-1} não tem raízes em comum. Logo $x^n - a$ só tem raízes simples. Seja agora K o corpo de raízes de $x^n - a$ e sejam $\alpha 1, \alpha 2, \cdots, \alpha n$ as raízes desse polinômio em K.

Vemos então que $\alpha_2\alpha_1^{-1}, \alpha_3\alpha_1^{-1}, \cdots, \alpha_n\alpha_1^{-1}$ são raízes de x^{n-1} e são distintas. Logo x^{n-1} tem todas as suas raízes em K. Portanto K contém um corpo de raízes de $(x^n - 1)(x^n - a)$. Como a inclusão contrária é clara, obtemos o resultado.

Vamos a seguir fazer um breve estudo das raízes do polinômio $x^n - 1$. Com vimos acima esse polinômio só tem raízes simples. Seja K um corpo que contenha todas as raízes de $x^n - 1$. Claramente $U_n = \varsigma \in K | \varsigma^n = 1$ é um subgrupo de K^x de ordem n (é igual ao conjunto das raízes de x^{n-1}).

Seja U_n um grupo cíclico, portanto existe $\xi \in U_n$ que tem ordem n, isto é, $\xi^n = 1$ e para todo $1 \leq r < n, \xi^r \neq 1$. Uma raiz da unidade com essa propriedade é chamada de primitiva. Neste caso raiz primitiva n-ésima da unidade.

Voltando ao grupo U_n temos então que $U_n = 1, \xi^1\xi^2, \cdots, \xi^{(n-1)}$. Observe também que se tomamos $x^n - 1 \in F[x]$, então o corpo de raízes de $x^n - 1$ sobre F é dado por $F(\xi)$, onde ξ é uma raiz primitiva n-ésima da unidade. Uma questão é determinar o polinômio mínimo de ξ sobre F (observe que $x^n - 1$ é claramente redutível). Claro que para cada corpo F temos um polinômio mínimo diferente (em particular $x - \xi$ caso $\xi \in F$). Vamos porém encontrar um polinômio mais específico do que $x^n - 1$ que tem ξ com raiz.

Definição 7.4. Seja $n \geq 1$ um número natural. Definimos uma função $\varphi : N \longrightarrow N$ pondo $\varphi(n) =$ número de elementos de $1 \leq r \leq n | r$ é relativamente primo com n.

Essa função é chamada função φ de Euler.

Observe que se n é primo, trivialmente $\varphi(n) = n - 1$, mas em geral temos uma fórmula bastante elaborada. Seja $n = p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$ a fatoração de n em irredutíveis de $\mathbb{N}$, então

$$\varphi(n) = (p_1 - 1)(p_2 - 1)\cdots(p_t - 1)p_1^{(n-1)}p_2^{(n-2)}\cdots p_t^{(nt-1)}$$

A função de Euler tem uma íntima ligação com os grupos cíclicos.

Baseando-se então nessa questão temos que o grupo U_n das raízes n-ésimas da unidade tem $\varphi(n)$ geradores, ou equivalentemente, existem $\varphi(n)$ raízes primitivas n-ésimas da unidade. Vamos denotar por P_nU_n ao conjunto $P_n = \xi \in U_n | \xi^n = 1$ e $\xi^r \neq 1$para todo$1 \leq$ r $<$ n. Pelo que vimos P_n tem $\varphi(n)$ elementos, ou então denotamos $|P_n| = \varphi(n)$ para indicar a quantidade de elementos do conjunto P_n.

Vamos a seguir relacionar U_n com Ud para cada divisor d de n. Se $d|n$ e ς é uma raiz d-ésima da unidade (raiz de $x^d - 1$), então, como $n = dq$, para algum q, $\varsigma^n = 1$, implicando que $\varsigma \in U_n$.

Podemos concluir que $Ud \subset U_n$, para todo divisor d de n. Reciprocamente, para cada $\varsigma \in U_n$, se $|\varsigma| = d$, então $d|n$, mas $|\varsigma| = d$ significa $\varsigma^d = 1$ e assim $\varsigma \in U_d$. Isto é cada $\varsigma \in U_n$ está em algum U_d com $d|n$ (na verdade $|\varsigma| = d$ implica $\varsigma \in P_d$).

Mais ainda, dado um divisor $d|n$ e $n = dq$, então verifica-se facilmente que $|\xi^q| = d$, para $\xi \in Pn$.

Logo $\xi^n \in U_d$. Podemos então concluir que

$$U_n = \bigcup_{d/n} U_d \text{ e também } U_n = \bigcup_{d/n} P_d$$

Observe que para $\varphi \in U_n$ temos $\varphi \in P_d$ se e somente se $|\varphi| = d$. Portanto a segunda união acima é disjunta, isto é, se $d \neq e$ são dois divisores de n então $P_d \cap P_e = \varnothing$, pois um elemento ς não pode ter ordem d e e ao mesmo tempo. Logo

$$U_n = \sum_{d/n} |P_d| \text{ ou então } n = \sum_{d/n} \varphi(d)$$

Em relação ao polinômio $x^n - 1$ obtemos

$$x^n - 1 = \prod_{\varsigma \in U_n} (x - \varsigma) = \prod_{d/n} \left(\prod_{\varsigma \in P_d} \right) (x - \varsigma) = \prod_{d/n} \phi d(x)$$

onde

$$\phi d(x) = \prod_{\varsigma \in P_n} (x - \varsigma)$$

Cada polinômio $\phi d(x)$ é chamado de polinômio ciclotômico de índice d e como $|P_d| = \varphi(d)$ temos $gr\phi d(x) = \varphi(d)$. Vamos ressaltar esse fato:

$$x^n - 1 = \prod_{d/n} \phi d(x) = \phi_1(x) \cdots \phi_2(x)$$

Proposição 7.4. (a) $\phi_n(x)$ é irredutível sobre $\mathbb{Q}[x]$. Se ξ é uma raiz de $\phi_n(x)$, então $\mathbb{Q}(\xi)$ é o corpo de raízes de $\phi_n(x)$ e $G(\mathbb{Q},(\xi);\mathbb{Q})$ é isomorfo ao grupo $(Z/nZ)^x$ que é o grupo das unidade do anel quociente.

(b) Se F é um corpo de característica $p \neq 0$ e ξ é uma raiz de $\phi_n(x)$, então $F(\xi)$ é o corpo de raízes de $\phi_n(x)$ sobre F e $G(F(\xi);F)$ é isomorfo a um subgrupo do grupo $(Z/nZ)^x$.

(c) Mais geralmente, dado um corpo F cuja característica não divida n se ξ é uma raiz primitiva n-ésima da unidade, então $F(\xi)$ é o corpo de raízes de $\phi_n(x)$ sobre F, $[F(F(\xi);F)] \leq \varphi(n)$ e $G(F(\xi);F)$ é isomorfo a um subgrupo de $(Z/nZ)^x$. Logo $G(F(\xi);F)$ é sempre abeliano.

Demonstração 7.5. Não vamos fazer a demonstração de que $\phi_n(x)$ é irredutível em $Q[x]$. Mesmo porque não temos um resultado semelhante para F_p. Quanto aos grupos de Galois vamos ver como a coisa funciona.

Seja F um corpo qualquer com a única restrição de que $p\dagger n$ se $0 \neq c(F) = p$. Claro que $F(\xi)$ é o corpo de raízes de $\phi_n(x)$ sobre F, pois onde estiver uma raiz primitiva n-ésima da unidade ξ também estarão todas as outras. Seja agora $\sigma \in G(F(\xi);F)$. Como $\xi^n = 1$ e $\xi^n \neq 1$, para todo $1 \leq r < n$, também será verdade que $\sigma(\xi)^n = 1$ e $\sigma(\xi)^r \neq 1$, para todo $1 \leq r < n$, pois σ é um automorfismo. Logo $\sigma(\xi) = \xi^s$ para algum $1 \leq s \leq n$ que é relativamente primo com n. Vamos então definir $\sigma : G(F(\xi);F) \to (Z/nZ)^x$ pondo $\theta(\sigma) = s$. Observe que θ é uma função pois caso acontecesse $\sigma(\xi) = \xi^s = \xi^t$ com $1 \leq s \leq t < n$, então $\xi^{(t-s)} = 1$. Como ξ é raiz primitiva n-ésima da unidade isso implica que $t-s = 0$. Assim θ é uma função. Verifica-se facilmente que θ é homomorfismo injetivo de grupos. Portanto, no caso $F = \mathbb{Q}$, como sabemos que $\phi_n(x)$ é irredutível obtemos que $\varphi(n) = gr\phi_n(x) = [\mathbb{Q}(\xi) : \mathbb{Q}] = |G(\mathbb{Q}(\xi) : \mathbb{Q})| = (Z/nZ)^x$. Assim θ também é sobrejetiva, ou melhor, é um isomorfismo.

Corolário 7.1. A equação $x^n - 1 = 0$ é resolúvel por radicais.

Observe que o estudo do corpo de raízes de uma equação do tipo $x^n - 1 \in F[x]$ pode ser feito em duas etapas: toma-se primeiro $E = F(\xi)$, onde ξ é uma raiz primitiva n-ésima da unidade, e em seguida toma-se o corpo de raízes de $x^n - a \in E[x]$ sobre E. Podemos portanto restringir o estudo ao caso em que $\xi \in F$.

Teorema 7.2. Dado um corpo F contendo uma raiz primitiva n-ésima da unidade ξ seja $x^n - a \in F[x]$ um polinômio irredutível (em geral basta supor $a \in (F^x)^n$) e seja K um corpo de raízes desse polinômio. Então $G(K;F) \simeq Z/nZ$.

Reciprocamente, se um corpo F contém uma raiz primitiva n-ésima da unidade ξ e K é uma extensão galoisiana com $G(K;F) \simeq Z/nZ$, então existe $a \in F$ tal que $x^n - a$ é irredutível em $F[x]$ e $K = F(\sqrt[n]{a})$ é o corpo de raízes de $x^n - a$.

Observação 7.2. Observe que a existência de uma raiz primitiva n-ésima da unidade ξ em F implica que $c(F)$ não divide n. De fato, se $n = pm$, com $p = c(F)$, então $1 = \xi^n = (\xi^m)^p$ implica que $(\xi^m - 1)^p = 0$, pois $1 = 1^p$. Mas $(\xi^m - 1)^p = 0$ em um corpo só é possível se $\xi^m - 1 = 0$. Mas isso contraria o fato de ξ ser raiz primitiva n-ésima ($x^n - a$ lembrar que $\xi^n = 1$ e para todo $1 \leq r < n$, $\xi^r \neq 1$).

Demonstração 7.6. Para demonstrarmos a primeira parte do teorema basta observarmos que se α é uma raiz de $x^n - a$, então $\xi\alpha$ será uma outra raiz. Observe que os elementos $\alpha, \xi\alpha, \cdots, \xi^{(n-1)}\alpha$ são todos distintos e são raízes de $x^n - a$. Logo esse conjunto se constituí no conjunto de todas as raízes de $x^n - a$ e estão todas elas em $F(\alpha)$. Portanto $K = F(\alpha)$ e assim $[K : F] = n$.

Por outro lado, como $x^n - a$ é irredutível por hipótese, existe $\sigma : K \longrightarrow K$, um F-automorfismo, tal que $\sigma(\alpha) = \xi\alpha$. Calculando-se iteradamente $\sigma_2(\alpha) = \xi^2\alpha, \cdots, \sigma^{(n-1)}(\alpha) = \xi^{(n-1)}\alpha e \sigma^n(\alpha) = \alpha$. Como $\sigma^n|F = id$, $K = F(\alpha)$ e $\sigma^n(\alpha) = \alpha$, podemos concluir que $\sigma^n = id$ e para todo $1 \leq r < n$, $\sigma^r \neq id$. Isto é $|\sigma| = n$ e como $|G(K;F)| = [K : F] = n$, obtemos que $G(K;F) =< \sigma >?$ é cíclico com ordem n. Logo $G(K;F) \simeq Z/nZ$, pois para cada n existe um único grupo cíclico de ordem n, a saber Z/nZ.

Verifiquemos agora que $x^n - a$ é irredutível em $F[x]$. Seja $p(x) \in F[x]$ o polinômio mínimo de d. Logo $grp(x) \leq n$. Por outro lado, para todo $0 \leq j < n$ temos que $p(\sigma^j(d)) = 0$ (lembrar que $G(K;F) = id, \sigma, \cdots \sigma^{(n-1)}$). Como sabemos que $\sigma^j(d) = \xi^j d$ essa igualdade mostra que $p(x)$ tem n raízes distintas, logo $grp(x) \geq n$. Dessa forma $grp(x) = n$, e como $p(x)$ divide $x^n - a$, concluímos que $p(x) = x^n - a$. Isso mostra que o polinômio $x^n - a$ é irredutível e mostra também que $K = F(d)$, i.e., d é um elemento primitivo da extensão.

Observação 7.3. O teorema acima é atribuído a Kummer. Observe que só demonstramos a existência do elemento primitivo d, mas não fornecemos um processo para calculá-lo. A equação $c + \xi^{(-1)}\sigma(c) + \xi^{(-2)}\sigma^2(c) + \cdots + \xi^{(-(n-1)))}\sigma^{(n-1)}(c)$ é chamada de "Resolvente de Lagrange".

No caso geral, como mencionado anteriormente, dada a equação $x^n - a \in F[x]$ irredutível e supondo-se que $c(F)$ não divide n construímos uma torre onde ξ é uma raiz primitiva n-ésima da unidade. $F(\xi)$ é uma extensão galoisiana de F com grupo de Galois abeliano. Pelo Teorema de Kummer acima K é uma extensão galoisiana de $F(\xi)$ com grupo de Galois cíclico, e a fortiori, abeliano. K é o corpo de raízes de $x^n - a = 0$. Recorde que $G(F(\xi) : F) \simeq G(K;F)/G(K;F(\xi))$. Como $G(F(\xi);F)$ é abeliano e temos para o grupo derivado $G(K;F)_{(1)} \subset G(K;F(\xi))$, implicando $G(K;F)_{(2)} \subset G(K;F(\xi))_{(1)} = 1$. A última igualdade decorre de $G(K;F(\xi)$ ser abeliano. Portanto $G(K;F)$ é resolúvel e assim, a equação $x^n - a = 0$ é resolúvel por radicais.

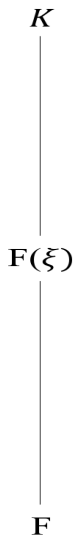

Figura 7.4: Extensão galoisiana de F.

Observe que por simples observação é claro que $x^n - a$ é resolúvel por radicais. Afinal tem como raiz $\sqrt[n]{a}$. Em outras palavras o teorema diz também que só no caso de $G(E;F)$ ser resolúvel, onde E é corpo de raízes de $f(x)$, é que a equação $f(x) = 0$ é resolúvel por radicais.

Por exemplo, seja ξ raiz primitiva n-ésima da unidade. A equação $x^n - 1$ é resolúvel por radicais, pois $G(F(\xi);F)$ é abeliano. Mas não podemos garantir que existem $F = F_o \subset F_1 \subset \cdots \subset F_t = F(\xi)$, onde $F_i = F_{i-1}(\alpha_i)$ com $\alpha_i^{ni} = \alpha_i \in F_{i-1}$, para todo $1 \leq i \leq t$. O que podemos garantir é que podemos colocar $F(\xi) \in K$ e para o K vai existir essa cadeia.

A questão de encontrar as equações do tipo $x^{ni} - ai$ é um tanto delicada, por isso a condição $G(E;F)$ é resolúvel para o corpo de raízes é importante. A condição garante que podemos fazer a construção, mas fazer a construção é muito mais complicado. Vejamos alguns exemplos da construção dos radicais para raízes primitivas n-ésimas da unidade ξ_n sobre $\mathbb{Q}$. Primeiro os fáceis:

Para $n = 3$, já sabemos que $\xi_3 \in \mathbb{Q}\sqrt{-3}$, um caso fácil.

Para $n = 4$, também é fácil: $\xi_4 \in F(\sqrt{-1})$.

Para $n = 5$, é fácil, mas não tanto. $[\mathbb{Q}(\xi_5), \mathbb{Q}] = 4$ e o grupo de Galois $G(\mathbb{Q}(\xi_5);\mathbb{Q}) \simeq (Z/5Z)^x$ será cíclico de ordem 4 gerado por $2+5\mathbb{Z}(G(\mathbb{Q}(\xi_5);\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$. Logo $G(\mathbb{Q}(\xi_5);\mathbb{Q})$ tem um subgrupo de ordem 2, $1 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$. Seja L o corpo fixo desse subgrupo; $\mathbb{Q} \subset L \subset \mathbb{Q}(\xi_5)$, onde $[L : \mathbb{Q}] = 2$ e $[\mathbb{Q}(\xi_5) : L] = 2$. Logo $L = \mathbb{Q}(\sqrt{a})$, para algum $a \in \mathbb{Q}$ e $\mathbb{Q}(\xi_5) = L(\sqrt{a})$, para algum $\alpha \in L$.

Mas quem são a e α se soubermos a, então $\alpha = b + c \cdot \sqrt{a}$, mas quem é a?

Para $n = 6$, temos $\phi_6(x) = x^2 - x + 1$, logo $\xi_6 \in \mathbb{Q}\sqrt{-3}$ e já encontramos uma extensão quadrática.

No caso $n = 7$ ainda estamos diante de um número pequeno (e primo), mas as dificuldades já aparecem. Na verdade podemos considerar que $n = 7$ ilustra bem como proceder para mergulhar um corpo dentro de uma extensão radical. Antes de tratar desse caso vamos apresentar um resultado geral que será necessário.

Proposição 7.5. Sejam E e L duas extensões finitas de um corpo F contidas em um fecho algébrico G de F. Definimos a composição de E e L como sendo $EL =$ interseção de todos os subcorpos de G que contém E e F simultaneamente. Nessas condições, se E for uma extensão galoisiana de F, então EL é uma extensão galoisiana de L e temos ainda $G(EL; L) \simeq G(E : E \cap L)$.

Demonstração 7.7. Observe que apesar da definição bastante geral da composição EL, temos que $E = F(\alpha_1, \cdots, \alpha_m)$, onde $\alpha_1, \cdots, \alpha_m$ são as raízes de um polinômio separável $f(x) \in F[x]$, pois E é galoisiana sobre F. Logo $EL = L(\alpha_1, \cdots, \alpha_m)$ é o corpo de raízes de $f(x) \in L[x]$ sobre L. Assim EL é galoisiana sobre L.

A única dificuldade está na descrição do grupo de Galois $G(EL; L)$. Para simplificar vamos assumir que $L = F(\beta)$ é uma extensão simples de F (caso contrário teríamos que trabalhar com uma base de L como F - espaço vetorial). Seja $g(x)$ o polinômio mínimo de β sobre F. Tomemos agora K o corpo de raízes de $f(x)g(x)$ sobre F. Logo $\alpha_1, \cdots, \alpha_m, \beta \in K$ e portanto $E, L \subset K$.

Como E é uma extensão galoisiana de F, pelo TG que $G(K; E) \lhd G(K; F)$. Por outro lado o TG também nos garante que $G(K; EL) = G(K; E) \cap G(K; L)$. De fato, observe que EL é o menor subcorpo de K que contém E e L simultaneamente. Pela correspondência entre corpos intermediários e subgrupos estabelecida no TG o grupo de Galois $G(K; EL)$ deverá ser o maior subgrupo de $G(K; F)$ contido em $G(K; E)$ e $G(K; L)$ simultaneamente; isso é precisamente a interseção $G(K; E) \cap G(K; L)$, como afirmado. Ilustramos abaixo o diagrama dos corpos envolvidos.

Vamos agora calcular o grupo de Galois $G(EL; L)$. Também pelo TG temos que

$$G(EL; L) \simeq G(K; L)/G(K; EL) = G(K; L)/(G(K; E) \cap (K; L)) \simeq G(K; L)G(K; E)/G(K; E), (\dagger)$$

onde o último isomorfismo vem do chamado "Terceiro Teorema do Isomorfismo".

Aqui novamente temos que interpretar o subgrupo $G(K; L)G(K; E)$. Esse é claramente o menor subgrupo de $G(K; F)$ que contém simultaneamente $G(K; L)$ e $G(K; E)$. Logo, pela correspondência entre corpos intermediários e subgrupos estabelecida no TG,

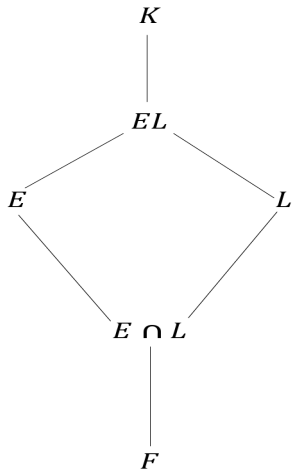

Figura 7.5: Diagrama da extensão de corpos.

$G(K;L)G(K;E)$ tem $E \cap L$ como corpo fixo, isto é, o maior subcorpo de K contido em E e L. Temos assim que $G(K;E \cap L) = G(K;L)G(K;E)$. Trocando-se o resultado obtido na equação (†) obtemos

$$G(EL;L) \simeq G(K;E \cap L)/G(K;E) = G(E : E \cap L)$$

como queríamos.

Para $n = 7$, temos que $[\mathbb{Q}(\xi_7) : \mathbb{Q}] = 6$ e $G(\mathbb{Q}(\xi_7);\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^x$ que novamente é um grupo cíclico de ordem 6. Seja H os subgrupo de $G = G(\mathbb{Q}(\xi_7);\mathbb{Q})$ com ordem 3 e seja também L o corpo fixo de H. Pelo TG temos que $[L : Q] = 2$. Logo $L = Q(\sqrt{c})$, para algum $c \in \mathbb{Q}$. Esse L tem a forma apropriada, mas o TG também nos diz que $G(Q(\xi_7);L) = H$ é um grupo cíclico de ordem 3. Mas existe algum $\alpha \in \mathbb{Q}(\xi_7)$ tal que $\alpha^3 \in L$. Na verdade vamos demonstrar que não existe um α nessas condições. De fato, se $Q(\xi_7) = L(\alpha)$ com $a = \alpha^3 \in L$, então $[L(\alpha) : L] = 3$ e α raiz de $x^3 - a \in L[x]$, implica que $x^3 - a$ é irredutível em $L[x]$ e tem como raízes $\alpha, \xi_3\alpha$, e $\xi^2\alpha$. Essas raízes estão todas em $L(\alpha)$, pois é uma extensão galoisiana de L. Resulta então que $\xi_3 \in L(\alpha)$. Seja $K = L(\alpha) = \mathbb{Q}(\xi_7)$. Temos então que $\xi_3, \xi_7 \in K^x$ e têm ordens relativamente primas, 3 e 7, respectivamente. Logo o produto $\xi = \xi_3\xi 7$ tem ordem 21 em K^x, isto é, ξ é uma raiz primitiva 21-ésima da unidade.

O polinômio mínimo de ξ sobre $\mathbb{Q}$ é $\phi_{21}(x)$ que tem grau $\sigma_{(21)} = 2 \times 6 = 12$. Logo $[\mathbb{Q}(\xi) : \mathbb{Q}] = 12$, $\sigma_{21}(x)$ é irredutível em $Q[x]$. Portanto não podemos ter $\alpha \in \mathbb{Q}(\xi_7)$, pois $[\mathbb{Q}(\xi_7) : \mathbb{Q}] = 6$. Conclusão: não podemos ter $\xi_3 \in \mathbb{Q}(\xi_7)$ e portanto não podemos ter $\alpha \in \mathbb{Q}(\xi_7)$ tal que $\alpha_3 \in L$, conforme afirmamos.

O que podemos ter é o seguinte: tomamos $F_o = \mathbb{Q}$ e $F_1 = F_o(\sqrt{a})$. Vimos acima

que tínhamos $L = \mathbb{Q}(\sqrt{c})$ com $c \in \mathbb{Q}$. Tomamos então $F_2 = F_1(\sqrt{c})$ e $F_3 = F_2(\xi_7)$. O diagrama, a seguir, ilustra as posições relativas dos corpos.

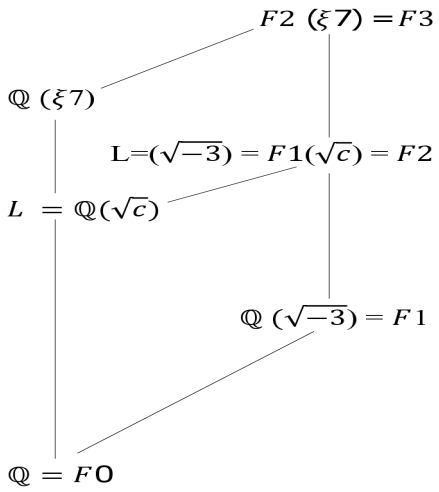

Figura 7.6: Extensão de radicais

Vimos que $\xi_3 \notin \mathbb{Q}(\xi_7)$, logo$\sqrt{(-3)} \notin \mathbb{Q}(\sqrt{c}) = L$. Portanto $\mathbb{Q}(\sqrt{c}) \cap \mathbb{Q}(\sqrt{(-3)}) = \mathbb{Q}$ e $L(\sqrt{(-3)}) = F_1(\sqrt{c}) = F_2$ é uma extensão quadrática tanto de L como de F_1. Observe que F_2 é a composição de L com F_1.

Temos que F_3 é a composição de $\mathbb{Q}(\xi_7)$ com F_2.

Por outro lado, vimos que $[Q(\xi_7) : L] = 3$ e que $[F_2 : L] = 2$. Portanto $\mathbb{Q}(\xi_7) \cap F_2 = L$. Também temos que $Q(\xi_7)$ é uma extensão galoisiana de L com grupo de Galois cíclico de ordem 3.

Em geral determinar que o grupo de Galois é resolúvel é mais simples do que construir uma extensão radical.

Caso quiséssemos demonstrar que podemos construir uma extensão radical K de $\mathbb{Q}$ contendo $\mathbb{Q}(\xi_n)$ para todo n teríamos que proceder por indução. O caminho é exatamente o que usamos no caso $n = 7$.

Capítulo 8

Considerações Finais

Évariste Galois concluiu que a construção de uma fórmula para as raízes de um polinômio $f(x)$ não-nulo, com $f \in K[x]$ em um corpo passa necessariamente pela construção de uma extensão L gerada por radicais e que contenha as raízes de $f(x)$, ou seja, o polinômio é solúvel por radicais quando suas raízes possam ser demonstradas como expressões envolvendo as propriedades de corpos e suas extensões, e que todo polinômio de grau 2,3 e 4 sobre os racionais é solúvel por radicais.

Em outras palavras a resolubilidade por radicais implica a resolubilidade do grupo de Galois. A recíproca também é verdadeira: se o grupo de Galois de uma extensão é solúvel, então a extensão é solúvel por radicais.

Referências Bibliográficas

1. H. Cohen, A COURSE IN COMPUTATIONAL ALGEBRAIC NUMBER THEORY, Springer.

2. P.A. Martin, INTRODUÇÃO À TEORIA DOS GRUPOS E À TEORIA DE GALOIS, IMEUSP

3. I.N. Herstein, TÓPICOS DE ÁLGEBRA, Polígono, São Paulo, 1964

4. I. Stewart, GALOIS THEORY, Chapman and Hall, 1989.

5. G. Butler and J.McKay, The transitive groups of degree up to eleven, Comm.in Algebra 11 A983), www. www.wikipédia.org, 14/12/2011.

6. S. Lang, ALGEBRA PARA GRADUAÇÃO, Ed. Ciência Moderna, Rio de Janeiro, 2008.

7. G. Ávila, ANÁLISE MATEMÁTICA PARA LICENCIATURA, Ed. Edgard Blucher, São Paulo, 2006.