Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

Introdução à Teoria de Galois

Autor: *Karina Branco da Cruz*

Orientador: *Waldeck Schützer*

Disciplina: Trabalho de Conclusão do Curso B

Curso: Licenciatura e Bacharelado em Matemática

Professores Responsáveis: Karina Schiabel
Sadao Massago
Vera Lúcia Carbone

São Carlos, 14 de março de 2014.

Introdução à Teoria de Galois

Autor: *Karina Branco da Cruz*

Orientador: *Waldeck Schützer*

Disciplina: Trabalho de Conclusão do Curso B

Curso: Licenciatura e Bacharelado em Matemática

Professores Responsáveis: Karina Schiabel
Sadao Massago
Vera Lúcia Carbone

Instituição: Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

São Carlos, 14 de março de 2014.

Karina Branco da Cruz

Waldeck Schützer

Ao Edson, meu pai.

Agradecimentos

Agradeço,

À Deus, primeiramente, por me guiar a esta carreira acadêmica, e ainda manter-me interessada diante a tantas dificuldades.

À minha família (minha mãe Rosana, meu pai Edson e meus irmãos: Igor e Vitor), pela devoção e suporte desde o meu nascimento.

Ao Kálley Menezes Carvalho Alves, por toda dedicação, companheirismo e estímulo que tornaram possível esta realização.

Aos meus estimados amigos, pela partilha de toda e qualquer emoção.

À todos os professores, pela contribuição à minha formação.

Em especial, ao Professor Waldeck Schützer, pela confiança, prazerosa oportunidade de aprendizado e excelente forma de findar meu curso.

Resumo

Assim como no Trabalho anterior, espera-se que este ajude a revisar, consolidar e fundamentar melhor os conhecimentos algébricos obtidos em disciplinas do Curso de Licenciatura e Bacharelado em Matemática, através do estudo sistemático, ainda que de forma introdutória, da formidável Teoria desenvolvida por Évariste Galois. Teoria esta, que se tem mostrado imprescindível para comprovação decisiva da não solubilidade de equações polinomiais de grau maior ou igual a cinco. Ademais, por sua grande abrangência, a mesma encontra inúmeras outras aplicações interessantes na, e fora da Matemática. A sua complexidade, exige um cuidadoso estudo de conceitos básicos da álgebra, como também dos da Teoria de Extensão de Corpos. E este cuidado, encontramos na consistência do Trabalho de Conclusão de Curso A. Agora, especificamente para o Trabalho de Conclusão de Curso B, entendemos o importante Teorema da Correspondência de Galois e sua consequência esplêndida na não solubilidade das equações polinomiais de grau maior ou igual a cinco.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

Segundo Eves (2011, [2]), Évariste Galois, pode ser considerado como um meteoro, que riscou o firmamento matemático com brilho intenso e matinal, para depois, súbita e pateticamente, extinguir-se em morte prematura, deixando material de valor extraordinário para ser trabalhado pelos matemáticos das gerações futuras.

Tal material, teve seu início de produção durante a adolescência de Galois, quando este, passou a construir uma teoria com aplicações sobretudo à teoria das equações algébricas. Um dos resultados mais salientes desta teoria é a impossibilidade de resolução por meio de radicais de equações gerais de grau maior ou igual a cinco.

Em busca de uma linguagem conveniente que permitisse capturar a essência do problema da resolubilidade de equações algébricas, Galois foi levado a considerar o conjunto das permutações das raízes da equação, essencialmente desenvolvendo a ideia de grupo, um conceito até então não formalizado. Foi ele quem utilizou o termo "grupo" pela primeira vez no seu sentido técnico atual.

A expressão do problema de construir soluções para equações partindo dos coeficientes é convenientemente realizada através do conceito de extensão de corpos. Um resultado fundamental da Teoria de Galois afirma que existe uma correspondência entre os subgrupos do grupo de Galois de uma equação e os subcorpos do corpo das raízes desta equação. A teoria das extensões, desenvolvida no Trabalho de Conclusão de Curso A, teve como aplicação imediata a demonstração na negativa das assim chamadas impossibilidades clássicas: a quadratura do círculo, a trissecção de um ângulo qualquer e a duplicação de um cubo, usando apenas régua e compasso.

O estudo da Teoria de Galois é particularmente interessante por motivar um estudo mais aprofundado de duas grandes sub-áreas da Álgebra: a Teoria dos Grupos e a Teoria dos Corpos.

Deste modo, o trabalho em questão, cujo objetivo imediato é o de consolidar e aprofundar alguns dos conceitos algébricos mencionados acima, dividiu-se primeiramente, em Trabalho de Conclusão de Curso A, contemplando os seguintes capítulos: Conceitos Básicos da Álgebra, O Teorema Fundamental da Álgebra, Fatoração de Polinômios, Extensões de Corpos, Extensões Simples, O Grau de uma Extensão e Construções com Régua e Compasso; e, em Trabalho de Conclusão de Curso B, abrangendo os capítulos: Normalidade e Separabilidade, Automorfismos de Corpos, A Correspondência de Galois, Um exemplo prático, Solubilidade e Simplicidade, Solução por Radicais e O Polinômio Geral.

O capítulo inicial apresenta alguns conceitos da álgebra clássica fundamentais para a futura compreensão da Teoria de Galois (foco do trabalho). Como também, exibe um panorama geral do significado da solubilidade por radicais de equações polinomiais e instiga a pensarmos sobre a impossibilidade desta, em equações de grau maior ou igual a cinco.

Os capítulos seguintes, dois e três, de um modo geral, retomam conceitos e propriedades importantes de polinômios (e portanto, de equações polinomiais). Dentre o que estes abrangem, o Teorema Fundamental da Álgebra merece destaque, uma vez que, este é responsável por responder a seguinte pergunta: existe alguma equação polinomial com coeficientes em $\mathbb{C}$ que não possui raiz sobre $\mathbb{C}$? E ao respondê-la, mostrar a não necessidade de extensão do corpo dos números complexos.

Enquanto que os demais capítulos: Extensões de Corpos, Extensões Simples e O Grau de uma Extensão, são responsáveis por introduzir parte do que contempla a Teoria de Extensões de Corpos, que como já mencionado, é consequência imediata de um estudo da Teoria de Galois.

O último capítulo referente ao Trabalho de Conclusão de Curso A, intitulado Construções com Régua e Compasso, tem como propósito aplicar a Teoria anteriormente descrita e solucionar o problema das impossibilidades clássicas, que há muito, perturbaram os gregos.

Quanto ao Trabalho de Conclusão de Curso B, temos seu início no oitavo capítulo. Neste, as propriedades de certo modo complementares, normalidade e separabilidade, são expressas, exemplificadas e devidamente compreendidas em virtude da posterior necessidade no Teorema da Correspondência de Galois. O trabalho prossegue apresentando o conceito de K-automorfismo e construindo o mesmo a partir da exigência da sobrejetividade de um K-monomorfismo, conceito este, que é imprescindível para o entendimento do Grupo de Galois de uma Extensão.

Os capítulos dez e onze, contemplam o auge deste Trabalho. Neles juntamos as peças do quebra-cabeças belíssimo proposto por Galois e exemplificamos o mesmo de modo a tornar esta Teoria digerível.

Por fim, os três capítulos finais, Solubilidade e Simplicidade, Solução por Radicais e O Polinômio Geral (respectivamente), englobam o contéudo já discutido e mostram o porquê de uma quíntica não ser resolvível por radicais.

Capítulo 1

Conceitos Básicos da Álgebra

Antes de iniciarmos nosso trabalho com a Teoria de Galois, apresentaremos alguns conceitos da álgebra, fundamentais para posterior compreensão. Deste modo, entenderemos o conceito de anel, corpo, subanel, subcorpo, homomorfismos (em suas variedades, por exemplo, monomorfismos), números complexos, relações de equivalência, classes de equivalência, equações e seus métodos de resoluções, como também soluções por meio de radicais.

1.1 Anel, Corpo, Subanel e Subcorpo - Definições e Exemplos

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

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

Chamaremos $(A, +, \cdot)$ um anel se as seguintes seis propriedades são satisfeitas, quaisquer que sejam $a, b, c \in A$:

A1) Associatividade da adição: $(a+b)+c = a+(b+c)$;

A2) Existência do elemento neutro para a adição: $\exists\ 0 \in A$ tal que $a+0 = 0+a = a$;

A3) Existência do inverso aditivo: $\forall x \in A$ existe um único $y \in A$, denotado por $y = -x$, tal que $x+y = y+x = 0$;

A4) Comutatividade da adição: $a+b = b+a$;

M1) Associatividade da multiplicação: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

D) Distributividade à esquerda: $a \cdot (b + c) = a \cdot b + a \cdot c$
Distributividade à direita: $(a + b) \cdot c = a \cdot c + b \cdot c$.

Além das propriedades que o caracterizam, um anel pode possuir (não necessariamente) outras propriedades:

M2) $\exists\ 1 \in A, 0 \neq 1$, *tal que,* $x \cdot 1 = 1 \cdot x = x$, $\forall x \in A$, *e neste caso, dizemos que* $(A, +, \cdot)$ *é um anel com unidade.*

M4) $\forall x, y \in A$, $x \cdot y = y \cdot x$, *e assim,* $(A, +, \cdot)$ *é um anel comutativo.*

DZ) $x, y \in A$, $x \cdot y = 0 \Rightarrow x = 0$ *ou* $y = 0$, *em que,* $(A, +, \cdot)$ *é dito ser um anel sem divisores de zero.*

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

Finalmente, se um domínio de integridade $(A, +, \cdot)$ *satisfaz a propriedade:*

$$M3) \quad \forall x \in A, x \neq 0, \exists\ y \in A, \text{ tal que, } \quad x \cdot y = y \cdot x = 1,$$

dizemos que $(A, +, \cdot)$ *é um corpo.*

Definição 1.1.2 (Subanéis)**.** *Seja* $(A, +, \cdot)$ *um anel e* B *um subconjunto não vazio de* A. *Suponhamos que* B *seja fechado para as operações* $+$ *e* $\cdot$ *de* A, *isto é,*

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

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

Assim podemos considerar a adição e a multiplicação de A *como operações de* B. *Se* $(B, +, \cdot)$ *for um anel com estas operações, dizemos que* B *é um subanel de* A.

Proposição 1.1.3. *Seja* $(A, +, \cdot)$ *um anel e seja* B *um subconjunto de* A. *Então,* B *é um subanel de* A, *se, e somente se, as seguintes condições são verificadas:*

(i) O elemento neutro de A *pertence a* B: $0 \in B$;

(ii) B *é fechado para a diferença:* $x, y \in B \Rightarrow x - y \in B$;

(iii) B *é fechado para o produto:* $x, y \in B \Rightarrow x \cdot y \in B$.

Demonstração. A demonstração de tal proposição, pode ser consultada em [3]. □

Definição 1.1.4. *Se* $(A, +, \cdot)$ *é um corpo, um subconjunto* B *de* A *é dito ser um subcorpo, se este é um subanel de* A, *e além disso, se* $x \in B$, $x \neq 0$, *então* $x^{-1} \in B$.

Exemplos 1.1.5. *Contemplaremos alguns exemplos dos conceitos anteriormente definidos de um modo superficial, o leitor curioso poderá consultar detalhes em livros de álgebra, como por exemplo, [3] e [4].*

1. *Se A for o conjunto de todas as matrizes reais 2×2, com as operações usuais, isto é,*
$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\},$$
temos que A é um anel não comutativo com unidade e com divisores de zero. Podemos generalizar tal fato a $Mat_n(\mathbb{R})$;

2. *Se $\mathcal{F}(\mathbb{R})$ é o conjunto das funções $f : \mathbb{R} \to \mathbb{R}$, definido com as operações usuais, então $\mathcal{F}$ é um anel comutativo com unidade e com divisores de zero;*

3. *$\mathbb{Z}$, o conjunto dos números inteiros, é um domínio de integridade;*

4. *$n \cdot \mathbb{Z}$, com $n \geq 2$ ($n \in \mathbb{N}$), são exemplos de anéis comutativos sem unidade;*

5. *$\mathbb{Z}_n$, com $n \geq 2$ ($n \in \mathbb{N}$) e não primo, são um anéis comutativos com divisores de zero. Em particular, $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ o é. Note que, $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$, ou seja, $\overline{2}, \overline{3}$ são divisores de zero em $\mathbb{Z}_6$;*

6. *$\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$ com p primo é um domínio de integridade;*

7. *$\mathbb{Z}_p$ com p primo é um corpo;*

8. *$\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos;*

9. *Como $\mathbb{Q} \subseteq \mathbb{C}$ temos que $\mathbb{Q}$ é um subcorpo de $\mathbb{C}$, e portanto, um subanel do mesmo.*

1.2 Homomorfismo de Anéis

O conceito de extensão, crucial para o desenvolvimento da Teoria de Galois, exige o conhecimento de algumas funções específicas entre corpos, de um modo mais geral, entre anéis. Para tanto, vejamo-nas brevemente.

Definição 1.2.1. *Sejam A e A' dois anéis. Denotemos (por comodidade), as operações de ambos anéis pelos símbolos $+$ e $\cdot$; 0 para o elemento neutro de A; $0'$, para o, de A'; 1 para a unidade de A (caso este possua), e $1'$, para a, de A'.*
Uma função $f : A \to A'$ diz-se um homomorfismo de A em A' se satisfaz as seguintes condições:

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

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

Definição 1.2.2. *Se $f : A \to A'$ for um homomorfismo injetor, dizemos que f é um monomorfismo.*

Definição 1.2.3. *Se $f : A \to A'$ for um homomorfismo bijetivo, dizemos que f é um isomorfismo. E portanto, os anéis A e A' são isomorfos, donde escrevemos $A \simeq A'$.*

Definição 1.2.4. *Os homomorfismos $f : A \to A$ são chamados também de endomorfismos de A, já os isomorfismos de A sobre si mesmo são chamados de automorfismos de A.*

Proposição 1.2.5. *Sejam A e A' anéis. Seja $f : A \to A'$ um homomorfismo. Então,*

(a) $f(0) = 0'$;

(b) $f(-a) = -f(a), \quad \forall a \in A$;

(c) Se A e A' são domínios de integridade, então ou f é a função constante zero, ou $f(1) = 1'$;

(d) Se A e A' são corpos, então ou f é a função constante zero, ou f é injetiva (isto é, f é um monomorfismo).

Demonstração. Esta demonstração pode ser encontrada em [3]. □

Partindo da ideia de trabalho com algo mais palpável, definiremos Grupos de Galois e toda a Teoria de Galois para números complexos, para futuramente apresentarmos de um modo mais simplificado uma visão abstrata dos mesmos.

Podemos entender as extensões naturais em inteiros, em racionais, em reais e em complexos como uma necessidade de resolver mais equações. Este é um ponto crucial da Teoria de Galois, que determina a solubilidade ou não de uma equação polinomial.

Sendo assim, a ideia de número complexo surge da necessidade de resolução de certas equações. Mais especificamente, do encontro das raízes da equação $x^2 + 1 = 0$, que não possui solução em $\mathbb{R}$ (notar que o discriminante é um número negativo, e não temos definida raiz de um número negativo em $\mathbb{R}$).

1.3 Números Complexos

Podemos representar um número complexo de três maneiras equivalentes: algébrica, matricial e geométrica.

Dado um número $z \in \mathbb{C}$, dizemos que sua forma algébrica é dada por: $z = x + iy$, onde $x = Re(z)$ e $y = Im(z)$; ou ainda, como par ordenado representado no plano $\mathbb{R}^2$, $z = (x, y)$.

Já a forma matricial, com $x = Re(z),\ y = Im(z)$, tem o seguinte aspecto,

$$z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Por fim, temos a forma geométrica, $z = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta))$, obtida considerando $\rho = \sqrt{x^2 + y^2}$ como sendo o módulo do número complexo $z = x + iy$ e $\theta \in [0, 2\pi]$, o argumento do ângulo, em que, $\cos(\theta) = \dfrac{x}{\rho}$ e $\mathrm{sen}(\theta) = \dfrac{y}{\rho}$.

Notemos que a equivalência destas três formas de representação de um número complexo é proveniente de isomorfismos, pela forma que definimos as formas matricial e geométrica, temos claramente o isomorfismo entre estas e a forma algébrica. Os demais isomorfismos são obtidos por meio de composição destes já conhecidos.

Uma maneira intuitiva de definir o significado de $\sqrt{-1}$ é considerar $\mathbb{C}$ na sua forma algébrica como um conjunto de $\mathbb{R}^2$, isto é, de todos os pares de números reais (x, y), com as operações:

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= (x_1 + x_2, y_1 + y_2)\\ (x_1, y_1) \cdot (x_2, y_2) &= (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)\end{aligned}$$

Assim, identificamos um número real como sendo da forma $(x, 0)$, com $x \in \mathbb{R}$, e vemos que $\mathbb{R} \subset \mathbb{C}$; ainda, definimos $i = (0, 1)$. Consequentemente, (x, y) se torna $x + iy$.

O modo como definimos as operações implicam que $i^2 = (0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 0 \cdot 1) = (-1, 0) = -1$, logo, $i = \sqrt{-1}$. Notemos que $i = (0, 1)$ não é da forma $(x, 0)$ real, o que de fato não deveria ser, pois não há raiz real de -1.

1.4 Relação de Equivalência

A importância desta seção no decorrer do trabalho, será evidenciada quando falarmos sobre a congruência módulo n, sendo n um inteiro positivo; algo presente inclusive no último capítulo sobre Construções com Régua e Compasso.

Suponhamos que em um conjunto A esteja definida uma relação entre pares de elementos de A. Se $x, x' \in A$ escreveremos $x\mathcal{R}x'$ se x estiver relacionado com x' por $\mathcal{R}$, e $x\not\mathcal{R}x'$ caso contrário.

Definição 1.4.1 (Relação de Equivalência)**.** *Seja A um conjunto e seja $\mathcal{R}$ uma relação entre pares de elementos de A. Dizemos que $\mathcal{R}$ é uma relação de equivalência em A se as seguintes propriedades são verificadas quaisquer que sejam $x, x', x'' \in A$:*

1. *Reflexiva: $x\mathcal{R}x$;*
2. *Simétrica: se $x\mathcal{R}x'$ então $x'\mathcal{R}x$;*
3. *Transitiva: se $x\mathcal{R}x'$ e $x'\mathcal{R}x''$ então $x\mathcal{R}x''$.*

Usaremos $\sim$ quando a relação for de equivalência.

Exemplos 1.4.2.

1. *Uma relação de equivalência trivial é a de igualdade sobre qualquer conjunto numérico;*

2. *A relação de ortogonalidade sobre o conjunto de retas do plano não é de equivalência, pois não é reflexiva e nem transitiva como pode ser visto na Figura 1.1.*

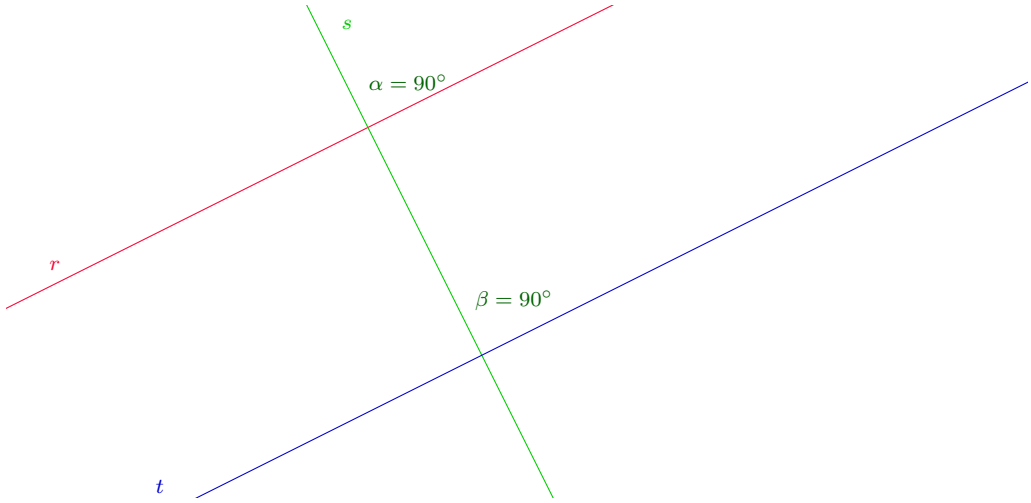

Figura 1.1: Ilustração demonstrando que ortogonalidade não é relação de equivalência

em que $r \perp s$, $s \perp t$, porém $t \parallel r$.

3. *Pode ser mostrado facilmente que a relação de paralelismo é de equivalência.*

4. *Seja $f : A \to B$ uma função, definamos uma relação de equivalência no domínio A da f, do seguinte modo:*

$$x, x' \in A,\ x \sim x' \text{ se } f(x) = f(x').$$

Verifiquemos as três propriedades (reflexiva, simétrica e transitiva) para vermos de fato que esta é uma relação de equivalência:

   (a) *Dado $x \in A$, $x \sim x$, pois $f(x) = f(x)$, já que f é função;*

   (b) *Dados $x, x' \in A$, se $x \sim x'$, então $f(x) = f(x')$, e como a igualdade é simétrica, concluímos que $x' \sim x$;*

   (c) *Dados $x, x', x'' \in A$, se $x \sim x'$ e $x' \sim x''$, então $f(x) = f(x')$ e $f(x') = f(x'')$, e usando a transitividade da igualdade, concluímos a transitividade da relação $\sim$ em questão.*

Definição 1.4.3 (Classe de Equivalência)**.** *Seja $\sim$ uma relação de equivalência em um conjunto A, e seja $x \in A$. Definamos a classe de equivalência $\overline{x}$ do elemento x em*

relação $a \sim$, como o conjunto de todos os elementos $a \in A$ relacionados a x, isto é, $\overline{x} = \{a \in A : a \sim x\}$.

Proposição 1.4.4. *Seja $\sim$ uma relação de equivalência em um conjunto A e sejam $x, y \in A$. Então,*

1. $\overline{x} = \overline{y} \Leftrightarrow x \sim y$;
2. $\overline{x} \neq \overline{y} \Rightarrow \overline{x} \cap \overline{y} = \emptyset$;
3. $\bigcup_{x \in A} \overline{x} = A$.

Ou seja, uma relação de equivalência define uma partição.

Demonstração.

1. ($\Rightarrow$) Sejam $x, y \in A$ e $\overline{x} = \overline{y}$. Temos de mostrar que $x \sim y$.

   Como $\sim$ é de equivalência, $x \in \overline{x}$ e $\overline{x} = \overline{y} \Rightarrow x \in \overline{y} \Rightarrow x \sim y$.

   ($\Leftarrow$) Sejam $x, y \in A$ e $x \sim y$. Temos de mostrar que $\overline{x} = \overline{y}$.

   Como $x \sim y$, temos que $x \in \overline{y}$, e portanto, $\overline{x} \subseteq \overline{y}$. Simetricamente, $\overline{y} \subseteq \overline{x}$. Donde, concluímos a igualdade desejada.

2. Suponhamos $x, y \in A$ e $\overline{x} \neq \overline{y}$. Se $a \in \overline{x} \cap \overline{y}$ então $a \sim x$ e $a \sim y$. Assim, $x \sim y$. Pelo item anterior, conseguimos que $\overline{x} = \overline{y}$, o que contraria a hipótese. Logo, $\overline{x} \cap \overline{y} = \emptyset$.

3. Vamos provar que $\bigcup_{x \in A} \overline{x} = A$. De fato, temos primeiramente que $\overline{x} \subset A, \forall x \in A$, daí segue que $\bigcup_{x \in A} \overline{x} \subset A$. Reciprocamente, temos que $x \in \overline{x}, \forall x \in A$, portanto, segue que $A \subset \bigcup_{x \in A} \overline{x}$.

□

Exemplo 1.4.5. *Seja $A = \mathbb{Z}$, e n um número inteiro arbitrariamente fixado.*
Vamos definir uma relação de equivalência em $\mathbb{Z}$ do seguinte modo:

$$x, x' \in \mathbb{Z},\ x \sim x' \Leftrightarrow x - x' \text{ é um múltiplo inteiro de } n.$$

Verifiquemos que esta é uma relação de equivalência:

1. *Dado $x \in \mathbb{Z}$, $x \sim x$, pois $x - x = 0 = n \cdot 0$;*
2. *Dados $x, x' \in \mathbb{Z}$, se $x \sim x'$, então $x - x' = n \cdot m$ para algum $m \in \mathbb{Z}$. Ora, $(x' - x) = -(x - x') = n \cdot -m$ para o mesmo $m \in \mathbb{Z}$, portanto, $x' \sim x'$;*

3. *Dados $x, x', x'' \in \mathbb{Z}$, se $x \sim x'$ e $x' \sim x''$, então $x - x' = n \cdot m$ para algum $m \in \mathbb{Z}$ e $x' - x'' = n \cdot p$ para algum $p \in \mathbb{Z}$. Mas, $(x - x'') = (x - x') + (x' - x'') = n \cdot m + n \cdot p = n \cdot (m + p)$ para m e p acima falados. Como o conjunto dos inteiros é um domínio de integridade, temos a validade da propriedade distributiva anteriormente usada, como também o fechamento diante as operações, isto é, $m + p \in \mathbb{Z}$, o que mostra que $x \sim x''$.*

Tal relação é chamada congruência módulo n e denotada por $\equiv (mod\ n)$.

Como, dado $x \in \mathbb{Z}$, $\overline{x} = \{a \in \mathbb{Z} : a \equiv x (mod\ n)\}$, e $a \in \overline{x} \Leftrightarrow a - x = n \cdot k$, para algum $k \in \mathbb{Z} \Leftrightarrow a = x + n \cdot k, k \in \mathbb{Z}$. Segue que $\overline{x} = \{x + n \cdot k, k \in \mathbb{Z}\}$.

Observe que se $n = 0$, temos que $\overline{x} = x$ e que $\equiv (mod\ 0)$ nada mais é do que a relação de igualdade em $\mathbb{Z}$. Por outro lado, se $n > 0$, a relação $\equiv (mod\ n)$ nos proporciona n classes distintas $\overline{0}, \overline{1}, ..., \overline{n-1}$.

Definição 1.4.6 (Conjunto Quociente)**.** *Seja $\sim$ uma relação de equivalência em um conjunto A. Chamamos de conjunto quociente de A pela relação de equivalência $\sim$, e denotamos por $\frac{A}{\sim}$, ao conjunto de todas as classes de equivalência relativamente a $\sim$.*

Assim,

$$\frac{A}{\sim} = \{\overline{x} : x \in A\}.$$

Proposição 1.4.7. *Seja $\sim$ uma relação de equivalência em um conjunto A, e seja $\frac{A}{\sim}$, o conjunto quociente de A por $\sim$. Seja $\pi : A \to \frac{A}{\sim}$ definida por $\pi(x) = \overline{x}, \forall x \in A$, chamada de projeção canônica.*

Então a relação $\sim$ é proveniente da função π.

Demonstração. De fato, basta observar que se $x, y \in A$ temos $x \sim y \Leftrightarrow \overline{x} = \overline{y} \Leftrightarrow \pi(x) = \pi(y)$, como queríamos. □

1.5 Resolvendo Equações

A História da Matemática nos mostra que a razão usual para a introdução de um novo tipo de número é a inadequação dos números antigos para a solução de alguns problemas relevantes.

Por exemplo, o passo de $\mathbb{N}$ para $\mathbb{Z}$ é necessário, uma vez que, equações como,

$$t + 7 = 2$$

não podem ser resolvidas para $t \in \mathbb{N}$. Entretanto, tais equações podem ser resolvidas em $\mathbb{Z}$.

Similarmente, o passo de $\mathbb{Z}$ para $\mathbb{Q}$, tornou possível a resolução da equação,

$$2t = 7.$$

E, de uma forma geral,

$$at + b = 0,$$

em que a, b são números específicos e t é um número desconhecido (ou variável). Tais equações são ditas lineares. E estas, vistas em subcorpos de $\mathbb{C}$, podem ser resolvidas com a solução única $t = \frac{-b}{a}$, quando $a \neq 0$.

O passo de $\mathbb{Q}$ para $\mathbb{R}$ é relatado por um tipo diferente de equação:

$$t^2 = 2,$$

já que a solução $t = \sqrt{2}$ é um número irracional.

Analogamente, o passo de $\mathbb{R}$ para $\mathbb{C}$ é centrado na equação,

$$t^2 = -1$$

que não tem soluções reais, pois o conjunto dos números reais é um corpo bem ordenado, e o quadrado de qualquer número real sempre é um número positivo.

Equações da forma,

$$at^2 + bt + c = 0$$

são chamadas de equações quadráticas. A fórmula clássica para suas soluções é:

$$t = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

com $a \neq 0$.

Para os números reais, a fórmula faz sentido se $b^2 - 4ac \geq 0$ e não se $b^2 - 4ac < 0$; para os complexos, ela faz sentido em qualquer um dos casos. Para os racionais, esta faz sentido apenas quando $b^2 - 4ac$ é um quadrado perfeito.

1.6 Solução por radicais

Entendendo solução por radicais de uma equação polinomial, como sendo o encontro de raízes da mesma, por meio de apenas operações elementares (adição, subtração, multiplicação, divisão e radiciação), analisaremos nesta seção o comportamento específico dos tipos de polinomiais.

1.6.1 Equações Lineares

Sejam $a, b \in \mathbb{C}$, com $a \neq 0$. Uma equação linear geral é:

$$at + b = 0$$

e a solução é claramente,

$$t = \frac{-b}{a}.$$

1.6.2 Equações Quadráticas

Sejam $a, b, c \in \mathbb{C}$, com $a \neq 0$. Uma equação quadrática geral é,

$$at^2 + bt + c = 0.$$

Dividindo todos os membros por a e renomeando os coeficientes, podemos considerar tal equação equivalente a,

$$t^2 + at + b = 0.$$

A maneira padrão de resolver esta equação é reescrevê-la na seguinte forma, através do completamento de quadrados (feito pelos Babilônios há 3600 anos):

$$\left(t + \frac{a}{2}\right)^2 = \frac{a^2}{4} - b;$$

Extraindo a raiz quadrada,

$$t + \frac{a}{2} = \pm\sqrt{\frac{a^2}{4} - b},$$

e então,

$$t = \frac{1}{2}\left(-a \pm 2\sqrt{\frac{a^2}{4} - b}\right).$$

1.6.3 Equações Cúbicas

Sejam $a, b, c \in \mathbb{C}$. Uma equação geral cúbica é da forma,

$$t^3 + at^2 + bt + c = 0,$$

Suponhamos primeiramente que $a \neq 0$, assim nosso primeiro passo para resolvermos tal equação é mudar a variável para termos uma outra equação equivalente a esta, com $a = 0$. Façamos a mudança $y = t + \frac{a}{3}$, e então $t = y - \frac{a}{3}$. A equação com tal mudança fica,

$$\begin{aligned}
\left(y - \frac{a}{3}\right)^3 + a\left(y - \frac{a}{3}\right)^2 + b\left(y - \frac{a}{3}\right) + c &= 0 \\
y^3 - y^2 a + y\frac{a^2}{3} - \frac{a^3}{27} + ay^2 - 2\frac{a^2 y}{3} + \frac{a^3}{9} + by - b\frac{a}{3} + c &= 0 \\
y^3 + \left(b - \frac{a^2}{3}\right)y + \left(\frac{a^3}{9} + c - b\frac{a}{3} - \frac{a^3}{27}\right) &= 0 \\
y^3 + py + q &= 0
\end{aligned}$$

onde $p = \left(b - \frac{a^2}{3}\right)$ e $q = \left(\frac{a^3}{9} + c - b\frac{a}{3} - \frac{a^3}{27}\right)$.

Podemos, assim, assumir que toda equação cúbica seja da forma $y^3 + py + q = 0$.

Donde, para encontrarmos a solução s, tentaremos a substituição

$$y = \sqrt[3]{u} + \sqrt[3]{v}.$$

Assim,

$$\begin{aligned} y^3 &= (\sqrt[3]{u} + \sqrt[3]{v})^3 \\ &= u + 3(\sqrt[3]{u})^2\sqrt[3]{v} + 3\sqrt[3]{u}(\sqrt[3]{v})^2 + v \\ &= u + v + 3\sqrt[3]{u}\sqrt[3]{v}(\sqrt[3]{u} + \sqrt[3]{v}). \end{aligned}$$

Então a equação $y^3 + py + q = 0$, torna-se,

$$\begin{aligned} u + v + 3\sqrt[3]{u}\sqrt[3]{v}(\sqrt[3]{u} + \sqrt[3]{v}) + p(\sqrt[3]{u} + \sqrt[3]{v}) + q &= 0 \\ \Leftrightarrow (u + v + q) + (\sqrt[3]{u} + \sqrt[3]{v})(3\sqrt[3]{u}\sqrt[3]{v} + p) &= 0. \end{aligned}$$

Escolhemos agora u e v de modo que:

$$u + v + q = 0$$

e

$$3\sqrt[3]{u}\sqrt[3]{v} + p = 0,$$

o que implica em,

$$u + v = -q \tag{1.1}$$

e

$$u \cdot v = \frac{-p^3}{27}. \tag{1.2}$$

Multiplicando a Equação (1.1) por u e substituindo a Equação (1.2), conseguimos,

$$u(u + v) - u \cdot v = -qu + \frac{p^3}{27}$$

que ao ser reorganizada, torna-se uma equação quadrática:

$$u^2 + qu - \frac{p^3}{27} = 0.$$

As soluções desta equação são, respectivamente,

$$u = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

e

$$v = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Disto, encontramos

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

que é chamada fórmula de Cardano (por virtude de publicação).

Finalmente, lembrando que a solução t da equação original é igual a $y - \frac{a}{3}$, resolvemos o problema.

1.7 Peculiaridades da Fórmula de Cardano

Lembremos de que, sobre $\mathbb{C}$, qualquer número complexo z não nulo possui três raízes cúbicas. Se uma delas é α, então as demais são $\omega\alpha$ e $\omega^2\alpha$. onde $\omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$.

A expressão para y, entretanto, aparece com nove soluções da forma:

$$\begin{array}{ccc} \alpha+\beta & \alpha+\omega\beta & \alpha+\omega^2\beta \\ \omega\alpha+\beta & \omega\alpha+\omega\beta & \omega\alpha+\omega^2\beta \\ \omega^2\alpha+\beta & \omega^2\alpha+\omega\beta & \omega^2\alpha+\omega^2\beta \end{array}$$

onde α, β são escolhas específicas das raízes cúbicas.

Entretanto, nem todas estas expressões são zeros. Se escolhermos α, β tal que $3\alpha\beta + p = 0$, então as soluções são: $\alpha+\beta$, $\omega\alpha+\omega^2\beta$, $\omega^2\alpha+\omega\beta$.

Outras peculiaridades emergem quando nos deparamos com equações cujas soluções são conhecidas. Por exemplo, $y^3+3y-36=0$, que tem $y=3$ como solução. Por Cardano, temos

$$\begin{aligned} y &= \sqrt[3]{18 + \sqrt{\frac{36^2}{4} + \frac{3^3}{27}}} + \sqrt[3]{18 - \sqrt{\frac{36^2}{4} + \frac{3^3}{27}}} \\ &= \sqrt[3]{18 + \sqrt{\left(\frac{36}{2}\right)^2 + 1}} + \sqrt[3]{18 - \sqrt{\left(\frac{36}{2}\right)^2 + 1}} \\ &= \sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}}, \end{aligned}$$

que parece estar bem longe de 3.

Como Cardano observou em seu livro, isto piora. A fórmula homônima aplicada a $t^3 - 15t - 4 = 0$, resulta em $t = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$, que contrasta com a solução por inspeção $t = 4$.

Estes pequenos erros de Cardano (que conscientemente os reconhecia), foram devidamente consertados por volta de 1560 com Raphael Bombelli e 1629 com Albert Girard.

1.8 Equações Quárticas

Começamos com, $t^4+at^3+bt^2+ct+d=0$. Fazemos a transformação de Tschirnhaus, $y=t+\frac{a}{4}$, donde $t=y-\frac{a}{4}$, e obtemos:

$$\left(y-\frac{a}{4}\right)^4+a\left(y-\frac{a}{4}\right)^3+b\left(y-\frac{a}{4}\right)^2+c\left(y-\frac{a}{4}\right)+d=0$$

$$\left(y-\frac{a}{4}\right)\left(y-\frac{a}{4}\right)^3+a\left(y^3-3y^2\frac{a}{4}+3y\frac{a^2}{16}-\frac{a^3}{64}\right)+b\left(y^2-\frac{a}{2}y+\frac{a^2}{16}\right)+cy-\frac{ca}{4}+d=0$$

$$\left(y-\frac{a}{4}\right)\left(y^3-3y^2\frac{a}{4}+3y\frac{a^2}{16}-\frac{a^3}{64}\right)+ay^3-3y^2\frac{a^2}{4}+3y\frac{a^3}{16}-\frac{a^4}{64}+by^2-b\frac{a}{2}y+b\frac{a^2}{16}+cy-c\frac{a}{4}+d=0$$

$$\begin{aligned}y^4-3y^3\frac{a}{4}+3y^2\frac{a^2}{16}-\frac{a^3}{64}y-y^3\frac{a}{4}+3y^2\frac{a^2}{16}-3y\frac{a^3}{64}+\frac{a^4}{64\cdot 4}+\\ +ay^3-3y^2\frac{a^2}{4}+3\frac{a^3}{16}-\frac{a^4}{64}+by^2-b\frac{a}{2}y+b\frac{a^2}{16}+cy-c\frac{a}{4}+d=0\end{aligned}$$

$$y^4+\left(6\frac{a^2}{16}-3\frac{a^2}{4}+b\right)y^2+\left(-\frac{a^3}{16}+3\frac{a^3}{16}-\frac{ba}{2}+c\right)y+\left(\frac{a^4}{64\cdot 4}-\frac{a^4}{64}-c\frac{a}{4}+d+b\frac{a^2}{16}\right)=0$$

Fazendo $p=\left(6\frac{a^2}{16}-3\frac{a^2}{4}+b\right)$, $q=\left(-\frac{a^3}{16}+3\frac{a^3}{16}-\frac{ba}{2}+c\right)$ e $r=\left(\frac{a^4}{64\cdot 4}-\frac{a^4}{64}-c\frac{a}{4}+d+b\frac{a^2}{16}\right)$, podemos reescrever a equação na forma,

$$\left(y^2+\frac{p}{2}\right)^2=-qy-r+\frac{p^2}{4}. \tag{1.3}$$

Introduzimos agora um novo parâmetro u, e observamos que:

$$\begin{aligned}\left(y^2+\frac{p}{2}+u\right)^2 &= \left(y^2+\frac{p}{2}\right)^2+2\left(y+\frac{p}{2}\right)u+u^2\\ &= -qy-r+\frac{p^2}{4}+2uy+pu+u^2\end{aligned}$$

onde na última igualdade usamos (1.3).

Escolhemos u de modo que o lado direito seja um quadrado perfeito. Se ele o é, este deve ser o quadrado de $\sqrt{2u}y-\frac{q}{2}\sqrt{2u}$, e então,

$$-r+\frac{p^2}{4}+pu+u^2=\frac{q^2}{8u}.$$

Equivalentemente, com $u\neq 0$,

$$8u^3+8pu^2+(2p^2-8r)u-q^2=0, \tag{1.4}$$

que é cúbica em u. Resolvendo pelo método de Cardano, encontramos u. Agora,

$$\left(y^2 + \frac{p}{2} + u\right)^2 = \left(\sqrt{2u}y - \frac{q}{2}\sqrt{2u}\right)^2$$

então, $y^2 + \frac{p}{2}u = \pm\left(\sqrt{2u}y - \frac{q}{2}\sqrt{2u}\right)$. Finalmente, conseguimos resolver a quadrática acima encontrando y.

Se $u = 0$, não obtemos (1.4), mas se $u = 0$, então $q = 0$, e a equação quártica $y^4 + py^2 + qy + r = 0$ é quadrática em y^2, e pode ser resolvida usando apenas raízes quadradas.

1.9 Equações Quínticas

Podemos começar resolvendo uma quíntica geral: $t^5 + at^4 + bt^3 + ct^2 + dt + e = 0$. A transformação de Tschirnhaus $y = t + \frac{a}{r}$ reduz a equação acima para

$$y^5 + py^3 + qy^2 + ry + s = 0.$$

Entretanto, aplicando todas as estratégias comuns de resoluções anteriores, obtemos um impasse.

Lagrange, em 1770-1771, analisou todas as estratégias, e mostrou que eles podem ser explicados usando princípios gerais sobre funções simétricas de raízes. Quando ele aplicou este método a quíntica, entretanto, ele descobriu que reduzia o problema a resolver uma equação do sexto grau. Uma fascinante descrição destas ideias, juntamente com um método para resolver quínticas, quando não solúveis por radicais, pode ser encontrado em anotações de George Neville Watson e reescritas por Bernatt, Spearman e Willians (2002).

Lagrange observou que todos os métodos para resolver equações polinomiais por radicais envolviam construção de funções racionais de raízes que assumiam um pequeno número de valores quando as raízes α_j eram permutadas. Proeminente através desta expressão:

$$\delta = \prod_{j<k}(\alpha_j - \alpha_k)$$

que traz somente dois valores, $\pm\delta$: mais para as permutações pares e menos para as permutações ímpares. Entretanto, $\Delta = \delta^2$ é uma função racional de coeficientes.

Lagrange trabalhou nestas expressões para cúbicas e quárticas, e percebeu um padrão. Por exemplo, se a polinomial cúbica tivesse as raízes $\alpha_1, \alpha_2, \alpha_3$ e ω como a raiz cúbica primitiva da unidade, então a expressão

$$\omega = (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3$$

tem exatamente dois valores distintos. De fato, permutações pares não a alteram, enquanto as ímpares a transformam em

$$v = (\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)^3.$$

Segue que $u + v$ e uv são fixadas pelas permutações de raízes e devem, ser expressas por funções racionais de coeficientes. Daí, u e v são soluções da equação quadrática, e podem ser expressas por raízes quadradas. Mas, o uso de raízes cúbicas expressa $\alpha_1+\omega\alpha_2+\omega^2\alpha_3 = \sqrt[3]{u}$ e $\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 = \sqrt[3]{v}$ por radicais. Por causa disso, nós também sabemos que $\alpha_1+\alpha_2+\alpha_3$ é menos o coeficiente do termo t^2, e temos três equações lineares independentes em raízes, o que é facilmente resolvido.

Algo muito similiar funciona para a quártica, com expressões como:

$$(\alpha_1 + i\alpha_2 + i^2\alpha_3 + i^3\alpha_4)^4.$$

Mas, quando tentamos a mesma ideia a quíntica, um obstáculo aparece. Suponha que as raízes da quíntica são $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Seja ξ uma raiz quinta primitiva da unidade. Segue de Lagrange, a consideração natural:

$$\omega = (\alpha_1 + \xi\alpha_2 + \xi^2\alpha_3 + \xi^3\alpha_4 + \xi^4\alpha_5)^5.$$

Há 120 permutações de cinco raízes, e elas transformam ω em 24 expressões distintas. Além disso, ω é uma raiz de uma polinomial de grau 24 - um passo bem distante.

A melhor maneira de resolver é usar a expressão derivada de Arthur Cayley em 1861, que é baseada em uma ideia de Robert Hayley de 1859. A expressão é

$$x = (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_5 + \alpha_5\alpha_1 - \alpha_1\alpha_3 - \alpha_2\alpha_4 - \alpha_3\alpha_5 - \alpha_4\alpha_1 - \alpha_5\alpha_2)^2$$

que mostra que x admite seis valores quando as variáveis são permutadas nas 120 maneiras.

Além disso, x é raiz de uma equação de ordem 6. Quando esta, possui uma raiz cujo quadrado é racional, a quíntica é solúvel por radicais. Explicando detalhadamente, a equação

$$t^5 + 15t + 12 = 0$$

tem a solução,

$$t = \sqrt[5]{\frac{-75 + 21\sqrt{10}}{125}} + \sqrt[5]{\frac{-75 - 21\sqrt{10}}{125}} + \sqrt[5]{\frac{225 + 72\sqrt{10}}{125}} + \sqrt[5]{\frac{225 - 72\sqrt{10}}{125}},$$

com expressões similares para as outras quatro raízes.

O método de Lagrange e outras impossibilidades levaram os matemáticos a pensarem na impossibilidade de solução da quíntica e não na procura de soluções.

Capítulo 2

O Teorema Fundamental da Álgebra

No início do século XIX, período em que Galois viveu, era natural pensar em investigações matemáticas sobre o corpo dos números complexos, uma vez que, os reais eram inadequados para determinados propósitos (por exemplo, não havia $\sqrt{-1}$ em $\mathbb{R}$). Além disso, a aritmética, a álgebra e análise dos complexos eram mais ricas, elegantes e mais completas do que a dos reais.

Uma das propriedades chaves de $\mathbb{C}$, o Teorema Fundamental da Álgebra, diz que qualquer equação polinomial com coeficientes em $\mathbb{C}$ tem uma solução em $\mathbb{C}$. Tal teorema é falso sobre $\mathbb{R}$, por exemplo, tome $t^2+1=0$, que não possui solução em $\mathbb{R}$ como já visto.

2.1 Equações Polinomiais

As equações lineares, quadráticas, cúbicas, quárticas e quínticas são exemplos de um tipo mais geral de equações: as polinomiais. Estas são da forma,

$$P(t)=0,$$

onde $P(t)$ é uma polinomial em t.

Polinomiais são importantes na matemática em diversos contextos, como também na literatura.

Estamos acostumados a pensar que uma polinomial é uma função que mapeia t com os valores da expressão conhecidas, tal que a primeira polinomial representa a função f tal que $f(t)=t^2-2t+6$. Como não é uma boa ideia pensar numa polinomial como uma função, devido a campos mais gerais, a definiremos em um contexto mais amplo.

Definiremos um polinômio sobre $\mathbb{C}$ com indeterminada t, como a expressão

$$r_0+r_1t+...+r_nt^n$$

onde $r_i \in \mathbb{C}$ com $0 \leq i \leq n, i \in \mathbb{N}$, e t indefinido. Para teóricos conjuntistas puristas (que não aceitam uma expressão logicamente falada como acima), podemos reorganizar a

expressão por meio de sequência $(r_0, r_1, ..., r_n)$. Que de algum modo, t é representado por $(0, 1, 0, ..., 0)$.

Os elementos $r_0, ..., r_n$ são os coeficientes do polinômio. De modo usual, os termos $0t^m$ podem ser omitidos ou escritos como 0, e $1t^m$ pode ser substituído por t^m.

Duas polinomiais são ditas iguais se, e só se, os correspondentes coeficientes são iguais, se potências de t não aparecem, estes devem ser entendidos como termos de coeficientes nulo.

Para definirmos a soma e o produto de duas polinomiais, escrevemos

$$\sum r_i t^i = r_0 + r_1 t + ... + r_n t^n \text{ com } i \geq 0 \text{ e } r_k = 0, \forall k \geq n.$$

Então, se

$$r = \sum r_i t^i \text{ e } s = \sum s_i t^i,$$

definimos

$$r + s = \sum (r_i + s_i) t^i$$

e

$$r \cdot s = \sum q_j t^j \text{ onde } q_j = \sum_{h+i=j} r_h s_i.$$

Com estas definições, verificamos que o conjunto $\mathbb{C}[t]$, dos polinômios sobre $\mathbb{C}$ com indeterminada t, é um anel. Na verdade, um domínio de integridade, mais ainda uma álgebra.

Pensemos um pouco na questão do inverso multiplicativo, uma vez que, é este axioma que impede $\mathbb{C}[t]$ de ser um corpo:

Seja $f \in \mathbb{C}[t] - \{0\}$ e suponha que existe $g \in \mathbb{C}[t] - \{0\}$ tal que $f(t) \cdot g(t) = 1$. Então $\partial(f(t) \cdot g(t)) = \partial f(t) + \partial g(t) = \partial 1 = 0 \Rightarrow \partial f(t) = \partial g(t) = 0$. Logo, $f(t)$ e $g(t)$ são polinômios constantes. Assim, os únicos polinômios invertíveis são os constantes dados por polinômios invertíveis de $\mathbb{C}$.

Podemos também definir polinômios em várias indeterminadas, $t_1, t_2, ..., t_n$ obtendo o anel de n variáveis polinomiais $\mathbb{C}[t_1, t_2, ..., t_n]$ de modo análogo.

Um elemento de $\mathbb{C}[t]$ é geralmente denotado por uma única letra, como f, exceto quando há ambiguidade, donde denotamos por $f(t)$ enfatizando t.

Definição 2.1.1. *Se f é um polinômio sobre $\mathbb{C}$ e $f \neq 0$, então o grau de f é a maior potência de t ocorrendo em f com coeficiente não nulo.*

De modo mais geral, se $f = \sum r_i t^i$ e $r_n \neq 0$ e $r_m = 0$ para $m > n$, então f tem grau n. Escrevemos ∂f para o grau de f. Para o caso $f = 0$, adotamos a convenção que $\partial 0 = -\infty$ (onde $-\infty < n, \forall n \in \mathbb{Z}; -\infty + n = -\infty; -\infty \cdot n = -\infty; (-\infty)^2 = -\infty$).

Proposição 2.1.2. *Se f, g são polinômios sobre $\mathbb{C}$, então*

$$\partial(f + g) \leq \max(\partial f, \partial g) \text{ e } \partial(f \cdot g) = \partial f + \partial g.$$

Justificativas informais da escolha se dão, no primeiro caso devido a possibilidade de cancelamento dos termos; e no segundo caso, resultado da propriedade da exponencial $x^n \cdot x^m = x^{n+m}$.

Proposição 2.1.3. *Dois polinômios* f, g *sobre* $\mathbb{C}$ *definem a mesma função se, e somente se, eles tem os mesmos coeficientes.*

Demonstração. Sejam $f(t) = g(t)$, com $f, g \in \mathbb{C}[t]$. Tomemos $h(t) = f(t) - g(t)$, como sabemos o que significa a igualdade, temos que $h(t) = a_{n-1}t^{n-1} + ... + a_0 = 0$, ou seja, todos seus coeficientes são nulos, e assim f e g definem a mesma função sobre g.

Como $h(t) = 0, \forall t \in \mathbb{C}$, podemos diferenciar n vezes para obtermos que $h^{(n)}(t) = 0, \forall t \in \mathbb{C}$. Em particular, $h^{(m)}(0) = 0, \forall n \in \mathbb{N}$. Mas, uma indução simples mostra que $h^{(n)}(0) = n' \cdot a_n$, então $a_n = 0, \forall n \in \mathbb{N}$. □

2.2 Teorema Fundamental da Álgebra

A partir de equações polinomiais insolúveis em um corpo, os estendemos até o $\mathbb{C}$. Agora fica a pergunta, por que paramos em $\mathbb{C}$? Por que não encontramos uma equação que não possui solução sobre $\mathbb{C}$, e estendemos o sistema numérico para encontrarmos tal solução?

A resposta é porque tal equação não existe, ao menos se nos limitarmos a polinomiais. Toda equação polinomial sobre $\mathbb{C}$ tem solução em $\mathbb{C}$. Tal proposição foi muito debatida por volta de 1700. Em 1702 (no papel), Leibniz mostrou que isto pode ser verdade, citando o exemplo:

$$x^4 + a^4 = (x + a\sqrt{\sqrt{-1}})(x - a\sqrt{\sqrt{-1}})(x + a\sqrt{-\sqrt{-1}})(x - a\sqrt{-\sqrt{-1}})$$

e Nicholas Bernoulli publicou a mesma fórmula em 1719. A resolução consiste em observar que $\sqrt{i} = \frac{1 \pm i}{2}$. Em 1742, Euler, sem provar, disse que todo polinômio real pode ser decomposto em lineares ou fatores de quadráticos com coeficientes reais; Bernoulli de outro modo, citou

$$x^4 - 4x^3 + 2x^2 + 4x + 4$$

com zeros/raízes $1 + \sqrt{2 + \sqrt{-3}}$, $1 - \sqrt{2 + \sqrt{-3}}$, $1 + \sqrt{2 - \sqrt{-3}}$ *e* $1 - \sqrt{2 - \sqrt{-3}}$.

Euler respondeu, em uma carta a seu amigo Christian Golbach, que os quatro fatores ocorrem como dois pares de complexos conjugados, e que o produto de tais pares de fatores é um número real ao quadrado. Ele mostrou isto como exemplo da proposta de Bernoulli. Golbach sugeriu que $x^4 + 72x - 20$ não concorda com a afirmação de Euler, e Euler pontuou um erro computacional adicionando que teria provado o teorema para polinômios de grau menor do que, ou igual a 6. Euler e Jean Le Rond d'Alembert deram provas completas para qualquer grau; Lagrange clamou pelo preenchimento dos buracos na prova de Euler em 1772, mas ele cometeu o erro de assumir que as raízes existiam, e

que usam as leis da álgebra para deduzir que deveriam ser números complexos, sem provar que as raízes - quaisquer que fossem - deveriam obedecer as leis da álgebra. A primeira prova genuína foi dada por Gauss na sua tese de doutorado em 1799. Depois, Gauss deu outras 3 provas, todas baseadas em ideias diferentes.

Teorema 2.2.1 (Teorema Fundamental da Álgebra)**.** *Seja $P(t)$ um polinômio sobre $\mathbb{C}$, com $\partial P \geq 1$. Então existe ao menos um $z \in \mathbb{C}$ tal que $P(z) = 0$.*

Tal número z é chamado de raiz da equação $P(t) = 0$, ou um zero do polinômio P. Por exemplo, i é uma raiz da equação $t^2+1 = 0$ e um zero de t^2+1. Equações polinomiais, podem ter mais de uma raiz, veja que $t^2 + 1 = 0$ tem ao menos outra raiz, $-i$.

Nesta seção provaremos o Teorema Fundamental da Álgebra usando algumas ideias relativamente simples da análise real e da topologia. As ideias por trás da prova aqui dada, remetem a Gauss, quem desmascarou a geometria convertendo em fórmulas trigonométricas complicadas. Por razões técnicas, usaremos diferentes táticas das empregadas na versão usual da prova. A ideia principal é considerar o número de "contornos" de uma curva, e começamos descrevendo isto.

Seja S o círculo unitário, parametrizado pelo arco de comprimento θ. Podemos pensar em θ de duas maneiras equivalentes. Se $\theta \in \mathbb{R}$, identificamos $\theta + 2k\pi$ com θ, qualquer inteiro k que efetivamente reduz θ a $[0, 2\pi)$; ou pensemos em θ como um elemento do conjunto quociente $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$.

Um laço em $\mathbb{R}^2$ é uma função contínua $\gamma : S \to \mathbb{R}^2$, e sua imagem $\gamma(S)$ é uma curva fechada no plano $\mathbb{R}^2$.

Suponha que $\gamma(S)$ não contenha a origem $(0, 0) \in \mathbb{R}^2$, isto é, $\gamma(\theta) \neq (0, 0)$ qualquer que seja $\theta \in S$. Então qualquer ponto $(x, y) \in \gamma(S)$ está de um único raio determinado a partir da origem, isto é, uma semirreta estendida da origem ao infinito. O argumento ϕ de (x, y) é o ângulo entre o eixo positivo x e este raio, medido no sentido anti-horário. O argumento pode ser considerado um elemento de $\mathbb{R}$, e é único, exceto pela adição de um múltiplo inteiro de 2π.

Usando θ para parametrizar S, com $\gamma(\theta) = (x_\theta, y_\theta)$. Escolha um valor ϕ_θ de argumento de (x_θ, y_θ). É plausível que exista uma única escolha de argumento ϕ_θ para o ponto (x_θ, y_θ) tal que,

1. ϕ_θ é igual a ϕ_0 quando $\theta = 0$;

2. ϕ_θ varia continuamente com θ.

Definição 2.2.2. *Seja γ um laço em $\mathbb{R}^2$ não passando pela origem. Seja ϕ_θ uma escolha contínua de argumento para γ. Então, o número de sinuosidades de γ ao redor da origem é*

$$\omega(\gamma) = \frac{\phi_{2\pi} - \phi_0}{2\pi}.$$

Este número independe da escolha inicial ϕ_0, pois começando com $\phi_0 + 2k\pi$ somos forçados a substituir ϕ_0 por $\phi_0 + 2k\pi$, e o extra $2k\pi$ é cancelado.

Exemplos 2.2.3.

1. *Suponha que γ é constante, digamos que $\gamma(\theta) = (x_0, y_0) \neq (0,0)$ para todo θ. Então a escolha de ϕ_0 funciona para todo θ, não só para o $\theta = 0$; em particular, sendo constante, este varia continuamente com θ. Neste caso, o número de sinuosidades é*
$$\omega = \frac{\phi_0 - \phi_0}{2\pi} = 0.$$

2. *Suponha que $\gamma(\theta) = e^{ni\theta}$ onde $n \in \mathbb{Z}$. Agora, podemos escolher $\phi_\theta = n\theta$. Portanto,*
$$\omega(\gamma) = \frac{\phi_{2\pi} - \phi_0}{2\pi} = \frac{2\pi n - 0}{2\pi} = n.$$
O número de sinuosidades é uma propriedade importante: ele permanece constante se γ é continuamente deformado, sempre evitando passar pela origem (isto é, invariante por homotopias não envolvendo a origem). Considere a função contínua:
$$\gamma : S \times [0,1] \to \mathbb{R}^2 \setminus \{(0,0)\}.$$
Então, γ define uma família continuamente variante de laços γ_ϵ onde $\gamma_\epsilon(\theta) = \gamma(\theta, \epsilon)$.

Teorema 2.2.4. *Com a notação acima, $\omega(\gamma_\epsilon) = \omega(\gamma_0)$ para todo $\epsilon \in [0,1]$. Em particular,*
$$\omega(\gamma_1) = \omega(\gamma_0). \tag{2.1}$$

Demonstração. Faremos um esboço da demonstração. Para tal, é necessário o uso de alguns elementos topológicos.

Os números de sinuosidades estão bem definidos quando nenhum γ_ϵ encontra a origem. O valor de $\omega(\gamma_\epsilon)$ varia continuamente com ϵ. Por ser um número inteiro, deve ser, portanto, constante. Então, $\omega(\gamma_\epsilon) = \omega(\gamma_0)$ para todo $\epsilon \in [0,1]$. Colocando $\epsilon = 1$, temos provado (2.1).

Se algum γ_{ϵ_0} passar pela origem, então o número de sinuosidades pode mudar. □

Teorema Fundamental da Álgebra. Seja $P(t)$ um polinômio não constante em $\mathbb{C}[t]$. Sem perda de generalidade, podemos assumir que o coeficiente da maior potência de t em $P(t)$ é 1. Assumamos que $P(t)$ não possua raízes em $\mathbb{C}$ e obteremos uma contradição.

Seja $\partial P = n \geq 1$.

Para cada $\epsilon \in [0,1)$ definimos um laço γ_ϵ por:
$$\gamma_\epsilon(\theta) = \frac{P(r(\epsilon)e^{i\theta})}{r(\epsilon)^n + 1},$$

onde,

$$r(\epsilon) = \frac{\epsilon}{1-\epsilon},$$

quando $\epsilon = 1$, definimos,

$$\gamma_1(\theta) = e^{ni\theta}.$$

Agora, γ_ϵ é definida para todo $\epsilon \in [0,1]$.

Afirmamos que $\gamma : S \times [0,1] \to \mathbb{R}^2$ é contínua, onde $\gamma(\theta,\epsilon) = \gamma_\epsilon(\theta)$. Temos isto nitidamente (quociente de contínuas), exceto quando $\epsilon = 1$. Como $\epsilon \to 1$, a função $r(\epsilon)$ tende a $+\infty$, então

$$\lim_{\epsilon\to 1} \gamma_\epsilon(\theta) = \lim_{r(\epsilon)\to+\infty} \frac{P(r(\epsilon)e^{i\theta})}{r(\epsilon)^n + 1}.$$

Suponha que

$$P(t) = t^n + a_{n-1}t^{n-1} + ... + a_0$$

Então,

$$\frac{P(r(\epsilon)e^{i\theta}}{r(\epsilon)^n+1} = \frac{r(\epsilon)^n}{r(\epsilon)^n+1}e^{ni\theta} + \frac{a_{n-1}r(\epsilon)^{n-1}e^{(n-1)i\theta} + ... + a_0}{r(\epsilon)^n+1}.$$

O segundo termo do lado direito da equação tende a 0 quando $r(\epsilon) \to +\infty$, e o primeiro, tende a $e^{ni\theta}$. Portanto, para cada θ,

$$\lim_{\epsilon\to 1} \gamma_\epsilon(\theta) = \gamma_1(\theta).$$

Do fato de podermos tomar θ no intervalo fechado $[0, 2\pi]$, a convergência é uniforme em θ. E assim, γ é contínua.

Ao assumirmos que $P(z)$ é não nulo para todo $z \in \mathbb{C}$, implicamos que a curva definida por γ_ϵ não encontra/passa pela origem para qualquer $\epsilon \in [0,1]$. Além do mais, $\gamma_\epsilon(\theta) = 0$ se, e somente se, $P(r(\epsilon)e^{i\theta}) = 0$. Pelo Teorema anterior $\omega(\gamma_0) = \omega(\gamma_1)$. Entretanto, os exemplos mostram que $\omega(\gamma_0) = 0$, onde $\omega(\gamma_1) = n \geq 1$. O que é uma contradição. Portanto, a suposição de que $P(t)$ não tem raízes em $\mathbb{C}$ é falsa, como queríamos demonstrar. □

2.3 Implicações

O Teorema Fundamental da Álgebra tem algumas implicações uteis. Antes de provarmos a mais básica destas, provaremos primeiro o Teorema do Resto.

Teorema 2.3.1 (Teorema do Resto)**.** *: Seja $p(t) \in \mathbb{C}[t]$ com $\partial p \geq 1$, e seja $\alpha \in \mathbb{C}$.*

1. *Existe $q(t) \in \mathbb{C}[t]$ e $r \in \mathbb{C}$ tal que $p(t) = (t-\alpha)q(t) + r$;*

2. *A constante r satisfaz, $r = p(\alpha)$.*

Demonstração. Seja $y = t - \alpha$ tal que $t = y + \alpha$. Escrevemos $p(t) = p_n t^n + ... + p_0$ onde $p_n \neq 0$ e $n \geq 1$. Então,

$$p(t) = p_n(y + \alpha)^n + ... + p_0.$$

Expanda as potências de $(y + \alpha)$ pelo teorema binomial, e reagrupe os teoremas de modo a obter:

$$\begin{aligned} p(t) &= a_n y^n + ... + a_1 y + a_0,\ a_j \in \mathbb{C} \\ &= y(a_n y^{n-1} + ... + a_1) + a_0 \\ &= (t - \alpha)q(t) + r \end{aligned}$$

onde,

$$q(t) = a_n(t - \alpha)^n + ... + a_1(t - \alpha) + a_0$$

e

$$r = a_0.$$

Agora substituindo $t = \alpha$ em $p(t) = (t - \alpha)q(t) + r$, teremos

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

□

Corolário 2.3.2. *O número complexo α é raiz de $p(t)$ se, e somente se, $(t - \alpha)$ divide $p(t)$ em $\mathbb{C}[t]$.*

Proposição 2.3.3. *Seja $p(t) \in \mathbb{C}[t]$ com $\partial p = n \geq 1$. Então existe $\alpha_1, ..., \alpha_n \in \mathbb{C}$, e $0 \neq k \in \mathbb{C}$, tal que,*

$$p(t) = k(t - \alpha_1) \cdot ... \cdot (t - \alpha_n). \tag{2.2}$$

Demonstração. Usemos indução sobre n. Para o caso $n = 1$ é imediato. Se $n > 1$, sabemos do Teorema Fundamental da Álgebra, que $p(t)$ tem ao menos uma raiz em $\mathbb{C}$; chamemos tal de α_n. Pelo Teorema do Resto, existe $q(t) \in \mathbb{C}[t]$ tal que

$$p(t) = (t - \alpha_n)q(t). \tag{2.3}$$

(Notemos que $r = p(\alpha_n) = 0$). Então, $\partial q = n - 1$, assim por indução,

$$q(t) = k(t - \alpha_1) \cdot ... \cdot (t - \alpha_{n-1}). \tag{2.4}$$

Para alguns números complexos $k, \alpha_1, ..., \alpha_{n-1}$. Substituamos (2.4) em (2.3), e o passo de indução está completo.

Segue imediatamente que os complexos α_j são os únicos zeros de $p(t)$. □

Os zeros α_j não precisam ser distintos. Agrupando aqueles que são iguais, reescrevemos

(2.2) como,

$$p(t) = k(t - \beta_1)^{m_1} \cdot ... \cdot (t - \beta_l)^{m_l}$$

onde β_j são distintos, e m_j são inteiros maiores do que, ou iguais a 1, e ainda, $m_1+...+m_l = n$. Chamamos m_j de multiplicidade do zero β_j de $p(t)$.

Em particular, provamos que todo polinômio complexo de grau n tem precisamente n raízes complexas, contadas a partir da multiplicidade.

Capítulo 3

Fatoração de Polinômios

Não há só uma álgebra de polinômios, há uma aritmética. Isto é, há noções análogas aos inteiros, como divisibilidade, primos, fatoração prima, etc. Estas noções são essenciais para um entendimento de equações polinomiais, que desenvolveremos neste capítulo.

Se f é um produto gh de polinômios de graus menores, então a solução de $f(t) = 0$ é precisamente aquelas em que $g(t) = 0$ e $h(t) = 0$. Por exemplo,

$$t^3 - 6t^2 + 11t - 6 = 0$$

pode ser fatorada em $(t-1)(t-2)(t-3)$, logo, $t = 1, 2, 3$ são as raízes.

Todo polinômio sobre um subcorpo de $\mathbb{C}$ pode ser expresso como um produto de polinômios irredutíveis sobre o mesmo subcorpo, de modo único. Relataremos zeros de polinômios por meio da teoria de fatoração.

Ao longo deste capítulo, assumiremos os polinômios em $K[t]$, onde K é um subcorpo dos números complexos, ou em $R[t]$, onde R é um subanel dos números complexos. Alguns teoremas são válidos sobre R, enquanto outros somente sobre K; precisaremos dos dois tipos.

3.1 O Algoritmo Euclidiano

Quando trabalhamos com teoria dos números, um dos conceitos chaves é divisibilidade: um inteiro a é divisível por um inteiro b se existe um inteiro c tal que $a = bc$.

Muitos resultados importantes na teoria de fatoração de polinômios derivam da observação de que um polinômio pode sempre ser dividido por outro advindo do fato de ter termo restante é permitido. Esta é uma generalização do Teorema do Resto, no qual f é assumida linear.

Proposição 3.1.1 (O Algoritmo da Divisão). *Sejam f e g polinômios sobre K (um corpo), e suponhamos que f é não nulo. Então existem únicos polinômios q e r sobre K, tal que $g = fq + r$ e r tem grau estritamente menor do que f.*

Demonstração. Usaremos indução do segundo tipo no grau de g. Se $\partial g = -\infty$, então $g \equiv 0$ e tomaremos $q = r \equiv 0$ resolvendo o problema. Se $\partial g = 0$, então $g = k$, para algum $k \in K$. Se também, $\partial f = 0$, então f é um elemento de K, e podemos tomar $q = \frac{k}{f}$ e $r \equiv 0$. Por outro lado, $\partial f > 0$, teremos $q \equiv 0$ e $r = g$. Donde começaremos nossa indução.

Suponhamos que o resultado valha para todos os polinômios de grau $< n$, e seja $\partial g = n > 0$. Se $\partial f > \partial g$, então teremos $q \equiv 0$ e $r = g$. Por outro lado,

$$f = a_m t^m + ... + a_0 \text{ e } g = b_n t^n + ... + b_0$$

onde $a_m \neq 0$, $b_n \neq 0$ e $m \leq n$. Seja,

$$g_1 = b_n {a_m}^{-1} t^{n-m} f - g.$$

Temos que $\partial g_1 < \partial g$. Por hipótese de indução, existem polinômios q_1 e r_1 em K tal que $g_1 = fq_1 + r_1$ e $\partial r_1 < \partial f$. Sejam

$$q = b_n {a_m}^{-1} t^{n-m} - q_1 \text{ e } r_1 = r.$$

Então,

$$g = fq + r = b_n {a_m}^{-1} t^{n-m} f - q_1 f - r_1 = g + g_1 - g_1 = g$$

Então $g = fq + r$, e claramente $\partial r < \partial f$.

Finalmente, provaremos a unicidade. Suponhamos que,

$$g = fq_1 + r_1 = fq_2 + r_2$$

onde $\partial r_1, \partial r_2 < \partial f$.

Então, $f(q_1 - q_2) = r_2 - r_1$. Por meio da definição de graus, o polinômio a esquerda tem grau maior do que o da direita, exceto que ambos são zeros. Como $f \not\equiv 0$, devemos ter $q_1 = q_2$ e $r_1 = r_2$. Portanto, q e r são únicos.

Com a notação acima, q é chamado de quociente, r, de resto da divisão de g por f. O processo indutivo empregado para encontrarmos q e r é chamado de Algoritmo da Divisão. □

Exemplo 3.1.2. *Divida* $g(t) = t^4 - 7t^3 + 5t^2 + 4$ *por* $f(t) = t^2 + 3$ *e encontre o quociente*

e o resto.

$$\begin{array}{rl} t^4 - 7t^3 + 5t^2 + 4 & \mid \underline{t^2 + 3} \\ \underline{-t^4 - 3t^2} & t^2 - 7t + 2 = q(t) \\ -7t^3 + 2t^2 + 4 & \\ \underline{7t^3 + 21t} & \\ 2t^2 + 21t + 4 & \\ \underline{-2t^2 - 6} & \\ r(t) = 21t - 2. & \end{array}$$

Observe que

$$t^2(t^2 + 3) = t^4 + 3t^2$$

tem o mesmo coeficiente líder que tem a g. Então,

$$g - t^2(t^2 + 3) = -7t^3 + 2t^2 + 4,$$

que tem o mesmo coeficiente líder do que

$$-7t(t^2 + 3) = -7t^3 - 21t.$$

Assim,

$$g - t^2(t^2 + 3) + 7t(t^2 + 3) = 2t^2 + 21t + 4,$$

que possui o mesmo coeficiente líder que

$$2(t^2 + 3) = 2t^2 + 6.$$

Portanto,

$$g - t^2(t^2 + 3) + 7t(t^2 + 3) - 2(t^2 + 3) = 21t - 2.$$

Então,

$$g = (t^2 + 3)(t^2 - 7t + 12) + (21t - 2)$$

e o quociente $q(t) = t^2 - 7t + 2$, enquanto que o resto $r(t) = 21t - 2$.

Definição 3.1.3. *Sejam f e g polinômios sobre K. Dizemos que f divide g (ou f é um fator de g, ou g é múltiplo de f), se existe algum polinômio h sobre K tal que $g = fh$. A notação $f|g$ significará f divide g, enquanto que $f \nmid g$, f não divide g.*

Definição 3.1.4. *Um polinômio d sobre K é um <u>maior fator comum</u> (mdc) dos polinômios f e g sobre K se $d|f$ e $d|g$ e além disso, sempre que $e|f$ e $e|g$, temos $e|d$.*

Maior fator comum não precisa ser único. O lema seguinte mostrará que eles são únicos exceto por fatores constantes.

Lema 3.1.5. *Se d é um maior fator comum dos polinômios f e g sobre K, e se $0 \neq k \in K$ então kd também é um fator comum para f e g.*

Se d e e são dois maiores fatores comuns para f e g, então existe um elemento não nulo $k \in K$, tal que, $e = kd$.

Demonstração. Como $d|f$, então $f = m \cdot d$ para algum $m \in K$; também $d|g$, ou seja, para algum $l \in K$, $g = l \cdot d$. Se tomarmos $\frac{m}{k}$ e $\frac{l}{k}$ vemos claramente que $kd|f$ e $kd|g$. Se $e|f$ e $e|g$, então $e|d$, logo $e|kd$. Assim, kd é o maior fator comum. Se d e e são maiores fatores comuns, então pela definição $e|d$ e $d|e$. Portanto, $e = k \cdot d$ para algum polinômio em K. Por causa que $e|d$, o grau de e é menor do que ou igual ao grau de d, então k deve ter grau ≤ 0. Assim, k é uma constante, e pertence a K. Como $0 \neq e = k \cdot e$, devemos ter $k \neq 0$. □

Algoritmo 3.1.6 (Algoritmo Euclidiano)**.**

***Entrada**: Dois polinômios f e g sobre K, ambos não nulos.*
***Saída**: Um polinômio m que é o maior fator comum entre f e g (provado no Teorema 3.1.7 abaixo).*
***Descrição**: Por conveniência de notação, seja $f = r_{-1}$ e $g = r_0$. Use o Algoritmo da Divisão para encontrar sucessivamente polinômios q_j e r_i tais que:*

$$\begin{aligned} r_{-1} &= q_1 r_0 + r_1 & \partial r_1 < \partial r_0 \\ r_0 &= q_2 r_1 + r_2 & \partial r_2 < \partial r_1 \\ r_1 &= q_3 r_2 + r_3 & \partial r_3 < \partial r_2 \\ &\ldots & \ldots \\ r_i &= q_{i+2} r_{i+1} + r_{i+2} & \partial r_{i+2} < \partial r_{i+1}. \end{aligned}$$

Por causa dos graus de r_i formarem uma sequência de inteiros não negativos estritamente decrescente, após um número finito de divisões certamente obteremos um resto igual a zero, digamos $r_{s+2} = 0$ e, nesse momento, o processo para. Sendo assim, a última equação nesta lista (cujo resto não é zero) seria

$$r_s = q_{s+2} r_s + r_{s+1}. \tag{3.1}$$

Podemos tomar $m = r_{s+1}$.

Teorema 3.1.7. *Com a notação acima, $m = r_{s+1}$ é um maior fator comum para f e g.*

Demonstração. Primeiro, mostremos que r_{s+1} divide f e g. Usaremos indução decrescente para mostrar que $r_{s+1}|r_i$ para todo i. Claramente, $r_{s+1}|r_{s+1}$. Pela Equação (3.1) temos que $r_{s+1}|r_s$. Já (3.1.6) implica que se, $r_{s+1}|r_{i+2}$ e $r_{s+1}|r_{i+1}$ então, $r_{s+1}|r_i$. Como $r_{s+1}|r_i$ para todo i; em particular, $r_{s+1}|r_0 = g$ e $r_{s+1}|r_{-1} = f$.
Agora suponhamos que $e|f$ e $e|g$. Por (3.1.6) e induções, $e|r_i$ para todo i. Em particular, $e|r_{s+1}$. Portanto, r_{s+1} é um maior fator comum de f e g, como afirmado. □

Exemplo 3.1.8. *Seja* $f(t) = t^4+3t^3+2t^2+2t+1$, *e* $g(t) = t^2-1$ *sobre* $\mathbb{Q}$. *Calcularemos o maior fator comum como segue:*

$$\begin{aligned} t^4+2t^3+2t^2+2t+1 &= (t^2+2t+3)(t^2-1)+4t+4 \\ t^2-1 &= (4t+4)\left(\frac{1}{4}t-\frac{1}{4}\right). \end{aligned}$$

Percebemos que $4t+4$ *é um maior fator comum. Então qualquer múltiplo racional deste também o é. Em particular,* $t+1$.

Teorema 3.1.9. *Sejam* f *e* g *polinômios não nulos sobre* K, *e seja* d *um maior fator comum de* f *e* g. *Então existem polinômios* a *e* b *sobre* K, *tais que*

$$d = af + bg.$$

Demonstração. Sabemos que o maior fator comum é único a menos de constantes, devemos assumir que $d = rs+1$, onde (3.1.6) e (3.1) valem. Suponhamos por hipótese de indução que existam polinômios a_i e b_i tais que,

$$d = a_i r + b_i r_i + 1.$$

Temos claramente que isto é verdade quando $i = s+1$, donde devemos tomar $a_i = 1$, $b_i = 0$. Por (3.1.6),

$$r_{i+1} = r_{i-1} - q_{i+1}r_i.$$

Como, por indução,

$$d = a_i r_i + b_i(r_{i-1} - q_{i+1}r_1),$$

colocando

$$a_{i-1} = b_i \quad e \quad b_{i-1} = a_i - b_i q_i + 1$$

teremos

$$d = a_{i-1}r_{i-1} + b_{i-1}r_i,$$

e da indução decrescente,

$$d = a_{-1}r_{-1} + b_{-1}r_0 = af + bg,$$

com $a = a_{-1},\ b = b_{-1}$. Completando a demonstração. □

3.2 Irredutibilidade

Em particular, nós provamos que todo polinômio sobre um subanel de $\mathbb{C}$ pode ser expresso como um produto de polinômios irredutíveis essencialmente de um modo único.

Associaremos na definição seguinte polinômios a números inteiros primos.

Definição 3.2.1. *Um polinômio sobre um subanel $\mathcal{R}$ de $\mathbb{C}$ é redutível se é um produto de dois polinômios sobre $\mathcal{R}$ de graus menores. Caso contrário, dizemos que é irredutível.*

Exemplos 3.2.2. *1. Todos os polinômios de graus 0 e 1 são irredutíveis, pois certamente não podem ser expressos como um produto de polinômios de graus menores.*

2. O polinômio $t^2 - 2$ é irredutível sobre $\mathbb{Q}$. Pois, caso não o fosse, teríamos

$$t^2 - 2 = (at + b)(ct + d),$$

com $a, b, c, d \in \mathbb{Q}$. Dividindo se necessário, podemos assumir $a = c = 1$, ou seja, polinômios mônicos. Então,

$$\begin{aligned} t^2 - 2 &= (at + b)(ct + d) \\ &= (t + b)(t + d) \\ \Rightarrow t^2 - 2 &= t^2 + dt + bt + bd \\ \Rightarrow t^2 - 2 &= t^2 + (b + d)t + bd. \end{aligned}$$

E assim, $b+d = 0$ e $bd = -2$. Isolando d na primeira equação, conseguimos $d = -b$. Donde substituindo na segunda, ficamos com $b^2 = 2$. Mas, não há número racional tal que sua raiz quadrada seja 2.

3. O mesmo polinômio, $t^2 - 2$ é redutível sobre $\mathbb{R}$, já que,

$$t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2}).$$

Mostrando que um polinômio irredutível pode se tornar redutível ao considerarmos um subcorpo maior de $\mathbb{C}$. Guardemos tal ideia!!!

4. O polinômio $6t + 3$ é irredutível em $\mathbb{Z}[t]$. Além disso, tem como fatores,

$$6t + 3 = 3(2t + 1),$$

onde $2t + 1$ tem o mesmo grau do que $6t + 3$ não contando como fatoração para redutibilidade.

Teorema 3.2.3. *Qualquer polinômio não nulo sobre o subanel $\mathcal{R}$ de $\mathbb{C}$ é um produto de polinômios irredutíveis sobre $\mathcal{R}$.*

Demonstração. Seja g um polinômio não nulo sobre $\mathcal{R}$. Procederemos por indução sobre o grau de g. Se $\partial g = 0$ ou $\partial g = 1$, então ele é automaticamente irredutível, e não há o que fazermos. Suponhamos então $\partial g > 1$, então ou g é irredutível, ou $g = hk$, com $h, k \in \mathcal{R}$

e $\partial h, \partial k < \partial g$. Continuamos o procedimento analisando h e k, estes são produtos de polinômios irredutíveis por hipótese de indução, portanto g também o é. Continuamos a indução de modo a concluirmos a demonstração do teorema. □

Exemplo 3.2.4. *Podemos usar o Teorema 3.2.3 para provarmos a irredutibilidade em alguns casos, especialmente para polinômios cúbicos sobre $\mathbb{Z}$. Por exemplo, seja $\mathcal{R} = \mathbb{Z}$. O polinômio*

$$f(t) = t^3 - 5t + 1$$

é irredutível em $\mathcal{R}$. Caso não o fosse, deveria existir um fator linear do tipo $t - \alpha$ em $\mathbb{Z}$, e então, $\alpha \in \mathbb{Z}$ e $f(\alpha) = 0$. Além do mais, existem $\beta, \gamma \in \mathbb{Z}$ tais que

$$\begin{aligned} f(t) &= (t-\alpha)(t^2+\beta t+\gamma) \\ &= t^3 + (\beta-\alpha)t^2 + (\gamma-\alpha\beta)t - \alpha\gamma \end{aligned}$$

então, em particular, $\alpha\gamma = -1$. Portanto, $\alpha = \pm 1$. Mas, $f(1) = -3 \neq 0$ e $f(-1) = 5 \neq 0$. E assim, temos que nenhum fator existe.

Polinômios irredutíveis são análogos a números primos em $\mathbb{Z}$. A importância dos números primos em $\mathbb{Z}$ não reside apenas na possibilidade de fatoração de qualquer inteiro em primos, mas também na unicidade (a menos da ordem) dos fatores primos. Unicidade da fatoração dos polinômios não é algo óbvio. Em certos casos, é possível expressar todo elemento como produto de elementos irredutíveis, sem que esta expressão seja única. Restringiremos nossa atenção sobre um subcorpo K de $\mathbb{C}$ (numa tentativa de resolver o problema da unicidade).

Por conveniência, faremos o seguinte:

Definição 3.2.5. *Se f e g são polinômios sobre um subcorpo K de $\mathbb{C}$ com maior fator comum igual a 1, diremos que f e g são primos entre si.*

Lema 3.2.6. *Seja K um subcorpo de $\mathbb{C}$, f um polinômio irredutível sobre K; e g, h polinômios sobre K. Se f divide gh, então ou f divide g, ou f divide h.*

Demonstração. Suponhamos que $f \nmid g$. Afirmamos que f e g são primos entre si. Se d é um maior fator comum para f e g, então como f é irredutível e $d|f$, ou $d = kf$ para algum $k \in K$, ou $d = k$, com $k \in K$. No primeiro caso, conseguimos que $f|g$, o que contraria a hipótese. No segundo caso, 1 também é um maior fator comum para f e g, donde temos que estes são primos entre si (como já havíamos afirmado). Usando o Teorema 3.1.9, existem polinômios a e b sobre K tais que,

$$1 = af + bg$$

E então,

$$h = haf + hbg.$$

Agora, $f|haf$, e $f|hbg$ já que $f|gh$. Portanto, $f|h$, completando assim a demonstração. □

Teorema 3.2.7. *Dado qualquer subcorpo K de $\mathbb{C}$, a fatoração de polinômios sobre K em polinômios irredutíveis é única, exceto por fatores constantes e a ordem em que estes fatores são escritos.*

Demonstração. Suponha que $f = f_1 \cdot ... \cdot f_r = g_1 \cdot ... \cdot g_s$, em que f é um polinômio sobre K e $f_1, ..., f_r, g_1, ..., g_s$ são polinômios irredutíveis sobre K. Se todos os f_i são constantes, então $f \in K$, e todos os g_j também são constantes. Por outro lado, assumamos que nenhum f_i é constante (basta dividirmos pelos que o são). Então, $f_1|g_1 \cdot ... \cdot g_s$. Por indução baseada no Lema anterior, $f_1|g_j$ para algum j. Escolhamos por facilidade, $j = 1$, então $f_1|g_1$. Como f_1 e g_1 são irredutíveis e f_1 não é constante, devemos ter $f_1 = k_1 g_1$ para alguma constante $k_1 \in K$. Analogamente, $f_2 = k_2 g_2, ..., f_r = k_r g_r$, com $k_2, ..., k_r$ constantes em K. Os demais g_l com $l > r$ devem ser constantes, ou o grau do lado direito da equação seria muito mais alto do que o esquerdo. Assim, temos o teorema demonstrado. □

3.3 Lema de Gauss

Em geral é difícil de decidir - sem usar álgebra computacional, de nenhum modo - se um polinômio dado é irredutível. Por exemplo, tome

$$t^{16} + t^{15} + t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$$

Este exemplo será retomado no final do trabalho, onde a questão de irredutibilidade(ou não) será imprescindível.

Testar irredutibilidade tentando todas as possibilidades de fatores é geralmente inútil. Além do mais, em um primeiro momento, há infinitamente muitos fatores potenciais para se tentar, com um sutil corte, as possibilidades podem ser reduzidas a um número finito, geralmente grande.

O método pode ser aplicados para polinômios em $\mathbb{Q}$, mesmo este sendo realmente impraticável.

Logo, devemos inventar algo mais prático. Nas próximas duas seções, descreveremos dois deles: Critério de Eisenstein e Redução Módulo p, com p primo. Ambos os métodos, aplicam-se num primeiro momento sobre $\mathbb{Z}$. Entretanto, devido a Gauss, sabemos que irredutibilidade sobre $\mathbb{Z}$ é equivalente a irredutibilidade sobre $\mathbb{Q}$.

Lema 3.3.1 (Lema de Gauss)**.** *Seja f um polinômio sobre $\mathbb{Z}$ que é irredutível sobre $\mathbb{Z}$. Então f, considerado como um polinômio sobre $\mathbb{Q}$, é também irredutível sobre $\mathbb{Q}$.*

Demonstração. Quando estendemos um subanel de coeficientes em $\mathbb{Z}$ a $\mathbb{Q}$, há novos polinômios, que talvez, possam ser fatores de f. Mostraremos que, de fato, isto não é possível. Então suponhamos que f é irredutível sobre $\mathbb{Z}$, mas redutível sobre $\mathbb{Q}$, isto é,

$f = gh$, com g, h polinômios sobre $\mathbb{Q}$ de graus menores do que o de f. Multipliquemos a equação pelo produto dos denominadores dos coeficientes de g e h, donde ficamos com $nf = f'g'$, em que $n \in \mathbb{Z}$, n é igual ao produto dos denominadores, e g', h' são polinômios em $\mathbb{Z}$. Mostraremos agora que, podemos cancelar os fatores primos de n um por um, sem sairmos de $\mathbb{Z}[t]$.

Suponhamos que p é um fator primo de n. Afirmamos que

$$g' = g_0 + g_1 t + ... + g_r t^r \quad e \quad h' = h_o + h_1 t + ... + h_s t^s$$

então, p divide todos os coeficientes g_i, ou p divide todos os coeficientes de h_j. Caso contrário, deveríamos ter menores valores para i e j tais que $p \nmid g_i$ e $p \nmid h_j$. Entretanto, p divide todos os coeficientes t^{i+j} em $g'h'$, que são

$$h_0 g_{i+j} + h_1 g_{i+j-1} + ... + h_j g_i + ... + h_{i+j} g_0$$

e pela escolha de i e j, o primo p divide todos os termos desta expressão, exceto talvez $h_j g_i$. Ora, p divide toda a expressão, então $p | h_j g_i$. Entretanto, $p \nmid h_j$ e $p \nmid g_i$, uma contradição. O que acaba por provar nossa afirmação.

Sem perda de generalidade, devemos assumir que p divide todo o coeficiente de g_i. Daí, $g' = pg''$, onde g'' é um polinômio sobre $\mathbb{Z}$ do mesmo grau que g'(ou g). Seja $n = pn_1$. Então $pn_1 f = pg''h'$, donde, $n_1 f = g''h'$. Procedendo deste modo, podemos remover todos os fatores primos de n chegando na equação, $f = \overline{g}\overline{h}$, com $\overline{g}, \overline{h}$ polinômios sobre $\mathbb{Z}$. Ou seja, são múltiplos racionais do original g e h, então $\partial\overline{g} = \partial g$ e $\partial\overline{h} = \partial h$. O que contradiz a irredutibilidade de f sobre $\mathbb{Z}$, o que leva a termos provado o lema. □

Corolário 3.3.2. *Seja $f \in \mathbb{Z}[t]$ e suponha que sobre $\mathbb{Q}[t]$ há uma fatoração em irredutíveis*

$$f = g_1 \cdot ... \cdot g_s.$$

Então existe $a_i \in \mathbb{Q}$ tal que $a_i, g_i \in \mathbb{Z}[t]$ e $a_1 \cdot ... \cdot a_s = 1$. Além do mais,

$$f(a_1 g_1) \cdot ... \cdot (a_s g_s),$$

que é uma fatoração de f em irredutíveis em $\mathbb{Z}[t]$.

Demonstração. Fazendo a fatoração de f em irredutíveis sobre $\mathbb{Z}[t]$, obtemos $f = h_1 \cdot ... \cdot h_r$. Pelo Lema de Gauss, cada h_j é irredutível sobre $\mathbb{Q}$. Assim, pela unicidade da fatoração em $\mathbb{Q}[t]$, devemos ter $r = s$ e $h_j = a_j g_j$ para $a_j \in \mathbb{Q}$. E, claramente, $a_1 \cdot ... \cdot a_s = 1$. Logo, o corolário está devidamente provado. □

3.4 Critério de Eisenstein

Ferdinand Gotthold Eisenstein era um aluno de Gauss, e seu tutor. Vemos que isto influenciou trabalhos, podemos aplicar o Lema do tutor no critério descoberto pelo aluno.

Teorema 3.4.1 (Critério de Eisenstein). *Seja* $f(t) = a_0 + a_1t + a_2t^2 + ... + a_nt^n$ *um polinômio sobre* $\mathbb{Z}$. *Suponha que exista um primo* q *tal que,*

1. $q \nmid a_n$;
2. $q|a_i (i = 0, 1, ..., n-1)$;
3. $q^2 \nmid a_0$.

Então f *é irredutível sobre* $\mathbb{Q}$.

Demonstração. Pelo Lema de Gauss, é suficiente mostrar que f é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que $f = gh$, em que,

$$g = b_0 + b_1t + ... + b_rt^r \qquad h = c_0 + c_1t + ... + c_st^s$$

são polinômios de grau menor do que f sobre $\mathbb{Z}$. Então, $r \geq 1, s \geq 1, r + s = n$. Agora, $b_0c_0 = a_0$, e pelo item 2., $q|a_0$ e como q é primo, $q|b_0$ ou $q|c_0$. Já pelo item 3., temos que q não pode dividir ambos b_0 e c_0, assim, sem perda de generalidade, podemos assumir que $q|b_0$ e $q \nmid c_0$. Se todos os b_j forem divisíveis por q, então a_n é divisível por q, o que contraria o item 1.. Consideremos b_j o primeiro coeficiente de g que não é divisível por q. Então,

$$a_j = b_jc_0 + ... + b_0c_j$$

com $j < n$. Deste modo, concluímos que $q|c_0$, pois q divide $a_j, b_0, ..., b_{j-1}$, mas não b_j. O que é uma contradição. Portanto, f é irredutível. □

Exemplos 3.4.2.

1. *Consideremos* $f(t) = \frac{2}{9}t^5 + \frac{5}{3}t^4 + t^3 + \frac{1}{3}$ *sobre* $\mathbb{Q}$. *Afirmemos que este polinômio é irredutível sobre* $\mathbb{Q}$. *Ora, se* $9f(t) = 2t^5 + 15t^4 + 9t^3 + 3$ *é irredutível sobre* $\mathbb{Q}$, *então* $f(t)$ *também o é. Apliquemos agora o Critério de Eisenstein com* $q = 3$*:*

   - $3 \nmid 2$;
   - $3|a_i (i = 0, 1, 2, 3, 4)$;
   - $3^2 = 9 \nmid 3$.

   O que mostra que $9f(t)$ *é irredutível sobre* $\mathbb{Q}$, *e portanto,* $f(t)$ *também o é.*

2. *Consideremos* $f(t) = t^{16} + t^{15} + t^{14} + t^{13} + t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$, *o exemplo que iniciamos o capítulo. Como o termo independente deste polinômio é* 1, *não somos capazes de analisar a irredutibilidade pelo Critério de Eisenstein. Porém,* $f(t)$ *é irredutível em* $\mathbb{Q}$, *se, e só se,* $f(t+1)$ *o for. Ao expandirmos* $f(t+1)$ *conseguimos,*

$$\begin{aligned} f(t+1) &= t^{16} + 17t^{15} + 136t^{14} + 680t^{13} + 2380t^{12} + 6188t^{11} \\ &+ 12376t^{10} + 19448t^9 + 24310t^8 + 24310t^7 + 19448t^6 \\ &+ 12376t^5 + 6188t^4 + 2380t^3 + 680t^2 + 136t + 17 \\ &= t^{16} + 17(t^{15} + 8t^{14} + 40t^{13} + 140t^{12} + 364t^{11} + 728t^{10} \\ &+ 1144t^9 + 1430t^8 + 1430t^7 + 1144t^6 + 728t^5 + 364t^4 \\ &+ 140t^3 + 40t^2 + 8t + 1). \end{aligned}$$

Portanto, usando o Critério de Eisenstein com $q = 17$, *temos que* $f(t+1)$ *é irredutível sobre* $\mathbb{Q}$, *e por consequência,* $f(t)$ *também o é.*

3.5 Redução Módulo p

Um segundo modo para provar a irredutibilidade de polinômios em $\mathbb{Z}[t]$ envolve a redução polinomial módulo p com p um inteiro primo.

Relembremos que se $n \in \mathbb{Z}$, e $a, b \in \mathbb{Z}$ são congruentes módulo n,

$$a \equiv b (mod\ n),$$

temos que $a - b$ é divisível por n. O número n é chamado de módulo, e a congruência módulo n é uma relação de equivalência como anteriormente visto. E mais, denotaremos o conjunto das classes de equivalência por $\mathbb{Z}_n$, que possui de certo modo a mesma aritmética que $\mathbb{Z}$.

Definição 3.5.1. *O grupo de unidades* $\mathbb{Z}_n^*$ *de* $\mathbb{Z}_n$ *consiste nos elementos* $a \in \mathbb{Z}_n$ *tal que* $1 \leq a \leq n$ *e* a *é primo a* n *sob a operação de multiplicação.*

A ordem deste grupo é dada por uma importante função aritmética,

Definição 3.5.2. *A função de Euler,* $\phi(n)$, *é o número de inteiros* a, *com* $1 \leq a \leq n-1$, *tal que* a *é primo a* n.

Ou seja, a ordem de $\mathbb{Z}_n^*$ é igual a $\phi(n)$.

Temos que a função de Euler, tem inúmeras propriedades interessantes, em particular,

$$\phi(p^k) = (p-1)p^{k-1},$$

se p é primo, e

$$\phi(r)\phi(s) = \phi(rs),$$

quando r, s são primos entre si.

Ao considerarmos a aplicação $f : \mathbb{Z} \to \mathbb{Z}_n$ que associa, um número $m \in \mathbb{Z}$ a sua classe de equivalência módulo n (n aqui é um inteiro primo), podemos pensar em estender $g : \mathbb{Z}[t] \to \mathbb{Z}_n[t]$. Assim, como $\mathbb{Z}_n$ é finito, somos capazes de pensar em irredutibilidade mais facilmente em $\mathbb{Z}_n[t]$, para depois entendermos irredutibilidade em $\mathbb{Z}[t]$ (tudo isto por meio do isomorfismo criado).

Exemplo 3.5.3. *Consideremos $f(t) = t^4 + 15t^3 + 7$ sobre $\mathbb{Z}$.*

Sobre $\mathbb{Z}_5$, temos que este se torna $t^4 + \overline{2}$. Se este for redutível sobre $\mathbb{Z}_5$, então este tem um fator de grau 1, ou é produto de dois fatores de grau 2. A primeira possibilidade nos leva a um elemento $x \in \mathbb{Z}_5$ tal que $x^4 + \overline{2} = \overline{0}$. Vejamos que isto não é possível,

$$\begin{aligned}
(\overline{0})^4 + \overline{2} &\equiv \overline{0} + \overline{2} \equiv \overline{2} \\
(\overline{1})^4 + \overline{2} &\equiv \overline{1} + \overline{2} \equiv \overline{3} \\
(\overline{2})^4 + \overline{2} &\equiv \overline{16} + \overline{2} \equiv \overline{18} \equiv \overline{3} \\
(\overline{3})^4 + \overline{2} &\equiv \overline{81} + \overline{2} \equiv \overline{83} \equiv \overline{3} \\
(\overline{4})^4 + \overline{2} &\equiv \overline{256} + \overline{2} \equiv \overline{258} \equiv \overline{8} \equiv \overline{3}
\end{aligned}$$

No outro caso, temos sem perda de generalidade,

$$t^4 + \overline{2} = (t^2 + at + b)(t^2 + ct + d)$$

com $a, b, c, d \in \mathbb{Z}_5$.

Portanto, $a + c = \overline{0}$, $ac + b + d = \overline{0}$, $bd = \overline{2}$. Assim, $b + d = a^2$ que pode apenas assumir os valores, $\overline{0}, \overline{1}, \overline{4}$, que são os quadrados perfeitos em $\mathbb{Z}_5$. Logo, ou $b(1 - b) = 2$, ou $-b^2 = 2$, ou $b(4 - b) = 2$. Donde, tentando todas as possibilidades para b, vemos que não há uma que satisfaça estas equações. Daí, temos que $t^4 + \overline{2}$ é irredutível sobre $\mathbb{Z}_5$, e por consequência, $f(t)$ é irredutível sobre $\mathbb{Z}$, e daí também o é sobre $\mathbb{Q}$.

Capítulo 4

Extensões de Corpos

Neste capítulo, trataremos do conceito de extensões de corpos atreladas às equações polinomiais, uma vez que, ao considerarmos um determinado subcorpo dos complexos, este pode não conter todas as soluções de uma polinomial específica, donde procuramos por um outro subcorpo de $\mathbb{C}$ que as tenha, e por consequência contenha uma "cópia" deste subcorpo inicial. Expressemos matematicamente tal fala:

Definição 4.0.4. *Uma extensão de corpo é um monomorfismo $\iota : K \to L$, em que K e L são subcorpos complexos. Diremos que K que é o corpo menor e L é o corpo maior.*

Pensamos numa extensão de corpos como um par (K, L) de corpos, quando fica subentendido o monomorfismo entre eles.

Exemplos 4.0.5.

1. *Pensemos inicialmente em $\mathbb{Q}$, e consideremos a seguinte polinomial quártica:*

$$f(t) = t^4 - 4t^2 + 5.$$

Fatoramos tal, por irredutíveis em $\mathbb{Q}$ obtendo,

$$f(t) = (t^2 + 1)(t^2 - 5),$$

cujos zeros são os números irracionais $\pm i$ e $\pm\sqrt{5}$. Adiante, veremos que existe um subcorpo natural L de $\mathbb{C}$ associado a estes zeros, de fato, este subcorpo é o menor subcorpo que os contém. Afirmemos que L consiste de todos os números complexos da forma

$$p + qi + r\sqrt{5} + si\sqrt{5}, \quad p, q, r, s \in \mathbb{Q}.$$

E mais, observemos que $\mathbb{Q}$ está imerso em L, bastando tomarmos q, r e s como sendo zeros na expressão acima.

2. *As funções inclusões $\iota_1 : \mathbb{Q} \to \mathbb{R}$, $\iota_2 : \mathbb{R} \to \mathbb{C}$, e $\iota_3 : \mathbb{Q} \to \mathbb{C}$ são extensões de corpos. Claramente tais inclusões são monomorfismo.*

3. *Seja K o conjunto de todos os números reais da forma $p + q\sqrt{2}$, em que $p, q \in \mathbb{Q}$. Então, K é um subcorpo de $\mathbb{C}$, e a função inclusão $\iota : \mathbb{Q} \to K$ é uma extensão de $\mathbb{Q}$ em K.*

Se $\iota : K \to L$ é uma extensão de corpos, então geralmente identificamos K com sua imagem $\iota(K)$, então podemos pensar em ι como uma inclusão e K pode ser pensado como um subcorpo de L. Nestas circunstâncias, usamos a notação

$$L : K$$

para a extensão, e dizemos que L é uma extensão de K.

Definição 4.0.6. *Seja X um subconjunto de $\mathbb{C}$. Então o subcorpo de $\mathbb{C}$ gerado por X é a interseção de todos os subcorpos de $\mathbb{C}$ que contém X.*

Equivalentemente, este é o subcorpo X que satisfaz alguma das seguintes condições,

1. *O único menor subcorpo de $\mathbb{C}$ que contém X;*

2. *O conjunto de todos os elementos de $\mathbb{C}$ que pode ser obtido a partir de elementos de X por uma sequência de finita de operações.*

Uma questão natural é perguntarmos sobre a existência de um menor corpo contido nos complexos. Este conceito é conhecido como subcorpo primo.

Proposição 4.0.7. *Todo subcorpo de $\mathbb{C}$ contém $\mathbb{Q}$.*

Demonstração. Seja $K \subseteq \mathbb{C}$ um subcorpo. Então $0, 1 \in K$ por definição de subcorpo, daí por consequência (ou melhor por um processo de indução) qualquer número $n \in \mathbb{N}$ também está em K. Como K é fechado com relação a operação de adição e mais ainda, é um subcorpo, conseguimos que qualquer número $-n$ com $n \in \mathbb{N}$ pertence a K. Ou seja, temos que $\mathbb{Z} \subseteq K$. Finalmente, se $p, q \in \mathbb{Z}$ e $q \neq 0$, então temos que $p, q \in K$, e mais ainda, como K é subcorpo, $q^{-1} \in K$, e este sendo fechado com relação a operação de multiplicação, concluímos que $pq^{-1} \in K$.

Portanto, $\mathbb{Q} \subseteq K$, como queríamos demonstrar. □

Observação 4.0.8. *Em particular, todo subcorpo gerado por X contém $\mathbb{Q}$.*

Usamos a notação $\mathbb{Q}(X)$ para representar o subcorpo de $\mathbb{C}$ gerado por X.

Exemplo 4.0.9. *Procuraremos um subcorpo K de $\mathbb{C}$ gerado pelo conjunto $X = \{1, i\}$. Pelo que vimos na Proposição 4.0.7, K deve conter $\mathbb{Q}$. Como K é fechado com relação as operações de adição e multiplicação, uma vez que é um subcorpo de $\mathbb{C}$, este deve conter os números complexos da forma $p + qi$, com $p, q \in \mathbb{Q}$. Seja M o conjunto de todos os complexos desta forma. M é um subcorpo de $\mathbb{C}$, e portanto, fechado com relação as operações de adição e multiplicação. Além disso,*

$$(p + qi)^{-1} = \frac{p}{p^2 + q^2} - \frac{q}{p^2 + q^2} i,$$

também pertence a M. Como M é um subcorpo que contém X, e sabemos ser K o menor subcorpo contendo X, devemos ter $K \subseteq M$. Ora, $M \subseteq K$, por definição. Então, $K = M$, e assim temos a descrição do subcorpo gerado por X.

Dada uma extensão de corpos $L : K$, estamos interessados principalmente nos subcorpos entre K e L. Isto significa que nós iremos restringir nossa atenção nos subconjuntos X que contém K e estão contidos em L, ou melhor, em conjuntos $X = K \cup Y$, com $Y \subseteq L$.

Definição 4.0.10. *Se $L : K$ é uma extensão de corpos e Y é um subconjunto de L, então o subcorpo de $\mathbb{C}$ gerado por $K \cup Y$ é escrito como $K(Y)$ e é dito ser obtido a partir de K adicionando Y.*

Exemplo 4.0.11. *Logo no início do capítulo (no Exemplo 1) falamos brevemente sobre o exemplo em questão, porém trataremos este com um pouco mais de cuidado agora.*

Seja $K = \mathbb{Q}$, e seja $Y = \{i, \sqrt{5}\}$. Então $K(Y)$ deve conter K e Y. Este também deve conter o produto $i\sqrt{5}$. Como pela Proposição 4.0.7, temos que $K \subseteq \mathbb{Q}$, o subcorpo $K(Y)$ deve conter os elementos

$$\alpha = p + qi + r\sqrt{5} + si\sqrt{5} \quad (p, q, r, s \in \mathbb{Q}).$$

Seja $L \subseteq \mathbb{C}$, o conjunto de todos os números α como acima. Se conseguirmos provar que L é um subcorpo de $\mathbb{C}$, sabendo que $K(Y) \subseteq L$, por definição, e $K(Y)$ ser o menor subcorpo de $\mathbb{C}$ com a propriedade acima, segue que $K(Y) = L$. Para L ser um subcorpo de $\mathbb{C}$ resta provarmos que qualquer que seja $\alpha \neq 0$, encontramos o seu inverso α^{-1} pertencente a L (já temos nitidamente o fechamento das operações e a pertinência de 0 e 1 em L). De fato, temos que provar que $(p, q, r, s) \neq (0, 0, 0, 0)$, então

$$(p + qi + r\sqrt{5} + si\sqrt{5})^{-1} \in L.$$

Primeiro, suponhamos que $p + qi + r\sqrt{5} + si\sqrt{5} = 0$. Então,

$$p + r\sqrt{5} = -i(q + s\sqrt{5}).$$

Notemos que o lado esquerdo, $p + r\sqrt{5}$, é um número real, enquanto que o lado direito, $-i(q + s\sqrt{5})$, é um número complexo. Portanto, $p + r\sqrt{5} = 0$ e $q + s\sqrt{5} = 0$. Se $r \neq 0$, então $\sqrt{5} = \frac{-p}{r} \in \mathbb{Q}$, mas $\sqrt{5}$ é um irracional. Logo, devemos ter $r = 0$, donde $p = 0$. De modo análogo, $q = s = 0$.

Provaremos a existência de α^{-1} em duas etapas. Seja M um subconjunto de L contendo todos $p + qi$ $(p, q \in \mathbb{Q})$. Então escrevemos,

$$\alpha = x + y\sqrt{5},$$

com $x = p + iq$ *e* $y = r + is \in M$. *Seja*

$$\beta = p + qi - r\sqrt{5} - si\sqrt{5} = x - y\sqrt{5} \in L.$$

Então,

$$\alpha\beta = (x + y\sqrt{5})(x - y\sqrt{5}) = x^2 - 5y^2 = z$$

diremos, que $z \in M$. *Como* $\alpha \neq 0$ *e* $\beta \neq 0$, *temos* $z \neq 0$, *e portanto,* $\alpha^{-1} = \beta z^{-1}$. *Escrevemos agora,* $z = u + vi$ $(u, v \in \mathbb{Q})$, *e consideremos* $w = u - vi$. *Como* $zw = u^2 + v^2 \in \mathbb{Q}$, *temos*

$$z^{-1} = (u^2 + v^2)^{-1} w \in M$$

então, $\alpha^{-1} = \beta z^{-1} \in L$.

4.1 Expressões Racionais

Discutimos anteriormente que $\mathbb{C}[t]$ é um domínio de integridade (mais especificamente, na seção: Equações Polinomiais do Capítulo 2), não admitindo inverso multiplicativo qualquer que seja o polinômio, porém podemos pensar em ampliar este conceito a partir do que chamaremos de funções racionais ou mais formalmente expressões racionais de indeterminada t.

Definição 4.1.1. *Uma expressão racional de indeterminada* t *é uma função* $f(t) = \frac{p(t)}{q(t)}$ *em que,* $p(t), q(t) \in \mathbb{C}[t]$, *e ainda* $q(t) \neq 0$, *isto é, consideraremos o conjunto* $\{z \in \mathbb{C}; q(z) \neq 0\}$ *como sendo o domínio desta função racional.*

Podemos, de modo similar, pensar em funções racionais com mais indeterminadas.

4.2 Extensões Simples

Consideraremos agora os tijolos iniciais da teoria de extensão de corpos.

Definição 4.2.1. *Uma extensão simples é uma extensão de corpos* $L : K$ *tal que* $L = K(\alpha)$ *para algum* $\alpha \in L$, *ou seja, uma extensão simples é resultado da adição de um único elemento ao corpo menor.*

Exemplos 4.2.2.

1. *O subcorpo* $\mathbb{R}(i)$ *de* $\mathbb{C}$, *contém todos os elementos da forma* $x + iy$, *com* $x, y \in \mathbb{R}$. *Mas, estes elementos acabam por percorrer todo o conjunto* $\mathbb{C}$, *assim,* $\mathbb{C} = \mathbb{R}(i)$.

2. *O subcorpo* P *de* $\mathbb{R}$ *consistindo dos números* $p + q\sqrt{2}$, *com* $p, q \in \mathbb{Q}$ *é igual ao subcorpo* $\mathbb{Q}(\sqrt{2})$.

3. *Consideremos* $L = \mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5})$, *que aparentemente não parece ser uma extensão simples, porém afirmamos que o é. Se escrevermos* $L' = \mathbb{Q}(i + \sqrt{5})$, *temos nitidamente que* L' *é uma extensão simples. Provemos então que* $L = L'$. *Para isto, notemos primeiramente que* $L' \subseteq L$, *resta-nos mostrar a inclusão inversa, mas para esta basta concluirmos que* i *e* $\sqrt{5} \in L'$.

   Sabemos que L' *contém,*

$$(i + \sqrt{5})^2 = -1 + 2i\sqrt{5} + 5 = 4 + 2i\sqrt{5},$$

   e portanto, contém

$$(i + \sqrt{5})(2 + 2i\sqrt{5}) = 14i - 2\sqrt{5},$$

   e assim,

$$14i - 2\sqrt{5} + 2(i + \sqrt{5}) = 16i$$

   também pertence a L'. *Daí,* $i \in L'$, *e então* $(i + \sqrt{5}) - i = \sqrt{5}$ *também. Portanto,* $L' \subseteq L$ *e podemos concluir a igualdade entre os conjuntos. Concluímos assim que* $\mathbb{Q}(i, -i, \sqrt{r}, -\sqrt{5}) : \mathbb{Q}$ *é, de fato, uma extensão simples.*

Uma questão natural que surge neste contexto, é a da equivalência entre extensões. Ela será abordada através do conceito de isomorfismo de extensões. Este conceito será importante no desenvolvimento da classificação das extensões a ser realizado na próxima seção.

Definição 4.2.3. *Um isomorfismo entre duas extensões de corpos* $\iota : K \to \hat{K}$, $j : L \to \hat{L}$ *é um par* (λ, μ) *de isomorfismos* $\lambda : K \to L$, $\mu : \hat{K} \to \hat{L}$, *tal que para todo* $k \in K$,

$$j(\lambda(k)) = \mu(\iota(k)).$$

Ou de um modo mais visual, temos o seguinte diagrama comutativo,

$$\begin{array}{ccc} K & \xrightarrow{\iota} & \hat{K} \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\mu} \\ L & \xrightarrow[j]{} & \hat{L} \end{array}$$

isto é, os dois possíveis caminhos de K *a* $\hat{L}$ *originam a mesma função.*

A ideia de equivalência expressada por isomorfismo é válida, pois estes, preservam propriedades do corpo domínio no corpo imagem.

Várias identificações podem ser feitas. Se identificarmos K e $\iota(K)$, e L e $j(L)$, então ι e j são inclusões, e a condição de comutatividade agora torna:

$$\mu|_K = \lambda,$$

em que $\mu|_K$ denota a restrição de μ sobre K. Se identificarmos K e L, então λ torna-se a identidade, e então $\mu|_K$ é a identidade. Tentaremos usar sempre que possível esta identificação.

Capítulo 5

Extensões Simples

Durante este capítulo, continuaremos tratando de extensões simples, buscando realizar uma classificação. E ainda, exporemos o conceito de polinômio minimal, importante na construção de corpos a partir de um domínio de integridade dado pelos polinômios com coeficientes em um certo corpo e indeterminada t.

Extensões simples são classificadas em dois tipos: transcendentes e algébricas. Considerando K um subcorpo de $\mathbb{C}$, e caso o novo elemento α satisfaça uma equação polinomial sobre K, então, a extensão é dita algébrica; caso contrário, é transcendente. A partir de isomorfismos, K, tem exatamente uma extensão simples do tipo transcendente. Para a maioria dos corpos K, há muitas possibilidades para extensões simples algébricas, elas são classificadas pelos polinômios irredutíveis m sobre K.

Em resumo, este último paragrafo em linguagem matemática e contemplamos tal na seguinte definição,

Definição 5.0.4. *Seja K um subcorpo de $\mathbb{C}$, e seja $\alpha \in \mathbb{C}$. Então α é algébrico sobre K se existe um polinômio não nulo p sobre K, tal que, $P(\alpha) = 0$. Caso contrário, dizemos que α é transcendente sobre K.*

Exemplos 5.0.5.

1. *O número $\alpha = \sqrt{2}$ é algébrico sobre $\mathbb{Q}$, pois o polinômio $p(t) = t^2 - 2$ tem α como raiz, isto é, $p(\alpha) = \alpha^2 - 2 = \sqrt{2}^2 - 2 = 0$.*

2. *O número $\beta = \sqrt[3]{2}$ também é algébrico sobre $\mathbb{Q}$, pois $q(\beta) = 0$, onde $q(t) = t^3 - 2$.*

3. *O número π é transcendente sobre $\mathbb{Q}$, mas veremos com mais detalhes tal fato no capítulo sobre construções com régua e compasso.*

4. *Ora, $\lambda = \sqrt{\pi}$ é ainda transcendente sobre $\mathbb{Q}$. Suponhamos que este não o seja, isto é, existe um polinômio $p(t) \in \mathbb{Q}[t] - \{0\}$ tal que $p(\lambda) = 0$. Separando os termos de grau par dos de grau ímpar, conseguimos escrever $p(\sqrt{\pi})$ do seguinte modo, $a(\pi) + b(\pi)\sqrt{\pi} = 0$. Donde, $a(\pi) = -b(\pi)\sqrt{\pi}$ e $a^2(\pi) = b^2(\pi)\pi$. Daí,*

$f(\pi) = 0$, *onde*

$$f(t) = a^2(t) - tb^2(t) \in \mathbb{Q}[t].$$

Como $\partial(a^2)$ *é par, enquanto que* $\partial(b^2)$ *é ímpar, temos que* $f(t)$ *acima é um polinômio em* $\mathbb{Q}[t]$ *não nulo. Ou seja, acabamos de mostrar que* π *é um número algébrico sobre* $\mathbb{Q}$*, o que é um absurdo. Sendo assim,* $\sqrt{\pi}$ *de fato é transcendente sobre* $\mathbb{Q}$*.*

5. *Embora,* π *e* $\sqrt{\pi}$ *sejam transcendentes sobre* $\mathbb{Q}$*, como comentado nos itens anteriores, temos que* $\gamma = \sqrt{\pi}$ *é algébrico sobre* $\mathbb{Q}(\pi)$*, uma vez que* $\gamma^2 - \pi = 0$*.*

Afirmemos que se $K(t)$ é o conjunto de funções racionais com indeterminada t sobre K, então $K(t) : K$ é a única extensão transcendente simples de K por meio de isomorfismos. Se $K(\alpha) : K$ é algébrico, há mais de uma possibilidade de extensão por isomorfismos, ainda sim, são tratáveis. Mostraremos que há um único polinômio mônico irredutível m sobre K tal que $m(\alpha) = 0$, e m determina a extensão unicamente por isomorfismos.

Teorema 5.0.6. *O conjunto das expressões racionais* $K(t)$ *é uma extensão transcendente simples do subcorpo* K *de* $\mathbb{C}$*.*

Demonstração. Temos que $K(t) : K$ é uma extensão simples gerada pelo t. Se p é um polinômio sobre K, tal que $p(t) = 0$, então por definição de $K(t)$, $p = 0$. Daí, temos que t não anula nenhum polinômio sobre $K(t)$, e a extensão em questão é transcendente. □

5.1 O Polinômio Minimal

O polinômio minimal, como já falado, será importante para a determinação única de extensões simples algébricas a partir de isomorfismos. Porém, para o entendermos, precisamos de alguns conceitos anteriores.

Definição 5.1.1. *Um polinômio* $f(t) = a_0 + a_1t + ... + a_nt^n$ *sobre um subcorpo* K *de* $\mathbb{C}$ *é* <u>*mônico*</u> *se* $a_n = 1$*. Ou melhor dizendo, um polinômio é dito mônico se o coeficiente do maior termo é 1.*

Notamos que todo polinômio é um múltiplo de algum polinômio mônico, e para polinômios não nulos, este mônico é único. Além disso, o produto de dois polinômios mônicos é novamente um polinômio mônico.

Suponhamos agora, que $K(\alpha) : K$ é uma extensão algébrica simples. Portanto, existe um polinômio p sobre K, tal que α seja raiz, ou seja, $p(\alpha) = 0$. Podemos assumir que tal polinômio é mônico (caso este não o seja, basta multiplicarmos todos os coeficientes pelo inverso do que acompanha o termo de maior grau). Sendo assim, existe ao menos um polinômio mônico de menor grau que tenha α como um zero. Afirmamos que tal, é único. De fato, suponhamos que existam p, q polinômios de menor grau que tenham α como um zero. Então, $p(\alpha) - q(\alpha) = 0$. Como $p \neq q$, temos que alguma constante múltipla de $p - q$

é um polinômio mônico com α como zero. Donde, contrariamos o fato de p e q serem os polinômios mônicos de menor grau que tinham α como raiz (usando as propriedades de grau de polinômio). Concluímos assim que existe um único polinômio mônico p de menor grau tal que $p(\alpha) = 0$. A este p, damos o seguinte nome,

Definição 5.1.2. *Seja $L : K$ uma extensão de corpos, e suponhamos que $\alpha \in L$ é algébrico sobre K. Então, o polinômio minimal de α sobre K, é o único polinômio mônico m sobre K de menor grau tal que $m(\alpha) = 0$.*

Exemplo 5.1.3. *Sabemos que $\mathbb{R}(i) = \mathbb{C} : \mathbb{R}$ é uma extensão simples e algébrica sobre $\mathbb{R}$, pois $m(t) = t^2 + 1 \in \mathbb{R}[t]$ é um polinômio tal que $m(i) = 0$. Notemos que tal m é mônico. Afirmemos que este é o polinômio minimal de i sobre $\mathbb{R}$. De fato, se este não fosse, os polinômios de menor grau em $\mathbb{R}$ seriam da forma $t + r$ para algum $r \in \mathbb{R}$, ou o polinômio constante igual a 1. Ora, i não pode ser zero de nenhum destes, pois se o fosse, teríamos $i \in \mathbb{R}$. Portanto, o polinômio minimal de i sobre $\mathbb{R}$, é mesmo o $m(t) = t^2 + 1$.*

Veremos no lema a seguir quais são os polinômios que podem ser minimal.

Lema 5.1.4. *Se α é um elemento algébrico sobre um subcorpo K de $\mathbb{C}$, então o polinômio minimal de α sobre K é irredutível sobre K. Ele ainda divide qualquer polinômio em que α é um zero.*

Demonstração. Suponhamos que o polinômio minimal m de α sobre K é redutível, isto é, $m = fg$ com f e g polinômios sobre K de graus menores que m. Podemos assumir que f e g são mônicos. Então, como $m(\alpha) = 0$, devemos ter $f(\alpha)g(\alpha) = 0$, e como $K[t]$ é um domínio de integridade, $f(\alpha) = 0$ ou $g(\alpha) = 0$, o que contrariaria a definição de polinômio minimal. Portanto, m é irredutível sobre K.

Suponhamos agora que p é um polinômio sobre K, tal que, $p(\alpha) = 0$. Assim, pelo Algoritmo da Divisão, existem polinômios q e r sobre K, tais que, $p = mq + r$ e $\partial r < \partial m$. Então, $0 = p(\alpha) = m(\alpha)q(\alpha) + r(\alpha) = 0 \cdot q(\alpha) + r(\alpha) = r(\alpha)$. Se tivermos $r \neq 0$, então existe um múltiplo constante de r que é mônico, e deste modo, o grau deste é menor do que o grau de m, gerando uma contradição com o fato de m ser o polinômio minimal de α sobre K. Portanto, $r = 0$, e m divide p. □

Teorema 5.1.5. *Se K é um subcorpo de $\mathbb{C}$ e m é qualquer polinômio mônico irredutível sobre K, então existe um $\alpha \in \mathbb{C}$, algébrico sobre K, tal que α tem m como polinômio minimal sobre K.*

O teorema acima expresso deixa claro que qualquer polinômio mônico irredutível sobre um subcorpo K de $\mathbb{C}$ é minimal.

Demonstração. Seja α um zero qualquer de m em $\mathbb{C}$. Então, $m(\alpha) = 0$, e portanto, o polinômio minimal f de α sobre K, divide m. Ora, m é irredutível sobre K, e ambos f e m são mônicos, logo $f = m$. □

5.2 Extensões Algébricas Simples

Nesta seção iremos descrever a estrutura de corpo das extensões $K(\alpha) : K$, quando α tem um polinônio minimal m sobre K.

Definição 5.2.1. *Dados dois polinômios $a, b \in K[t]$, calcularemos a congruência módulo m, com m um polinômio sobre K, do seguinte modo,*

$$a \equiv b \ (mod\ m)$$

se $a(t) - b(t)$ é divisível por $m(t)$ em $K[t]$.

Lema 5.2.2. *Suponhamos que $a_1 \equiv b_1 (mod\ m)$ e $a_2 \equiv b_2 (mod\ m)$. Então, $a_1 + a_2 \equiv b_1 + b_2 (mod\ m)$, e $a_1 a_2 \equiv b_1 b_2 (mod\ m)$.*

Demonstração. Como $a_1 \equiv b_1 (mod\ m)$ e $a_2 \equiv b_2 (mod\ m)$, temos que $a_1 - b_1 = a \cdot m$ e $a_2 - b_2 = b \cdot m$, para alguns polinômios $a, b \in K[t]$.

Agora,

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = (a - b) \cdot m$$

provando a primeira afirmação.

Já para o produto, temos a demonstração saindo de,

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= a_1 a_2 - a_1 b_2 + a_1 b_2 - b_1 b_2 \\ &= a_1(a_2 - b_2) + b_2(a_1 - b_1) \\ &= (a_1 b + b_2 a) \cdot m. \end{aligned}$$

□

Lema 5.2.3. *Todo polinômio $a \in K[t]$ é congruente módulo m a um único polinômio de grau menor do que o grau de m.*

Demonstração. Sabemos pelo algoritmo da divisão que existem q e r, polinômios sobre K, tais que $a = q \cdot m + r$, com $\partial r < \partial m$. Logo, $a - r = q \cdot m$, e portanto, $a \equiv r (mod\ m)$. Resta agora provarmos a unicidade, para tal suponhamos que $r \equiv s (mod\ m)$, e que $\partial r, \partial s < \partial m$. Daí, $r - s$ é divisível por m, e possui grau menor do que m, o que nos leva a $r - s = 0$, e portanto, $r = s$, como gostaríamos de provar. □

Chamamos r de forma reduzida de a módulo m. E pelo Lema anterior, vemos que podemos calcular polinômios módulo m em termos das suas formas reduzidas.

De um modo mais abstrato podemos trabalhar com classes de equivalência. A relação $\equiv\ (mod\ m)$ é uma relação de equivalência em $K[t]$, e assim, particiona $K[t]$ em classes de equivalências.

Antes de continuarmos descrevendo as classes de equivalência segundo esta relação, vejamos que de fato, $\equiv\ (mod\ m)$ é uma relação de equivalência:

- Dado $a \in K[t]$, temos que $a - a = 0 = 0 \cdot m$, ou seja, $a \equiv a(mod\ m)$ - validade da reflexividade;
- Dados $a, b \in K[t]$, se $a \equiv b(mod\ m)$, então $a - b = n \cdot m$, para algum $n \in K[t]$. Sendo assim, como $(b - a) = -(a - b) = -n \cdot m$, e $K[t]$, é domínio de integridade, temos também que $b \equiv a(mod\ m)$ - validade da simetria;
- Dados $a, b, c \in K[t]$, se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$ então, $a - b = n \cdot m$ e $b - c = o \cdot m$, para alguns $n, o \in K[t]$. Ora, $a - c = (a - b) + (b - c) = n \cdot m + o \cdot m = (n + o) \cdot m$, e portanto $a \equiv c(mod\ m)$ - validade da transitividade.

Como de fato temos a relação de equivalência, escreveremos $[a]$ como sendo a classe de equivalência de $a \in K[t]$. Deste modo,

$$[a] = \{f \in K[t] : m|(a - f)\}.$$

A soma e o produto de duas classes de equivalência $[a]$ e $[b]$ podem ser definidos como:

$$[a] + [b] = [a + b] \quad e \quad [a][b] = [ab].$$

Cada classe de equivalência contém um único polinômio de grau menor do que o grau de m, o chamado polinômio reduzido.

Escreveremos,

$$\frac{K[t]}{\langle m \rangle}$$

para representar o conjunto de classe de equivalências de $K[t]$ módulo m. Apenas com a ideia de alertar o leitor, vemos que o quociente em questão é dado por um anel (melhor até dizendo, um domínio de integridade) e por um ideal gerado pelo polinômio m.

Teorema 5.2.4. *Todo elemento não nulo de $\frac{K[t]}{\langle m \rangle}$ tem um inverso multiplicativo em $\frac{K[t]}{\langle m \rangle}$ se, e somente se, m é irredutível sobre $K[t]$.*

O teorema anterior também nos diz que, se m é irredutível sobre K, então $\langle m \rangle$ é um ideal maximal, e portanto, $\frac{K[t]}{\langle m \rangle}$ é um corpo.

Demonstração. Suponhamos que m seja redutível em $K[t]$, logo, existem $a, b \in K[t]$, tais que $m = ab$ e $\partial a, \partial b < \partial m$. Então, $[a][b] = [ab] = [m] = [0]$. Suponhamos que $[a]$ tenha um inverso multiplicativo $[c]$, tal que $[a][c] = 1$. Então, $[0] = [c][0] = [c][a][b] = [1][b] = [b]$, então m divide b. Como $\partial b < \partial m$, devemos ter $b = 0$ e daí $m = 0$, mas por convenção 0 não é irredutível.

Se m é irredutível, seja $a \in K[t]$ com $[a] \neq [0]$; isto é, $m \nmid a$. Assim, a e m são primos entre si, ou seja, o maior fator comum entre eles é 1. Por teorema já visto, Teorema 3.1.9 temos que existem $h, k \in K[t]$ tais que $ha + km = 1$. Então, $[h][a] + [k][m] = [1]$, mas $[m] = [0]$ então $[1] = [h][a] + [k][m] = [h][a] + [k][0] = [h][a] + [0] = [h][a]$. Portanto, $[h]$ é o inverso procurado. □

5.3 Classificando Extensões Simples

Teorema 5.3.1. *Toda extensão transcendente simples $K(\alpha) : K$ é isomórfica a extensão $K(t) : K$ das expressões racionais de indeterminada t sobre K. O isomorfismo $K(t) \to K(\alpha)$ pode ser escolhido para associar t a α, e para ser a identidade sobre K.*

Demonstração. Definamos uma função

$$\phi : K(t) \to K(\alpha)$$

por

$$\phi\left(\frac{f(t)}{g(t)}\right) = \frac{f(\alpha)}{g(\alpha)}.$$

Se $g \neq 0$, então $g(\alpha) \neq 0$ (uma vez que α é transcendente). Logo, o modo como definimos a função faz sentido. Notemos que a função acima é um homomorfismo injetor, portanto, um monomorfismo:

$$\begin{aligned}
\phi\left(\frac{f(t)}{g(t)} + \frac{h(t)}{i(t)}\right) &= \phi\left(\frac{f(t)i(t) + h(t)g(t)}{g(t)i(t)}\right) \\
&= \frac{f(\alpha)i(\alpha) + h(\alpha)g(\alpha)}{g(\alpha)i(\alpha)} \\
&= \frac{f(\alpha)i(\alpha)}{g(\alpha)i(\alpha)} + \frac{h(\alpha)g(\alpha)}{g(\alpha)i(\alpha)} \\
&= \frac{f(\alpha)}{g(\alpha)} + \frac{h(\alpha)}{i(\alpha)} \\
&= \phi\left(\frac{f(t)}{g(t)}\right) + \phi\left(\frac{h(t)}{i(t)}\right).
\end{aligned}$$

E,

$$\begin{aligned}
\phi\left(\frac{f(t)}{g(t)} \cdot \frac{h(t)}{i(t)}\right) &= \phi\left(\frac{f(t)h(t)}{g(t)i(t)}\right) \\
&= \frac{f(\alpha)h(\alpha)}{g(\alpha)i(\alpha)} \\
&= \frac{f(\alpha)}{g(\alpha)} \cdot \frac{h(\alpha)}{i(\alpha)} \\
&= \phi\left(\frac{f(t)}{g(t)}\right) \cdot \phi\left(\frac{h(t)}{i(t)}\right).
\end{aligned}$$

Mais ainda,

$$\begin{aligned}
\phi\left(\frac{f(t)}{g(t)}\right) \neq \phi\left(\frac{h(t)}{i(t)}\right) &\Rightarrow \frac{f(\alpha)}{g(\alpha)} \neq \frac{h(\alpha)}{i(\alpha)} \\
&\Rightarrow \frac{f(\alpha)}{g(\alpha)} - \frac{h(\alpha)}{i(\alpha)} \neq 0
\end{aligned}$$

$$\Rightarrow \frac{f(\alpha)i(\alpha) - h(\alpha)g(\alpha)}{g(\alpha)i(\alpha)} \neq 0$$
$$\Rightarrow \phi\left(\frac{f(t)i(t) - h(t)g(t)}{g(t)i(t)}\right) \neq 0$$
$$\Rightarrow \frac{f(t)i(t) - h(t)g(t)}{g(t)i(t)} \neq 0$$
$$\Rightarrow \frac{f(t)i(t)}{g(t)i(t)} - \frac{h(t)g(t)}{g(t)i(t)} \neq 0$$
$$\Rightarrow \frac{f(t)}{g(t)} - \frac{h(t)}{i(t)} \neq 0$$
$$\Rightarrow \frac{f(t)}{g(t)} \neq \frac{h(t)}{i(t)}.$$

Vemos pelo modo em que ϕ foi definida, que é também sobrejetora. Donde, acabamos por ter um isomorfismo no lugar de um monomorfismo como havíamos mostrado. Além disso, $\phi|_K$ é a identidade, ou seja, ϕ define um isomorfismo de extensões. Finalmente, $\phi(t) = \alpha$. □

Teorema 5.3.2. *Seja $K(\alpha) : K$ uma extensão algébrica simples, e seja m o polinômio minimal de α sobre K. Então $K(\alpha) : K$ é isomórfico a $\frac{K[t]}{\langle m \rangle}$. O isomorfismo $\frac{K[t]}{\langle m \rangle}$ pode ser escolhido para associar t a α(ser a identidade sobre K).*

Demonstração. O isomorfismo em questão é definido por $[p(t)] \to p(\alpha)$, uma vez que, de modo análogo a demonstração do teorema anterior conseguimos mostrar o monomorfismo e a sobrejeção; e ainda a boa definição, já que $p(\alpha) = 0$ se, e somente se, $m|p$. Resta agora, mostrarmos que este é a identidade quando restrito a K, mas isto e nítido pela definição. □

Corolário 5.3.3. *Suponha $K(\alpha) : K$ e $K(\beta) : K$ extensões algébricas simples, tais que α e β tenham o mesmo polinômio minimal m sobre K. Então, estas duas extensões são isomorfas, e o isomorfismo de corpos maiores, pode ser entendido como uma função de α para β (e como a identidade sobre K).*

Demonstração. Pelo teorema anterior, sabemos que ambas extensões são isomorfas a $\frac{K[t]}{\langle m \rangle}$, e que tais isomorfismos associam t a α e t a β, respectivamente. Consideremos ι e j como sendo respectivamente tais isomorfismos. Assim, ao considerarmos $j\iota^{-1}$, temos um isomorfismo de $K(\alpha)$ em $K(\beta)$, exatamente como desejávamos. □

Lema 5.3.4. *Seja $K(\alpha) : K$ uma extensão algébrica simples, e seja m o polinômio minimal de α sobre K, e ainda $\partial m = n$. Então, $\{1, \alpha, ..., \alpha^{n-1}\}$ é uma base para $K(\alpha)$ sobre K (como veremos melhor no próximo capítulo). Em particular, $[K(\alpha) : K] = n$.*

Demonstração. Este teorema é consequência do já feito no Lema 5.2.3. □

Definição 5.3.5. *Seja $\iota : K \to L$ um monomorfismo entre corpos. Então existe uma função $\hat{\iota} : K[t] \to L[t]$ definida por,*

$$\hat{\iota}(k_0 + k_1 t + ... + k_n t^n) = \iota(k_0) + \iota(k_1)t + ... + \iota(k_n)t^n,$$

com $k_0, k_1, ..., k_n \in K$. Temos do fato de ι ser monomorfismo que $\hat{\iota}$ também o é. Assim, se ι for um isomorfismo, $\hat{\iota}$ também será.

Teorema 5.3.6. *Suponha que K e L sejam subcorpos de $\mathbb{C}$ e que $\iota : K \to L$ é um isomorfismo. Sejam $K(\alpha)$ e $L(\beta)$ extensões algébricas simples de K e L, respectivamente, tais que $m_\alpha(t)$ é o polinômio minimal de α sobre K, e $m_\beta(t)$, o polinômio minimal de β sobre L. Além disso, suponha que $m_\beta(t) = \iota(m_\alpha(t))$. Então, existe um isomorfismo $j : K(\alpha) \to L(\beta)$ tal que $j|_K = \iota$ e $j(\alpha) = \beta$.*

Demonstração. Analisemos as hipóteses do teorema no diagrama a seguir:

$$\begin{array}{ccc} K & \longrightarrow & K(\alpha) \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle j} \\ L & \longrightarrow & L(\beta) \end{array}$$

em que j ainda precisa ser determinada. Sabemos que todo elemento de $K(\alpha)$ é da forma $p(\alpha)$ para um polinômio p sobre K, cujo grau $< \partial m_\alpha$ (uso da forma reduzida). Definamos $j(p(\alpha)) = (\iota(p))(\beta)$, com $\iota(p)$ definida como no diagrama. Assim, estamos em condições de usar o Teorema 5.3.2 e concluirmos a demonstração. □

O ponto crucial do teorema acima, é que, dada uma função ι, podemos estendê-la a uma função j entre corpos maiores.

Capítulo 6

O Grau de uma Extensão

Neste capítulo associaremos o conceito de espaço vetorial a teoria de extensões de corpos, a partir do novo conceito a ser abordado, o grau de uma extensão.

Teorema 6.0.7. *Se $L : K$ é uma extensão de corpos, então as operações*

$$\begin{aligned}(\lambda, u) &\mapsto \lambda u, \quad \lambda \in K, u \in L \\ (u, v) &\mapsto u + v, \quad u, v \in L\end{aligned}$$

define sobre L uma estrutura de um espaço vetorial sobre K.

Demonstração. Para mostrarmos que L é um espaço vetorial sobre K, precisamos garantir que as operações anteriormente definidas satisfazem os sete axiomas seguintes:

1. $u + v = v + u, \ \forall u, v \in L$ - comutatividade da adição;
2. $(u + v) + w = u + (v + w), \ \forall u, v, w \in L$ - associatividade da adição;
3. Existe um elemento em L, que chamaremos de 0, tal que $0 + u = u, \ \forall u \in L$ - existência do elemento neutro da adição;
4. Para todo $u \in L$, existe $-u \in L$, de modo que $u + (-u) = 0$ - existência de inverso aditivo;
5. Se $\lambda \in K$, e $u, v \in L$, então $\lambda(u + v) = \lambda u + \lambda v$ - distributividade do escalar diante a soma de vetores;
6. Seja 1 a unidade de K, então $1u = u, \ \forall u \in L$ - elemento neutro da operação de multiplicação;
7. Se $\lambda, \mu \in K$ e $u \in L$, então $\lambda(\mu u) = (\lambda\mu)u$ - distributividade de escalares diante a um vetor.

Sabendo que $K \subseteq L$ e ambos, K e L, são subcorpos de $\mathbb{C}$, temos a partir do modo que definimos as operações claramente a validade dos sete axiomas acima, mostrando que L define um espaço vetorial sobre K. □

Para a definição a seguir precisamos lembrar que a dimensão de um espaço vetorial é o número de elementos linearmente independentes que compõem uma base para o espaço, e que o geram.

Definição 6.0.8. *O grau, $[L : K]$, de uma extensão $L : K$ é a dimensão do espaço vetorial de L sobre K.*

Exemplos 6.0.9.

1. *Notemos que a extensão $\mathbb{C} = \mathbb{R}(i) : \mathbb{R}$ tem como grau 2, uma vez que, $\{1, i\}$ é uma base para o espaço vetorial de $\mathbb{C}$ sobre $\mathbb{R}$. Portanto, $[\mathbb{C} : \mathbb{R}] = 2$;*

2. *Como já visto anteriormente, $\{1, \sqrt{5}, i, i\sqrt{5}\}$ forma uma base para o espaço vetorial $\mathbb{Q}(i, \sqrt{5})$ sobre $\mathbb{Q}$, assim, $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] = 4$.*

Notoriamente vale ressaltar, que extensões de corpos isomorfas tem o mesmo grau.

6.1 A Lei da Torre

O próximo teorema garantirá uma facilidade maior no cálculo do grau de determinadas extensões, uma vez que, permite usarmos outras, com graus já conhecidos.

Teorema 6.1.1. *Se K, L, M são subcorpos de $\mathbb{C}$, e $K \subseteq L \subseteq M$, então*

$$[M : K] = [M : L][L : K].$$

Se $[M : L]$ ou $[L : K]$ são iguais a ∞, então $[M : K] = \infty$. E ainda, se $[M : K] = \infty$, então $[M : L] = \infty$ ou $[L : K] = \infty$.

Demonstração. Seja $(x_i)_{i\in I}$ uma base para o espaço vetorial de L sobre K, e seja $(y_j)_{j\in J}$ uma base para o espaço vetorial de M sobre L. Deste modo, para todo $i \in I$ e todo $j \in J$, temos $x_i \in L$, $y_j \in M$. Devemos mostrar que $(x_i y_j)_{i\in I, j\in J}$ é uma base para o espaço vetorial de M sobre K (notemos que $x_i y_j$ é o produto no subcorpo M). E assim, a dimensão da base deste último espaço terá a dimensão necessária.

Para mostrarmos que $(x_i y_j)_{i\in I, j\in J}$ é uma base, devemos inicialmente mostrar que estes são linearmente independentes. Para isto, consideremos

$$\sum_{i,j} k_{ij} x_i y_j = 0, \quad k_{ij} \in K,$$

como $k_{ij} x_i \in L$ e L é um corpo, temos que $\sum_i k_{ij} x_i \in L$, podemos assim, rearranjá-la de modo a obtermos,

$$\sum_j \left(\sum_i k_{ij} x_i \right) y_j = 0.$$

Sabendo que $\sum_i k_{ij}x_i \in L$ e que y_j são linearmente independentes sobre L, temos

$$\sum_i k_{ij}x_i = 0.$$

Analogamente, como x_i são linearmente independentes sobre K, conseguimos que $k_{ij} = 0,\ \forall i \in I, j \in J$. Ou seja, os elementos x_iy_j são linearmente independentes sobre K.

Resta-nos mostrar que qualquer elemento do espaço vetorial de M sobre K pode ser escrito como soma destes elementos.

Seja $x \in M$, qualquer. Temos,

$$x = \sum_j \lambda_j y_j,$$

para $\lambda_j \in L$, já que, $(y_j)_{j\in J}$ é uma base para o espaço vetorial de M sobre L.

Pensando do mesmo modo, temos que por $(x_i)_{i\in I}$ ser uma base para o espaço vetorial de L sobre K, podemos escrever λ_j para todo $j \in J$, como,

$$\lambda_j = \sum_i \lambda_{ij}x_i$$

para $\lambda_{ij} \in K$. Juntando o feito, conseguimos,

$$x = \sum_{i,j} \lambda_{ij}x_iy_j$$

como queríamos.

Assim, $(x_iy_j)_{i\in I, j\in J}$ é uma base para o espaço vetorial de M sobre K, e sua dimensão é exatamente a que diz o teorema. □

Exemplo 6.1.2. *Encontremos o grau da extensão* $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}]$. *Notemos que* $\{1, \sqrt{2}\}$ *é uma base para o espaço vetorial* $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$. *Vejamos isto melhor, dado* $\alpha \in \mathbb{Q}(\sqrt{2})$, *temos que* $\alpha = p+q\sqrt{2}$, *com* $p, q \in \mathbb{Q}$. *Ou seja,* $\{1, \sqrt{2}\}$ *realmente gera o espaço vetorial de* $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$. *Resta agora mostramos que,* 1 *e* $\sqrt{2}$ *são linearmente independentes sobre* $\mathbb{Q}$. *Suponhamos que* $p + q\sqrt{2} = 0$, *e mais que* $q \neq 0$. *Assim, conseguimos que* $\sqrt{2} = \frac{-p}{q}$, *isto é,* $\sqrt{2} \in \mathbb{Q}$, *o que é um absurdo, portanto,* $q = 0$. *Como* $q = 0$ *temos necessariamente que* $p = 0$, *donde vemos que estes,* 1 *e* $\sqrt{2}$, *são linearmente independentes sobre* $\mathbb{Q}$. *Logo, juntando as informações conseguimos que* $\{1, \sqrt{2}\}$ *é uma base de* $\mathbb{Q}(\sqrt{2})$ *sobre* $\mathbb{Q}$.

Analogamente, mostramos que $\{1, \sqrt{3}\}$ *é uma base para o espaço vetorial* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *sobre* $\mathbb{Q}(\sqrt{2})$.

Portanto, como $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$*, temos pela lei da torre,*

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

Assim, temos a combinação das bases $\{1, \sqrt{2}\}$ *e* $\{1, \sqrt{3}\}$ *gerando a base* $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *do espaço vetorial* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *sobre* $\mathbb{Q}$*.*

Corolário 6.1.3 (Lei da Torre)**.** *Se* $K_0 \subseteq K_1 \subseteq ... \subseteq K_n$ *são subcorpos de* $\mathbb{C}$*, então*

$$[K_n : K_0] = [Kn : K_{n-1}][K_{n-1} : K_{n-2}]...[K_1 : K_0].$$

Demonstração. Para provarmos a afirmação, basta usarmos o teorema anterior e indução sobre n. □

Proposição 6.1.4. *Seja* $K(\alpha) : K$ *uma extensão simples. Se esta, é transcendente, então* $[K(\alpha) : K] = \infty$*. Se a extensão é algébrica, então* $[K(\alpha) : K] = \partial m$*, em que* m *é o polinômio minimal de* α *sobre* K*.*

Demonstração. Para o caso transcendente, é suficiente mostrarmos que $1, \alpha, \alpha^2, ...$ são linearmente independente sobre K. Já para o caso algébrico, utilizamos o Lema 5.3.4 para concluirmos o dito. □

Exemplo 6.1.5. *Procuremos descobrir o grau da extensão de* $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ *sobre* $\mathbb{Q}$*, isto é,* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}]$*.*

Usemos a lei das torres, donde por $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$*, temos*

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

Percebemos que cada um dos fatores é igual a dois, porém é necessário demonstrarmos isto.

(a) Pelo que vimos no Exemplo 6.1.2, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$*.*

(b) Ainda pelo Exemplo 6.1.2, temos que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$*. Porém mostremos um pouco melhor. Suponhamos que* $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ *(pois se concluirmos um absurdo, teremos claramente o grau da extensão como sendo 2), assim*

$$\begin{aligned}\sqrt{3} &= p + q\sqrt{2}, \qquad p, q \in \mathbb{Q} \\ \Rightarrow 3 &= (p^2 + 2q^2) + 2pq\sqrt{2} \\ &\Rightarrow p^2 + 2q^2 = 3 \quad e \quad pq = 0\end{aligned}$$

Se $p = 0$, então $2q^2 = 3$, ou seja, $q = \frac{1}{\sqrt{2}}\sqrt{3} \notin \mathbb{Q}$; da mesma forma se $q = 0$ conseguimos uma impossibilidade com $p^2 = 3$. Donde, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, e $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}] = 2$.

(c) Finalmente, afirmamos que $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Suponhamos por absurdo, que

$$\sqrt{5} = p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6}, \quad p, q, r, s \in \mathbb{Q},$$

isto é, que $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Elevando ao quadrado,

$$5 = p^2 + 2q^2 + 3r^2 + 6s^2 + (2pq + 6rs)\sqrt{2} + (2pr + 4qs)\sqrt{3} + (2ps + 2qr)\sqrt{6},$$

portanto,

$$\begin{aligned} p^2 + q^2 + 3r^2 + 6s^2 &= 5 && (6.1)\\ pq + 3rs &= 0 && (6.2)\\ pr + 2qs &= 0 && (6.3)\\ ps + qr &= 0. && (6.4) \end{aligned}$$

Observemos que se (p, q, r, s) satisfaz (6.1), então $(p, q, -r, -s), (p, -q, r, -s)$, e $(p, -q, -r, s)$ também satisfazem. Logo,

$$\begin{aligned} p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6} &= \sqrt{5}\\ p + q\sqrt{2} - r\sqrt{3} - s\sqrt{6} &= \pm\sqrt{5}\\ p - q\sqrt{2} + r\sqrt{3} - s\sqrt{6} &= \pm\sqrt{5}\\ p - q\sqrt{2} - r\sqrt{3} + s\sqrt{6} &= \pm\sqrt{5}. \end{aligned}$$

Somando as duas primeiras equações acima, conseguimos $p + q\sqrt{2} = \sqrt{5}$, o que implica em $p = q = 0$. Somando agora, a primeira com a terceira equação, $r\sqrt{3} = 0$ ou $r\sqrt{3} = \sqrt{5}$, e então $r = 0$. Finalmente, $s = 0$, já que $s\sqrt{6} = \sqrt{5}$ é impossível.

Provada as afirmações, podemos deduzir que,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2,$$

donde concluímos que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$.

Definição 6.1.6. *Uma extensão finita é aquela cujo grau é finito.*

Exemplo 6.1.7. *Só a partir da Proposição 6.1.4 temos um grande número de extensões finitas.*

Definição 6.1.8. *Uma extensão $L : K$ é algébrica se todo elemento de L é algébrico sobre K.*

Lema 6.1.9. *$L : K$ é uma extensão finita, se, e somente se, L é algébrico sobre K e existe finitamente muitos elementos $\alpha_1, ..., \alpha_n \in L$ tais que $L = K(\alpha_1, ..., \alpha_n)$.*

Demonstração. Utilizando indução, o Teorema 6.1.1 e a Proposição 6.1.4, temos que qualquer extensão algébrica $K(\alpha_1, ..., \alpha_s) : K$ é finita. Consideremos agora $L : K$ uma extensão finita. Então, existe uma base $\{\alpha_1, ..., \alpha_s\}$ para o espaço vetorial de L sobre K. Assim, $L = K(\alpha_1, ..., \alpha_s)$. Donde nos resta apenas mostrar que $L : K$ é algébrica. Seja x um elemento qualquer de L, e $n = [L : K]$.

O conjunto $\{1, x, ..., x^n\}$ tem $n + 1$ elementos, e portanto, deve ser um conjunto linearmente dependente (a base deste espaço contém exatos n elementos) sobre K. Assim,

$$k_0 + k_1 x + ... + k_n x^n = 0, \quad k_0, k_1, ..., k_n \in K,$$

e x é algébrico sobre K. Como este é genérico, temos que a extensão é do tipo algébrico sobre K. □

Capítulo 7

Construções com Régua e Compasso

Problemas como as impossibilidades geométricas (duplicação do volume do cubo, quadratura do círculos e trissecção de um ângulo), com as quais os gregos se depararam, serão agora discutidos através do uso da importante ferramenta - o grau de uma extensão.

7.1 Formulação Algébrica

Devemos iniciar formulando a ideia de construção a partir dos instrumentos régua e compasso.

Consideremos que P_0 seja um conjunto de pontos do plano $\mathbb{R}^2$, obtidos por meio da teoria geométrica euclidiana. E mais, assumamos que nossas operações sejam do tipo:

- **Régua:** Através dois pontos de P_0 desenhamos uma linha reta.
- **Compasso:** Desenhamos um círculo cujo centro é um ponto de P_0 e o raio é igual a distância entre um par de pontos também de P_0.

Definição 7.1.1. *Os pontos de intersecção de qualquer duas retas distintas, ou círculos, desenhados a partir as operações de Régua e Compasso, são ditos construíveis de P_0. Mais geralmente, um ponto $r \in \mathbb{R}^2$ é construível de P_0, se há uma sequência $r_1, ..., r_n = r$ de pontos de $\mathbb{R}^2$, tais que para cada $j = 1, ..., n$ dos pontos r_j é construível a partir do conjunto $P_0 \cup \{r_1, ..., r_{j-1}\}$.*

Exemplo 7.1.2. *Suponhamos dados os pontos $P_1, P_2 \in \mathbb{R}^2$. Assim, consideremos $P_0 = \{P_1, P_2\}$. Desenhemos o ponto médio do segmento de extremos em P_1 e P_2. Para isto, seguimos os seguintes passos:*

1. *Existe uma reta passando pelos pontos P_1, P_2, desenhe-na (operação da Régua);*
2. *Com auxílio do compasso, desenhe o círculo com centro em P_1 e raio dado pela distância de P_1 a P_2;*

3. *Novamente com a operação compasso, desenhamos o círculo de centro em P_2 e raio $dist(P_1, P_2)$;*

4. *Sejam R_1, R_2 os pontos de intersecção das circunferências;*

5. *Tracemos a reta passando por R_1 e R_2 - operação com a Régua;*

6. *Chamemos de R_3 o ponto de intersecção entre a reta P_1P_2 e a reta R_1R_2.*

Afirmemos que R_3 é o ponto médio procurado. De fato, desenhemos o triângulo de vértices P_1, P_2 e R_1 e analisemos a semelhança de triângulos entre os dois que o forma, concluindo assim a afirmação feita.

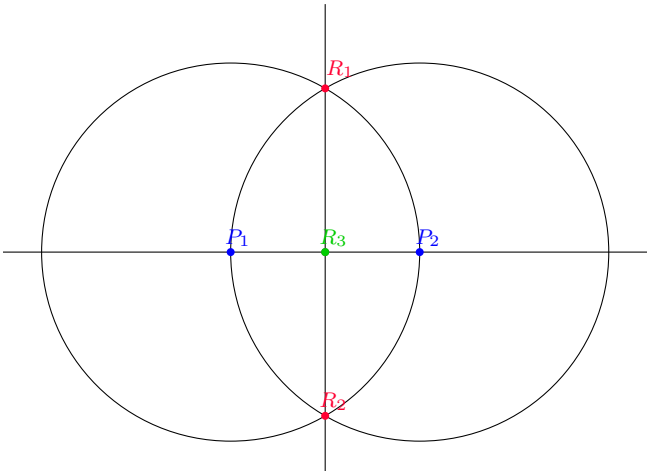

Figura 7.1: A construção do ponto médio do segmento P_1P_2

A chave para o entendimento das limitações das construções por régua e compasso está relacionada a ideia de extensões de corpos (como comentamos brevemente no início do capítulo). Há uma maneira natural para fazermos isto. A cada estágio da construção, associamos o subcorpo de $\mathbb{C}$ gerado pelas coordenadas dos pontos construídos, que é também um subcorpo de $\mathbb{R}$. Então, seja K_0 o subcorpo de $\mathbb{R}$ gerado por x, y coordenadas dos pontos em P_0. Se r_j tem coordenadas (x_j, y_j), então indutivamente definimos K_j como o corpo obtido de K_{j-1} adicionando x_j e y_j, ou seja,

$$K_j = K_{j-1}(x_j, y_j).$$

Notemos que não estamos adicionando o ponto (x_j, y_j) a K_{j-1}, estamos na verdade adicionando o conjunto $\{x_j, y_j\}$ formado pelas duas coordenadas do ponto.

Temos deste modo, a seguinte torre de subcorpos,

$$K_0 \subseteq K_1 \subseteq ... \subseteq K_n \subseteq \mathbb{R},$$

e usamo-na para obtermos um critério de construtividade.

Lema 7.1.3. *Com a notação acima, x_j e y_j são zeros em K_j dos polinômios quadráticos sobre K_{j-1}.*

Demonstração. Temos três casos a considerar: encontro de retas, encontro de retas com circunferências, e encontro entre circunferências. Cada caso é demonstrado por meio da geometria, para tanto faremos apenas um destes, o caso de encontro entre reta e circunferência.

Sejam A, B, C pontos de coordenadas $(p, q), (r, s), (t, u)$ em K_{j-1}. Desenhemos a reta passando pelos pontos A e B, e também a circunferência de centro em C e raio w. Sabemos que $w^2 \in K_{j-1}$, pois w é a distância entre dois pontos cujas coordenadas estão em K_{j-1}. Para ver isto, podemos usar a semelhança entre os triângulos ACX e ADB, como ilustrado na Figura 7.2, obtendo a seguinte equação da reta que passa pelos pontos A e B:

$$\frac{x-p}{r-p} = \frac{y-q}{s-q}.$$

Por outro lado, a equação da circunferência é

$$(x-t)^2 + (y-u)^2 = w^2.$$

Resolvendo estas duas equações simultâneas, chegamos a seguinte expressão:

$$(x-t)^2 + \left(\frac{(s-q)}{(r-p)}(x-p) + q - u\right)^2 = w^2,$$

a partir da qual podemos ver claramente que a coordenada x da intersecção dos pontos X e Y são exatamente os zeros de um polinômio quadrático sobre K_{j-1}, e o mesmo é válido para a coordenada y. Esta situação encontra-se ilustrada na Figura 7.3.

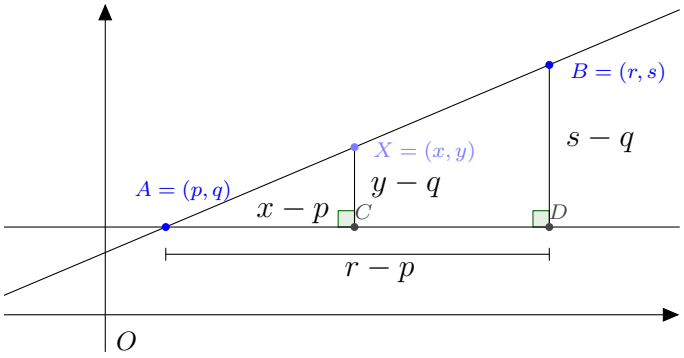

Figura 7.2: Equação da reta AB obtida por meio da semelhança de triângulos

□

Teorema 7.1.4. *Se $r = (x, y)$ é construtível a partir de um subconjunto de P_0 de $\mathbb{R}^2$, e K_0 é um subcorpo de $\mathbb{R}$ gerado pelas coordenadas dos pontos de P_0, então os graus*

$$[K_0(x) : K_0] \quad e \quad [K_0(y) : K_0]$$

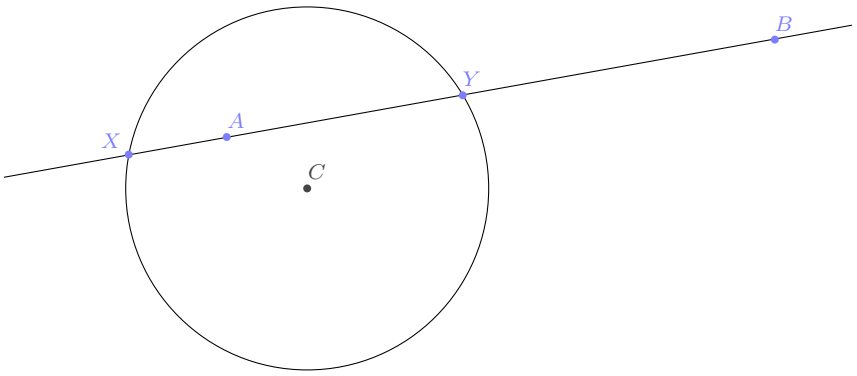

Figura 7.3: A construção de pontos a partir de pontos como intersecção da reta AB com o círculo de centro C e raio w dados

são potências de 2.

Demonstração. Com a mesma notação de antes, temos pelo Lema 7.1.3 e pela Proposição 6.1.4,

$$[K_{j-1}(x_j) : K_{j-1}] = 1 \quad \text{ou} \quad 2.$$

O valor 2 aparece se o polinômio quadrático sobre K_{j-1} que tem x_j como zero é irredutível, caso contrário o valor é 1. Similarmente,

$$[K_{j-1}(y_j) : K_{j-1}] = 1 \quad \text{ou} \quad 2$$

Portanto, pela lei da torre,

$$\begin{aligned} [K_{j-1}(x_j, y_j) : K_{j-1}] &= [K_{j-1}(x_j, y_j) : K_{j-1}(x_j)][K_{j-1}(x_j) : K_{j-1}] \\ &= 1, 2, \quad \textit{ou} \quad 4 \end{aligned}$$

Como $[K_j : K_{j-1}]$ é uma potência de 2. Temos pela lei da torre, que $[K_n : K_0]$ é também uma potência de 2. Ora,

$$[K_n : K_0(x)][K_0(x) : K_0] = [K_n : K_0]$$

e $[K_0(x) : K_0]$ é uma potência de 2. Analogamente, $[K_0(y) : K_0]$ é uma potência de 2. □

7.2 Impossibilidade de Provas

Aplicaremos neste momento a teoria discutida na seção anterior para mostrarmos a não existência de construção por meio de régua e compasso que resolva os problemas clássicos mencionados, a duplicação do cubo, a trissecção do ângulo e a quadratura do círculo.

Teorema 7.2.1 (Wantzel)**.** *O cubo não pode ser duplicado usando construções com régua e compasso.*

Demonstração. Dado um cubo de lado unitário, assumamos que $P_0 = \{(0,0),(1,0)\}$. Deste modo, $K_0 = \mathbb{Q}$, e $\sqrt{2}$, $\sqrt{3}$ que são as outras distâncias possíveis entre os vértices do cubo, podem ser obtidas a partir de P_0. Se desejamos duplicar o cubo, devemos construir o ponto $(\alpha, 0)$, em que $\alpha^3 = 2$. Assim, pelo Teorema 7.1.4 $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ deve ser uma potência de 2. Mas, α é zero do polinômio $t^3 - 2$ sobre $\mathbb{Q}$, que é irredutível pelo Critério de Eisenstein. Portanto, $t^3 - 2$ é o polinômio minimal de α sobre $\mathbb{Q}$, e devido a Proposição 6.1.4, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Como 3 não é uma potência de 2, temos uma contradição. Daí, o cubo não pode ser duplicado. □

Teorema 7.2.2 (Wantzel)**.** *O ângulo $\frac{\pi}{3}$ não pode ser trissectado usando construções com régua e compasso.*

Demonstração. Conseguimos construir o ângulo $\frac{\pi}{3}$ a partir dos pontos $(0,0)$ e $(1,0)$. Portanto, trissectar o ângulo $\frac{\pi}{3}$ é o mesmo que construir o ponto $(\alpha, 0)$, com $\alpha = \cos(\frac{\pi}{9})$. A partir disto, conseguimos construir $(\beta, 0)$, sendo $\beta = 2\cos(\frac{\pi}{9})$. De trigonometria, temos

$$\cos(3\theta) = 4\cos(\theta)^3 - 3\cos(\theta).$$

Se colocarmos $\theta = \frac{\pi}{9}$, então $\cos(3\theta) = \frac{1}{2}$, e β satisfaz a cúbica,

$$\beta^3 - 3\beta - 1 = 0.$$

Agora, $f(t) = t^3 - 3t - 1$ é irredutível sobre $\mathbb{Q}$, como

$$f(t+1) = t^3 + 3t^2 - 3$$

é irredutível pelo Critério de Eisenstein. Pelo teorema anterior, $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, uma contradição. □

Teorema 7.2.3. *Não e possível fazermos a quadratura do círculo por meio de construções com régua e compasso.*

Demonstração. Tal construção é equivalente a construirmos o ponto $(0, \sqrt{\pi})$ a partir dos pontos iniciais $P_0 = \{(0,0),(1,0)\}$. Deste conjunto, podemos facilmente construir $(0, \pi)$.

Portanto, se tal construção existir, então $[\mathbb{Q}(\pi) : \mathbb{Q}]$ é uma potência de 2, em particular, π é algébrico sobre $\mathbb{Q}$. Por outro lado, vimos, ou melhor, assumimos que π não é algébrico sobre $\mathbb{Q}$, ou seja, temos demonstrado o teorema. □

Capítulo 8

Normalidade e Separabilidade

Neste capítulo inicial discutiremos duas propriedades de certo modo complementares. Estas serão imprescendíveis para o estudo do Teorema da Correspondência de Galois, que sem sombra de dúvidas é o auge de toda esta teoria.

Suponha que K é um subcorpo de $\mathbb{C}$. Frequentemente um polinômio $p(t) \in K[t]$ não tem zeros em K. Mas, este tem zeros em $\mathbb{C}$, pelo Teorema Fundamental da Álgebra. Portanto, deve haver alguns zeros, ao menos, em alguma extensão de corpo L de K. Por exemplo, $t^2 + 1 \in \mathbb{R}[t]$ não tem zeros em $\mathbb{R}$, mas tem zeros, $\pm i$, em $\mathbb{C}$. Estudaremos este fenômeno em detalhes, mostrando que todo polinômio pode ser resolvido por um produto de fatores lineares (e, portanto, tem seus zeros) se o corpo K é suavemente extendido a um corpo N. Uma extensão $N : K$ é normal se qualquer polinômio irredutível sobre K com ao menos um zero em N, decompõe-se em fatores lineares em N. Mostraremos também que uma extensão é normal se, e somente se, é um corpo de decomposição.

Separabilidade, como já mencionado, é uma propriedade complementar a normalidade. Um polinômio irredutível é separável se seus zeros nestas divisões são simples. Isto mostra que sobre $\mathbb{C}$, tal propriedade é sempre satisfeita (diremos automática).

8.1 Corpos de Decomposição

O Teorema Fundamental da Álgebra afirma que f se decompõe sobre K se, e somente se, todos os zeros de f em $\mathbb{C}$ na verdade pertencem a K. Ou seja, K contém o subcorpo gerado por todos os zeros de f. Partiremos desta ideia de decomposição linear, um modo de tornarmos um polinômio mais tratável, para discorrermos neste capítulo sobre Normalidade, Corpo de Decomposição, Separabilidade e as Extensões de Corpos envolvendo as duas propriedades complementares que nomeiam o capítulo.

Definição 8.1.1. *Se K é um subcorpo de $\mathbb{C}$, e f é um polinômio sobre K, então f decompõe-se sobre K, se este pode ser expresso por um produto de fatores lineares,*

$$f(t) = k(t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n),$$

em que, $k, \alpha_1, \ldots, \alpha_n \in K$.

Se este é o caso, então os zeros de f em K são precisamente $\alpha_1, \ldots, \alpha_n$.

Exemplos 8.1.2. *1. O polinômio* $f(t) = t^3 - 1 \in \mathbb{Q}[t]$ *se decompõe sobre* $\mathbb{C}$*, pois pode ser escrito como*

$$f(t) = (t-1)(t-\omega)(t-\omega^2),$$

em que $\omega = \exp(\frac{2\pi i}{3}) \in \mathbb{C}$.

De modo análogo, temos que f *se decompõe sobre o subcorpo* $\mathbb{Q}(i, \sqrt{3})$*, uma vez que,* $\omega \in \mathbb{Q}(i, \sqrt{3})$.

Ainda mais, sabemos que o menor subcorpo de $\mathbb{C}$ *com a propriedade de* f *se decompor linearmente é o* $\mathbb{Q}(\omega)$.

2. O polinômio $f(t) = t^4 - 4t^2 - 5$ *se decompõe sobre* $\mathbb{Q}(i, \sqrt{5})$*, pois*

$$f(t) = (t-i)(t+i)(t-\sqrt{5})(t+\sqrt{5}).$$

Entretanto, sobre $\mathbb{Q}(i)$*, o máximo que conseguimos fazer é fatorá-lo como,*

$$(t-i)(t+i)(t^2-5),$$

com $t^2 - 5$*, fator irredutível, de grau maior do que* 1 *(notemos que* 5 *não é quadrado de nenhum um número em* $\mathbb{Q}(i)$*).*

Então, sobre $\mathbb{Q}(i)$*, o polinômio em questão não se decompõe linearmente. Assim, percebemos que um polinômio* $f(t)$ *pode ter alguns fatores lineares na extensão de corpo* L*, mas ele não necessariamente se decompõe linearmente na mesma.*

Se f é um polinômio em K e L é uma extensão de corpo de K, então f é também um polinômio sobre L. Isto, portanto, faz com que tenha sentido falar sobre f se decompor em L, significando que é um produto de fatores lineares com coeficientes em L. Mostraremos que dados K e f, podemos sempre construir uma extensão $Gal(f, K)$ de K tal que f se decompõe sobre a mesma. É conveniente requerer que f não se decomponha em qualquer corpo menor, então $Gal(f, K)$ é tão econômico quanto possível.

Definição 8.1.3. *Um subcorpo* Σ *de* $\mathbb{C}$ *é um corpo de decomposição para o polinômio* f *sobre o subcorpo* K *de* $\mathbb{C}$*, se* $K \subseteq \Sigma$ *e*

1. f *decompõe-se linearmente sobre* Σ*;*
2. *Se* $K \subseteq \Sigma' \subseteq \Sigma$ *e* f *decompõe-se linearmente sobre* Σ'*, então* $\Sigma' = \Sigma$.

Notação: *Chamaremos de* $Gal(f, K)$ *o corpo de decomposição do polinômio* f *sobre o subcorpo* K *de* $\mathbb{C}$.

Observação 8.1.4. *A segunda condição da definição anterior, 2, é equivalente à:* $Gal(f,K) = K(\sigma_1,\ldots,\sigma_n)$ *em que* $\sigma_1,\ldots,\sigma_n$ *são os zeros de* f *em* $Gal(f,K)$*. Logo, o corpo de decomposição existe (na pior das hipóteses este é o próprio* $\mathbb{C}$*), é único, e* $[Gal(f,K):K]$ *é finito (Lema 6.1.9).*

Subcorpos isomorfos de $\mathbb{C}$ têm corpos de decomposição isomorfos no sentido a seguir.

Lema 8.1.5. *Suponha que* $\iota : K \to K'$ *é um isomorfismo de subcorpos de* $\mathbb{C}$*. Seja* f *um polinômio sobre* K *e* $Gal(f,K)$ *o corpo de decomposição para* f*. Considere* L *qualquer extensão de corpo de* K' *tal que* $\iota(f)$ *decompõe-se linearmente sobre* L*. Então, existe um monomorfismo* $j : Gal(f,K) \to L$*, tal que* $j|_K = \iota$*.*

Demonstração. Temos a seguinte situação,

$$\begin{array}{ccc} K & \longrightarrow & Gal(f,K) \\ {\scriptstyle\iota}\downarrow & & \downarrow{\scriptstyle j} \\ K' & \longrightarrow & L \end{array}$$

em que j ainda precisa ser encontrada. Construiremos, assim, j por indução no grau de f. Como um polinômio sobre $Gal(f,K)$, temos que,

$$f(t) = k(t-\sigma_1)\cdots(t-\sigma_n).$$

Se m for o polinômio minimal de σ_1 sobre K, sabemos que este é um fator irredutível de f. Assim, $\iota(m)$ divide $\iota(f)$, o qual se decompõe sobre L, ou seja, sobre L,

$$\iota(m) = (t-\alpha_1)\cdots(t-\alpha_r),$$

em que $\alpha_1,\ldots,\alpha_r \in L$. Como $\iota(m)$ é irredutível sobre K', este deve ser o polinômio minimal de α_1 sobre K'. Então, pelo Teorema 5.3.6, existe um isomorfismo

$$j_1 : K(\sigma_1) \to K'(\alpha_1),$$

tal que, $j_1|_K = \iota$ e $j_1(\sigma_1) = \alpha_1$. Deste modo, $Gal(f,K)$ é o corpo de decomposição sobre $K(\sigma_1)$ do polinômio $g = \frac{f}{(t-\sigma_1)}$. Por indução, existe um monomorfismo $j : Gal(f,K) \to L$ tal que $j|_{K(\sigma_1)} = j_1$. Ora, então $j|_K = \iota$ e terminamos a demonstração. □

Teorema 8.1.6. *Seja* $\iota : K \to K'$ *um isomorfismo. Seja* $Gal(f,K)$ *o corpo de decomposição de* f *sobre* K*, e seja* $Gal'(\iota(f),K')$ *o corpo de decomposição de* $\iota(f)$ *sobre* K'*. Então, existe um isomorfismo* $j : Gal(f,K) \to Gal'(\iota(f),K')$ *tal que* $j|_K = \iota$*. Em outras palavras, as extensões* $Gal(f,K) : K$ *e* $Gal(\iota(f),K') : K'$ *são isomorfas.*

Demonstração. Comecemos pelo diagrama,

$$\begin{array}{ccc} K & \longrightarrow & Gal(f,K) \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle j} \\ K' & \longrightarrow & Gal(\iota(f),K') \end{array}$$

Devemos, deste modo, encontrar j para que o diagrama acima comute.

Pelo Lema 8.1.5, sabemos que existe um monomorfismo $j : Gal(f,K) \to Gal(\iota(f),K')$ tal que $j|_K = \iota$. Ora, $j(Gal(f,K))$ é claramente o corpo de decomposição de $\iota(f)$ sobre K', e está contido em $Gal(\iota(f),K')$. Como $Gal(\iota(f),K')$ é também o corpo de decomposição para $\iota(f)$ sobre K', nós temos por definição, 2, que $j(Gal(f,K)) = Gal(\iota(f),K')$, donde conseguimos j sobrejetora. Portanto, j é na verdade um isomorfismo (j já era um monomorfismo, portanto, injetora). □

Exemplos 8.1.7. *1. Seja $f(t) = (t^2-3)(t^3-1)$ sobre $\mathbb{Q}$. Este decompõe-se do seguinte modo:*

$$f(t) = (t+\sqrt{3})(t-\sqrt{3})(t+1)\left(t-\frac{1+i\sqrt{3}}{2}\right)\left(t-\frac{1-i\sqrt{3}}{2}\right).$$

Logo, o corpo de decomposição de f em $\mathbb{C}$ é:

$$\mathbb{Q}\left(\sqrt{3},\frac{1+i\sqrt{3}}{2}\right) = \mathbb{Q}(\sqrt{3},i).$$

2. Seja $f(t) = (t^2-2t-2)(t^2+1)$ sobre $\mathbb{Q}$. Os zeros de f em $\mathbb{C}$ são $1\pm\sqrt{3}$, $\pm i$, e então, o corpo de decomposição é denotado por $\mathbb{Q}(1+\sqrt{3},i) = \mathbb{Q}(\sqrt{3},i)$. (Observemos que corpo de decomposição é o mesmo do polinômio no item anterior, embora estes sejam distintos).

3. É possível ter dois polinômios <u>irredutíveis</u> distintos com o mesmo corpo de decomposição. Por exemplo, t^2-3 e t^2-2t-2 são ambos irredutíveis sobre $\mathbb{Q}$, e ambos têm $\mathbb{Q}(\sqrt{3})$ como corpo de decomposição sobre $\mathbb{Q}$.

8.2 Normalidade

Definição 8.2.1. *Uma <u>extensão</u> $L:K$ é <u>normal</u> se todo polinômio irredutível f sobre K que tem ao menos um zero em L se decompõe linearmente em L.*

Exemplo 8.2.2. $\mathbb{C} : \mathbb{R}$ *é normal já que todo polinômio (irredutível ou não) se decompõe em* $\mathbb{C}$ *(Teorema Fundamental da Álgebra). Por outro lado, se considerarmos* $\alpha = \sqrt[3]{2}$ *e a extensão* $\mathbb{Q}(\alpha) : \mathbb{Q}$*, teremos um exemplo de extensão que não é normal. Ora, o polinômio irredutível* $t^3 - 2$ *tem um zero, o* α*, em* $\mathbb{Q}(\alpha)$*, mas este não se decompõe linearmente em* $\mathbb{Q}(\alpha)$ *(se o fizesse, deveria existir três raízes cúbicas de dois em* $\mathbb{Q}(\alpha)$*, não todas iguais, o que sabemos ser um absurdo, já que as outras são complexas).*

Teorema 8.2.3. *Uma extensão de corpo* $L : K$ *é normal e finita se, e somente se,* L *é um corpo de decomposição para algum polinômio sobre* K*.*

Demonstração. Suponhamos a priori que $L : K$ é normal e finita, logo, pelo Lema 6.1.9, $L = K(\alpha_1, \ldots, \alpha_s)$ para certos α_j algébricos sobre K. Seja m_j o polinômio minimal de α_j sobre K, e $f = m_1 \cdots m_s$. Cada m_j é irredutível sobre K e tem um zero, $\alpha_j \in L$. Então, por normalidade, m_j decompõe-se linearmente sobre L. Deste modo, f decompõe-se linearmente sobre L. Como L é gerado por K e pelos zeros de f, este é o corpo de decomposição de f sobre K.

Suponhamos agora que L seja o corpo de decomposição para algum polinômio g sobre K. A extensão $L : K$ é assim obviamente finita; devemos mostrar que é normal. Para fazermos isto, precisamos tomar um polinômio irredutível f sobre K, com um zero em L, e mostrar que este se decompõe linearmente em L. Consideremos $M \supseteq L$ um corpo de decomposição para fg sobre K. Suponhamos que θ_1 e θ_2 são zeros de f em M. Por irredutibilidade, f é o polinômio minimal de θ_1 e θ_2 sobre K.

Afirmamos que

$$[L(\theta_1) : L] = [L(\theta_2) : L].$$

Consideremos os seguintes subcorpos: $K, L, K(\theta_1), L(\theta_1), K(\theta_2), L(\theta_2)$ de M tais que,

$$K \subseteq K(\theta_1) \subseteq L(\theta_1) \subseteq M,$$

$$K \subseteq K(\theta_2) \subseteq L(\theta_2) \subseteq M.$$

Obviamente, $K \subseteq K(\theta_j)$ e $L \subseteq L(\theta_j)$, $(j = 1, 2)$, e $K \subseteq L \subseteq M$. A afirmação seguirá do simples cálculo dos graus das extensões destas torres. Para $j = 1$ ou 2,

$$[L(\theta_j) : L] \cdot [L : K] = [L(\theta_j) : K] = [L(\theta_j) : K(\theta_j)] \cdot [K(\theta_j) : K] \tag{8.1}$$

Pela Proposição 6.1.4, $[K(\theta_1) : K] = [K(\theta_2) : K]$. Claramente, $L(\theta_j)$ é o corpo de decomposição de g sobre $K(\theta_j)$, e pelo Corolário 5.3.3, $K(\theta_1)$ é isomorfo a $K(\theta_2)$. Portanto, pelo Teorema 8.1.6, as extensões $L(\theta_j) : K(\theta_j)$ são isomorfas para $j = 1, 2$, e assim, têm o mesmo grau. Substituindo em (8.1) e fazendo os devidos cancelamentos,

$$[L(\theta_1) : L] = [L(\theta_2) : L],$$

como afirmado. Tendo obtido alguns resultados técnicos difíceis esperamos que o restante desta discussão seja mais fácil. Ora, se $\theta_1 \in L$, então $[L(\theta_1) : L] = 1$, e também $[L(\theta_2) : L] = 1$ e $\theta_2 \in L$. Logo, $L : K$ é normal. □

8.3 Separabilidade

O conceito de separabilidade não aparece explicitamente nos trabalhos de Galois, pois ele preocupou-se apenas com o corpo dos complexos, em que a separabilidade é automática. Entretanto, o conceito está implícito em muitas demonstrações, e deve ser invocado quando estudamos corpos mais gerais.

Definição 8.3.1. *Um polinômio irredutível f sobre um subcorpo K de $\mathbb{C}$ é separável sobre K se tem apenas zeros simples em $\mathbb{C}$.*

Observação 8.3.2. *Isto é o mesmo que f possuir apenas zeros simples no seu corpo de decomposição, pois este é um subcorpo de $\mathbb{C}$. Portanto, se f é separável, ele é da forma*

$$f(t) = k(t - \sigma_1) \cdots (t - \sigma_n), \tag{8.2}$$

em que os $\sigma_j \in \mathbb{C}$ são todos distintos.

A recíproca pode não ser verdadeira, por exemplo, o polinômio $f(t) = (t^3 - 1)(t^2 - 2)$ se fatora como em 8.2 sobre $\mathbb{C}$, porém não é irredutível sobre $\mathbb{Q}$, logo, não é separável sobre este.

Exemplo 8.3.3. *Os zeros de $t^4 + t^3 + t^2 + t + 1$ são os números complexos:*

$$\exp\left(\frac{2\pi i}{5}\right), \exp\left(\frac{4\pi i}{5}\right), \exp\left(\frac{6\pi i}{5}\right), \exp\left(\frac{8\pi i}{5}\right).$$

Logo, como estes são todos e simples, f é separável sobre $\mathbb{Q}$.

Para polinômios sobre $\mathbb{R}$, há um método padrão, para detectarmos os zeros múltiplos por diferenciação. Para obtermos o máximo de generalidade, definiremos derivada de maneira puramente formal.

Definição 8.3.4. *Suponhamos que K seja um subcorpo de $\mathbb{C}$, e*

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n \in K[t].$$

Então, a derivada formal de f é o polinômio

$$Df = a_1 + 2a_2 t + \ldots + n a_n t^{n-1} \in K[t].$$

Para $K = \mathbb{R}$ (e ainda $K = \mathbb{C}$), esta é a derivada usual. Não há, em geral, razão para pensarmos em Df como a taxa de variação de f, mas certamente as propriedades de

derivação valem para D. Em particular, simples cálculos mostram que para todo polinômio f e g sobre $K[t]$,

$$D(f+g) = Df + Dg,$$

$$D(fg) = (Df)g + f(Dg).$$

Também, se $\lambda \in K$, então $D(\lambda) = 0$, e assim,

$$D(\lambda f) = \lambda(Df).$$

Estas propriedades de D permitem estabelecermos critérios para existência de zeros múltiplos sem sabermos quem os são.

Lema 8.3.5. *Seja $f \neq 0$ um polinômio sobre um subcorpo K de $\mathbb{C}$, e seja $Gal(f,K)$ seu corpo de decomposição. Então, f tem um zero múltiplo (em $\mathbb{C}$ ou em $Gal(f,K)$) se, e somente se, f e Df tem um fator comum de grau maior do que ou igual a 1 em $Gal(f,K)[t]$. Ou seja, f é separável sobre K se, e somente se, f é irredutível sobre K e primo com Df.*

Demonstração. Suponhamos que f tenha um zero repetido em $Gal(f,K)$, então sobre $Gal(f,K)$,

$$f(t) = (t-\alpha)^2 g(t),$$

em que $\alpha \in Gal(f,K)$. Assim,

$$Df = 2(t-\alpha)g(t) + (t-\alpha)^2 Dg = (t-\alpha)[(t-\alpha)Dg + 2g].$$

Donde, f e Df tem o fator $(t-\alpha) \in Gal(f,K)[t]$ em comum. Portanto, f e Df tem um fator comum em $K[t]$, chamado, de o polinômio minimal de α sobre K.

Agora, suponhamos que f não tenha zeros repetidos. Mostraremos, por indução no grau de f, que f e Df são primos entre si em $Gal(f,K)[t]$, portanto, também o são em $K[t]$. Se $\partial f = 1$, isto é óbvio, pois $f = t - \alpha$ e $Df = 1$. Por outro lado, $f(t) = (t-\alpha)g(t)$ onde $(t-\alpha) \nmid g(t)$. Então,

$$Df = (t-\alpha)Dg + g.$$

Se um fator irredutível de g divide Df, então este deve também dividir Dg, já que não divide $(t-\alpha)$. Mas, por hipótese de indução, g e Dg são primos entre si. Portanto, f e Df são primos entre si, como queríamos. □

Provaremos agora que a separabilidade em polinômios irredutíveis é uma propriedade automática em $\mathbb{C}$.

Proposição 8.3.6. *Se K é um subcorpo de $\mathbb{C}$, então toda polinômio irredutível sobre K é separável.*

Demonstração. Um polinômio irredutível f sobre K é inseparável se, e somente se, f e Df têm um fator comum de grau maior ou igual a 1 (Lema 8.3.5). Se isto, então como f é irredutível, o fator comum entre estes deve ser f. Mas, Df tem grau menor do que f, e o único múltiplo de f de grau menor é 0, donde $Df = 0$. Portanto, se

$$f(t) = a_0 + \ldots + a_n t^n,$$

temos que $na_n = 0$ para todos os inteiros $n > 0$. Para subcorpos de $\mathbb{C}$, isto é equivalente a $a_n = 0, \forall n$. □

Capítulo 9

Automorfismos de Corpos

Este capítulo contemplará os conceitos de K-automorfismo, a partir de generalização de K-monomorfismo, e o, de Fecho Normal de uma extensão finita. O primeiro é fundamental para a ideia de Grupo de Galois de uma determinada extensão, enquanto o segundo permite-nos construirmos extensões normais dada uma extensão finita.

9.1 K- Monomorfismos

Começaremos a generalizar o conceito de K-automorfismo de um subcorpo L de $\mathbb{C}$ exigindo à sobrejetividade além da injetividade em um K-monomorfismo.

Definição 9.1.1. *Suponhamos que K seja um subcorpo dos subcorpos M e L de $\mathbb{C}$. Assim, um K-monomorfismo de M em L é um monomorfismo $\Phi : M \to L$, tal que, $\Phi(k) = k$ para todo $k \in K$.*

Exemplo 9.1.2. *Consideremos $K = \mathbb{Q}$, $M = \mathbb{Q}(\alpha)$, em que $\alpha = \sqrt[3]{2}$, e $L = \mathbb{C}$. Podemos definir um K-monomorfismo $\Phi : M \to L$, colocando $\Phi(\alpha) = \omega\alpha$, onde $\omega = \exp\left(\frac{2\pi i}{3}\right)$. Como sabemos, todo elemento de M é da forma $p+q\alpha+r\alpha^2$, em que, $p, q, r \in \mathbb{Q}$. Assim,*

$$\Phi(p + q\alpha + r\alpha^2) = p + q\omega\alpha + r\omega^2\alpha^2.$$

Como α e $\omega\alpha$ têm o mesmo polinômio minimal, $t^3 - 2$, o Corolário 5.3.3 nos garante que Φ é um K-monomorfismo.

Notemos que há ainda outros dois K-monomorfismos de M em L para o caso. Um é a identidade, e o outro leva α em $\omega^2\alpha$.

O teorema a seguir será responsável por nos auxiliar na construção de K-automorfismos.

Teorema 9.1.3. *Suponhamos que $L : K$ seja uma extensão normal e finita, e que $K \subseteq M \subseteq L$ (assim, pela Lei das Torres, $[L : K] = [L : M] \cdot [M : K]$). Seja τ um K-monomorfismo de M em L. Então, existe um K-automorfismo σ de L tal que $\sigma|_M = \tau$.*

Demonstração. Como $L : K$ é uma extensão normal e finita, o Teorema 8.2.3 nos diz que L é o corpo de decomposição de algum polinômio f sobre K. Portanto, este também é o corpo de decomposição de f sobre M (ora, $K \subseteq M$ e os coeficientes de f estão em K, logo, eles também estão em M), e, de $\tau(f)$ sobre $\tau(M)$. Mas, $\tau|_K$ é a identidade, então $\tau(f) = f$. Assim, conseguimos o seguinte diagrama,

$$\begin{array}{ccc} M & \xrightarrow{\tau} & L \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\sigma} \\ \tau(M) & \longrightarrow & L \end{array}$$

Precisamos agora encontrar tal σ. Para isto, utilizaremos o Teorema 8.1.6, que garante a existência de um isomorfismo $\sigma : L \to L$ tal que $\sigma|_M = \tau$. Deste modo, σ é um automorfismo de L, e como $\sigma|_K = \tau|_K$, e este é a identidade, σ é um K-automorfismo de L. □

Proposição 9.1.4. *Suponhamos que $L : K$ seja uma extensão normal e finita, e α, β sejam os zeros em L do polinômio irredutível p sobre K. Então, existe um K-automorfismo σ de L tal que,*

$$\sigma(\alpha) = \beta.$$

Demonstração. Aplicando o Corolário 5.3.3, temos a existência de um isomorfismo $\tau : K(\alpha) \to K(\beta)$, de modo que, $\tau|_K$ seja a identidade e $\tau(\alpha) = \beta$. Assim, pelo Teorema 9.1.3 conseguimos estender τ a um K-automorfismo σ de L. □

9.2 Corpos Intermediários: Corpos Fixos e Grupos de Galois - Uma olhadela

Nesta seção teremos um breve contato com estes dois conceitos, Corpos Fixos e Grupos de Galois de uma extensão, que serão retomados ou referidos daqui em diante.

Definição 9.2.1. *Se $L : K$ é uma extensão de corpo, chamamos de corpo intermediário todo corpo M tal que $K \subseteq M \subseteq L$.*

A cada corpo intermediário M, associamos o grupo $M^* = Gal(L : M)$ de todos os M-automorfismos de L. Então K^* é o grupo de Galois $Gal(L : K)$ e $L^* = \{1\}$, ou seja, o grupo contendo apenas a aplicação identidade em L.

Proposição 9.2.2. *Se $M \subseteq N$, então $M^* \supseteq N^*$.*

Demonstração. Nesta demonstração, basta notarmos que todo automorfismo de L que fixa os elementos de N também fixa os elementos de M, ou seja, é um automorfismo de M. □

A cada subgrupo H de $Gal(L:K)$, associamos o conjunto $H^\dagger = \{x \in L \ / \ \varphi(x) = x, \forall\ \varphi \in H\}$ e este é um corpo intermediário, como veremos pelo seguinte resultado:

Lema 9.2.3. *Se H é um subgrupo de $Gal(L:K)$, então $H^\dagger$ é um subcorpo de L que contém K.*

Demonstração. Sejam $x, y \in H^\dagger$ e $\varphi \in H$. Então $\varphi(x+y) = \varphi(x)+\varphi(y) = x+y$ e, assim, $x+y \in H^\dagger$. Analogamente, $H^\dagger$ é fechado para subtração, multiplicação e divisão (por elementos não nulos) e, então, $H^\dagger$ é um subcorpo de L. Como $\varphi \in Gal(L:K)$, temos $\varphi(k) = k$ para todo $k \in K$, e, portanto, $K \subseteq H^\dagger$. □

Definição 9.2.4. *De acordo com as notações anteriores, $H^\dagger$ é o corpo fixo de H.*

É fácil ver que, assim como $*$, a aplicação $\dagger$ também é uma inclusão reversa, isto é, se $H \subseteq G$, então $H^\dagger \supseteq G^\dagger$.

Proposição 9.2.5. *Sejam M um corpo intermediário e $H \leq Gal(L:K)$. Então $M \subseteq M^{*\dagger}$ e $H \subseteq H^{\dagger *}$.*

Demonstração. Para a primeira relação, temos $M^{*\dagger} = (M^*)^\dagger = \{x \in L \ / \ \varphi(x) = x, \forall\ \varphi \in M^*\}$ e isto nos mostra que $M^* = Gal(L:M)$, ou seja, se $x \in M$, então $\varphi(x) = x$ para todo $\varphi \in Gal(L:M) = M^*$, mas, isto nos diz que $x \in (M^*)^\dagger$. Portanto, $M \subseteq M^{*\dagger}$.

Para a segunda relação, temos $H^\dagger = \{x \in L \ / \ \varphi(x) = x, \forall\ \varphi \in H\}$ e isto nos mostra que $H^{\dagger *} = Gal(L:H^\dagger)$, ou seja, se $\varphi \in H$, então, como $\varphi \in Gal(L:K)$, devemos ter $\varphi(x) = x$ para todo $x \in H^\dagger$, mas, isto nos diz que $\varphi \in Gal(L:H^\dagger) = H^{\dagger *}$. Portanto, $H \subseteq H^{\dagger *}$. □

9.3 Fecho Normal

Procuraremos nesta seção recuperar a normalidade de uma extensão a tornando, se preciso, maior.

Definição 9.3.1. *Seja L uma extensão finita de K. Um fecho normal de $L:K$ é uma extensão N de L, tal que, as condições abaixo são satisfeitas,*

1. *$N:K$ é normal;*
2. *Se $L \subseteq M \subseteq N$ e $M:K$ é normal, então $M = N$.*

Assim, N é a menor extensão de L que é normal sobre K.

O teorema a seguir garante-nos ferramentas do fecho normal, e mostra-nos (em $\mathbb{C}$) que este é único.

Teorema 9.3.2. *Se $L:K$ é uma extensão finita em $\mathbb{C}$, então existe um único fecho normal $N \subset \mathbb{C}$ de $L:K$, que é uma extensão finita de K.*

Demonstração. Sejam $\{x_1, \ldots, x_r\}$ uma base de L sobre K, e m_j o polinômio minimal de x_j sobre K. Consideremos N o corpo de decomposição de $f = m_1 m_2 \cdots m_r$ sobre L, assim, N também é o corpo de decomposição de f sobre K. Portanto, $N : K$ é uma extensão normal finita pelo Teorema 8.2.3. Suponhamos que $L \subseteq P \subseteq N$ em que a extensão $P : K$ é normal. Notemos que cada polinômio m_j tem um zero $x_j \in P$, donde por normalidade f se decompõe linearmente em P. Ora, como N é o corpo de decomposição de f, temos $P = N$. Portanto, N é o fecho normal.

Suponhamos agora, que M e N sejam ambos fechos normais. O polinômio f, acima, decompõe-se linearmente em M e N, então, cada um, M e N, contém o corpo de decomposição de f sobre K. Este corpo de decomposição contém L e é normal sobre K, logo deve ser igual a M e a N. □

Exemplo 9.3.3. *Consideremos $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. Esta extensão não é normal, como já visto (Exemplo 8.2.2). Se considerarmos K como o corpo de decomposição para $t^3 - 2$ sobre $\mathbb{Q}$, contido em $\mathbb{C}$, teremos que $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$, em que, $\omega = \frac{-1+i\sqrt{3}}{2}$ (raiz da unidade).*

Podemos pensar em K como sendo $\mathbb{Q}(\sqrt[3]{2}, \omega)$. Desta forma, K é o fecho normal para $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. Assim, neste exemplo, obtivemos o fecho normal adicionando todos os zeros que faltavam.

Fechos normais permitem-nos estipular restrições na imagem de um monomorfismo.

Lema 9.3.4. *Suponhamos que $K \subseteq L \subseteq N \subseteq M$ onde $L : K$ é finita e N é o fecho normal de $L : K$. Seja τ qualquer K-monomorfismo de L em M. Então, $\tau(L) \subseteq N$.*

Demonstração. Sejam $\alpha \in L$ e m o polinômio minimal de α sobre K. Então, $m(\alpha) = 0$, e portanto, $\tau(m(\alpha)) = 0$. Mas, $\tau(m(\alpha)) = m(\tau(\alpha))$ (suponhamos que $m(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$, logo, $m(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0$, usando o fato de τ ser um K-monomorfismo, temos $\tau(m(\alpha)) = \tau(\alpha)^n + a_{n-1}\tau(\alpha)^{n-1} + \ldots + a_0 = m(\tau(\alpha)))$, donde $m(\tau(\alpha)) = 0$; e $\tau(\alpha)$ é um zero de m. Portanto, $\tau(\alpha)$ está em N, já que $N : K$ é normal. Assim, $\tau(L) \subseteq N$. □

Este resultado geralmente permite-nos restringir nossa atenção ao fecho normal de uma extensão dada quando discutimos monomorfismos. O próximo teorema, providencia uma espécie de recíproca.

Teorema 9.3.5. *Para uma extensão finita $L : K$ as afirmações a seguir são equivalentes:*

1. *$L : K$ é normal.*
2. *Existe uma extensão normal finita N de K contendo L, tal que, todo K-monomorfismo $\tau : L \to N$ é um K-automorfismo de L.*
3. *Para toda extensão finita M de K contendo L, todo K-monomorfismo $\tau : L \to M$ é um K-automorfismo de L.*

Demonstração. Provaremos (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1).

((1) $\Rightarrow$ (3)) Se $L : K$ é normal, então L é o fecho normal de $L : K$, e portanto, pelo Lema 9.3.4, $\tau(L) \subseteq L$, qualquer que seja τ, o K-monomorfismo de L em L. Mas, τ é uma função K-linear definida em um espaço vetorial de dimensão finita L sobre K, e ainda um monomorfismo.

Portanto, $\tau(L)$ tem a mesma dimensão de L, resultando em $\tau(L) = L$ e τ é, assim, um K-automorfismo de L.

((3) $\Rightarrow$ (2)) Seja N o fecho normal para $L : K$. Então, N existe pelo Teorema 9.3.2, e tem a propriedade requerida por (3).

((2) $\Rightarrow$ (1)) Suponhamos que f é qualquer polinômio irredutível sobre K com um zero $\alpha \in L$. Então, f se decompõe linearmente em N por normalidade. Se β é qualquer zero de f em N, pela Proposição 9.1.4 temos que existe um K-automorfismo σ de N tal que $\sigma(\alpha) = \beta$. Por hipótese, σ é um K-automorfismo de L, então $\beta = \sigma(\alpha) \in \sigma(L) = L$. Portanto, f se decompõe linearmente sobre L e $L : K$ é normal. □

Teorema 9.3.6. *Suponhamos que $L : K$ seja uma extensão finita de grau n. Então, existem precisamente n K- monomorfismos distintos de L no fecho normal N de $L : K$, e portanto, em, qualquer extensão normal M de K contendo L.*

Demonstração. Usaremos indução do segundo tipo em $[L : K]$. Se $[L : K] = 1$, o resultado é imediato. Suponhamos, então, que $[L : K] = k > 1$. Seja $\alpha \in L \setminus K$ com polinômio minimal m sobre K. Então,

$$\partial m = [K(\alpha) : K] = r > 1.$$

Agora, como m é um polinômio irredutível sobre um subcorpo de $\mathbb{C}$ com um zero na extensão normal N, temos que m se decompõe linearmente em N e seus zeros $\alpha_1, \ldots, \alpha_r$ são distintos. Por indução, há precisamente s $K(\alpha)$-monomorfismos distintos, $\rho_1, \ldots, \rho_0 : L \to N$, em que, $s = [L : K(\alpha)] = \frac{k}{r}$. Pela Proposição 9.1.4, existem r K-automorfismos distintos $\tau_1, \ldots, \tau_r$ de N tal que $\tau_i(\alpha) = \alpha_i$. As funções,

$$\Phi_{ij} = \tau_i \rho_j$$

nos dão $rs = k$, K-monomorfismos distintos L em N. Mostraremos que estes são todos os K-monomorfismos de L em N.

Seja $\tau : L \to N$ um K-monomorfismo. Então, $\tau(\alpha)$ é um zero de m em N, portanto, $\tau(\alpha) = \alpha_i$ para algum i. A função $\Phi = \tau_i^{-1}\tau$ é um $K(\alpha)$-monomorfismo de L em N, e assim, por indução, $\Phi = \rho_j$ para algum j. Portanto, $\tau = \tau_i \rho_j = \Phi_i j$ e o teorema está provado. □

Podemos agora calcular a ordem do Grupo de Galois de uma extensão normal finita, um resultado de extrema importância.

Corolário 9.3.7. *Se $L : K$ é uma extensão normal finita em $\mathbb{C}$, então existem precisamente $[L : K]$ K-automorfismos de L. Isto é,*

$$|Gal(L : K)| = [L : K].$$

Demonstração. A demosntração segue diretamente dos Teoremas 9.3.5 e 9.3.6. □

Teorema 9.3.8. *Seja $L : K$ uma extensão finita com Grupo de Galois G. Se $L : K$ é normal, então K é o corpo fixo de G.*

Demonstração. Seja K_0 o corpo fixo de G, e seja $[L : K] = n$. O Corolário 9.3.7 implica $|G| = n$. Pelo seguinte teorema: Seja G um subgrupo de um grupo de automorfismos de um corpo K, e seja K_0 o corpo fixo de G. Então, $[K : K_0] = |G|$ (vide [5]); temos $[L : K_0] = n$. Como $K \subseteq K_0$, devemos ter $K = K_0$ (como $K \subseteq K_0 \subseteq L$, $[L : K] = [L : K_0] \cdot [K_0 : K] \Rightarrow [K_0 : K] = 1 \Rightarrow K_0 = K$). □

Teorema 9.3.9. *Suponhamos que $K \subseteq L \subseteq M$ e $M : K$ é finita. Então, o número de K-monomorfismos distintos de L em M é no máximo $[L : K]$.*

Demonstração. Seja N o fecho normal de $M : K$. Então, $N : K$ é finita pelo Teorema 9.3.2, e todo K-monomorfismo L em M é também um K-monomorfismo L em N ($M \subseteq N$). Portanto, podemos assumir que M é uma extensão normal de K substituindo M por N. Argumentaremos, agora, por indução em $[L : K]$, como na demonstração do Teorema 9.3.6, exceto pelo fato de podermos deduzir somente que existem s' $K(\alpha)$-monomorfismos de L em N, onde $s' \leq s$ (por indução), e existem r' K-automorfismos de N, onde $r' \leq r$ (já que os zeros de m em N podem não ser distintos). O resto da demonstração segue como no Teorema 9.3.6. □

Teorema 9.3.10. *Se $L : K$ é uma extensão finita com Grupo de Galois G, tal que K é um corpo fixo de G, então $L : K$ é normal.*

Demonstração. Pelo mesmo teorema usado na demonstração do Teorema 9.3.8, temos que $[L : K] = |G| = n$, digamos. Assim, existem exatamente n K-monomorfismos distintos de L em L, denominados os elementos do Grupo de Galois.

Provaremos a normalidade usando o Teorema 9.3.5. Portanto, seja N uma extensão de K contendo L, e seja τ um K-monomorfismo de L em N. Como todo elemento do Grupo de Galois de $L : K$ define um K-monomorfismo de L em N, o Grupo de Galois providencia n K-monomorfismos de L em N, e estes são os automorfismos de L. Mas, pelo Teorema 9.3.9, existem no máximo n K-monomorfismos distintos τ', então, τ deve ser um destes monomorfismos. Portanto, τ é um automorfismo de L. Finalmente, pelo Teorema 9.3.5, $L : K$ é normal. □

Se a correspondência de Galois é uma bijeção, então K deve ser o corpo fixo do Grupo de Galois de $L : K$, então, pelo acima visto, $L : K$ deve ser normal. Estas hipóteses são

suficientes para fazer a correspondência de Galois bijetiva (para subcorpos de $\mathbb{C}$), o que provaremos no próximo capítulo.

Capítulo 10

A Correspondência de Galois

Estamos agora em posição de estabelecer propriedades fundamentais sobre a Correspondência de Galois, entre as Extensões de Corpos e os Grupos de Galois, auge desta teoria e, portanto, deste Trabalho de Conclusão de Curso. Por sorte, a maioria do trabalho já foi feita, tudo que o que faremos neste momento é juntar as peças deste belíssimo quebra-cabeças.

10.1 O Teorema Fundamental

Seja $L : K$ uma extensão em $\mathbb{C}$ com grupo de Galois G, que consiste de todos os K-automorfismos de L. Seja $\mathcal{F}$ o conjunto dos corpos intermediários, ou seja, o conjunto dos subcorpos M tais que $K \subseteq M \subseteq L$; e seja $\mathcal{G}$ o conjunto de todos os subgrupos H de G. Definimos as seguintes funções:

$$* : \mathcal{F} \to \mathcal{G}$$

$$\dagger : \mathcal{G} \to \mathcal{F},$$

como segue: se $M \in \mathcal{F}$, então M^* é o grupo de todos os M-automorfismos de L. Se $H \in \mathcal{G}$, então $H^\dagger$ é o corpo fixo de H. Já observamos, 9.2.5, que as funções $*$ e $\dagger$ são inclusões reversas, isto é, $M \subseteq M^{*\dagger}$ e $H \subseteq H^{\dagger *}$.

Antes de enunciarmos o Teorema Fundamental da Teoria de Galois, enunciaremos e demonstraremos um Lema crucial para a demonstração das últimas partes do mesmo.

Lema 10.1.1. *Suponhamos que $L : K$ seja uma extensão de corpo, M seja um corpo intermediário, e τ, um K-automorfismo de L. Então, $\tau(M)^* = \tau M^* \tau^{-1}$.*

Demonstração. Seja $M' = \tau(M)$, e considere $\gamma \in M^*, x_1 \in M'$. Então, $x_1 = \tau(x)$ para algum $x \in M$. Calculando:

$$(\tau\gamma\tau^{-1})(x_1) = \tau(\gamma(\tau^{-1}(x_1))) = \tau(\gamma(x)) = \tau(x) = x_1.$$

Então, $\tau M^* \tau^{-1} \subset M'^*$. Analogamente, se $\gamma \in (\tau(M))^*$ e $x \in M$, temos $\tau^{-1}(\gamma(\tau(x))) = \tau^{-1}(\tau(x)) = x$ e, assim, $\tau^{-1}(\tau(M))^* \tau \subset M^*$. Agora, se $\varphi \in \tau(M)^*$, então, pelo que acabamos de provar, segue que $\psi = \tau^{-1}\varphi\tau \in M^*$ e, portanto, $\varphi = \tau(\tau^{-1}\varphi\tau)\tau^{-1} = \tau\psi\tau^{-1} \in \tau M^* \tau^{-1}$, o que nos diz que $(\tau(M))^* \subset \tau M^* \tau^{-1}$. Portanto, $(\tau(M))^* = \tau M^* \tau^{-1}$, e o lema está provado. □

Teorema 10.1.2 (Teorema Fundamental da Teoria de Galois)**.** *Se $L : K$ é uma extensão normal finita em $\mathbb{C}$, com grupo de Galois G, e se $\mathcal{F}, \mathcal{G}, *, \dagger$ são definidas como acima, então:*

1. *O Grupo de Galois G tem ordem $[L : K]$.*

2. *As funções $*$ e $\dagger$ são mutuamente inversas, e geram uma correspondência bijetiva entre $\mathcal{F}$ e $\mathcal{G}$ (revertem tamanho).*

3. *Se M é um corpo intermediário, então*

$$[L : M] = |M^*|,$$

$$[M : K] = \frac{|G|}{|M^*|}.$$

4. *Um corpo intermediário M é uma extensão normal de K se, e somente se, M^* é um subgrupo normal de G.*

5. *Se um corpo intermediário M é uma extensão normal de K, então o Grupo de Galois de $M : K$ é isomorfo ao grupo quociente $\frac{G}{M^*}$.*

Demonstração. A primeira parte é resultado do Corolário 9.3.7. Para a segunda parte, o Teorema 8.2.3 implica $L : M$ é normal. Agora, o Teorema 9.3.8 implica que M é um corpo fixo de M^*, então

$$M^{*\dagger} = M \tag{10.1}$$

Considere agora $H \in \mathcal{G}$. Sabemos que $H \subseteq H^{\dagger *}$. Portanto, $H^{\dagger *\dagger} = (H^\dagger)^{*\dagger} = H^\dagger$ por (10.1). Pelo Teorema referenciado em 9.3.8, $|H| = [L : H^\dagger]$. Portanto, $|H| = [L : H^{\dagger *\dagger}]$, e novamente pelo Teorema na demonstração do Teorema 9.3.8, $[L : H^{\dagger *\dagger}] = |H^{\dagger *}|$ e então $|H| = |H^{\dagger *}|$. Como, H e $H^{\dagger *}$ são grupos finitos e $H \subseteq H^{\dagger *}$, devemos ter $H = H^{\dagger *}$. A segunda parte do Teorema 10.1.2 segue daí.

Para terceira parte, notemos que $L : M$ é normal. O Corolário 9.3.7 garante que $[L : M] = |M^*|$, e a outra igualdade segue imediatamente.

Para provarmos as últimas duas partes do Teorema 10.1.2, necessitamos do Lema 10.1.1.

Provaremos a quarta parte do Teorema 10.1.2. Se $M : K$ é normal, seja $\tau \in G$. Então, $\tau|_M$ é um K-monomorfismo de M em L, e então um K-automorfismo de M pelo Teorema

9.3.5. Portanto, $\tau(M) = M$. Pelo Lema 10.1.1, $\tau M^* \tau^{-1} = M^*$, então M^* é um subgrupo normal de G.

Reciprocamente, suponha que M^* é um subgrupo normal de G. Seja σ qualquer K-monomorfismo de M em L. Pelo Teorema 9.1.3, existe um K-automorfismo τ de L tal que $\tau|_M = \sigma$. Agora, $\tau M^* \tau^{-1} = M^*$, como M^* é um subgrupo normal de G, assim pelo Lema 10.1.1, $\tau(M)^* = M^*$. Pela segunda parte do Teorema 10.1.2 (aplicando †), $\tau(M) = M$. Portanto, $\sigma(M) = M$ e σ é um K-automorfismo de M. Pelo Teoremma 9.3.5, $M : K$ é normal.

Agora, provamos a parte final do teorema. Seja G' o Grupo de Galois de $M : K$. Podemos definir uma função $\Phi : G \to G'$ por

$$\Phi(\tau) = \tau|_M, \ \tau \in G.$$

Claramente, tal função é um homomorfismo de grupos, $G \to G'$, pelo Teorema 9.3.5, $\tau|_M$ é um K-automorfismo de M. Pelo Teorema 9.1.3, Φ é sobrejetora. O núcleo de Φ é sem dúvidas M^*, e então por teoria de grupos (Teorema do Isomorfismo),

$$G' = Im(\Phi) \cong \frac{G}{Ker(\Phi)} = \frac{G}{M^*}.$$

Perceba agora como o Teorema referido na demonstração do Teorema 9.3.8 é usado na demonstração da segunda parte do Teorema 10.1.2, e seu uso é crucial. Muitos dos mais bonitos resultados da matemática usam este tratamento.

As últimas partes deste teorema podem ser generalizadas. Note que a demonstração da parte (5) resulta de um isomorfismo explícito entre $Gal(M : K)$ e $\frac{G}{M^*}$, chamado, restrição de M. □

A importância do Teorema Fundamental da Teoria de Galois deriva da ferramenta em potencial do que pelo seu mérito intrínseco. Este, permite-nos aplicar a teoria de grupos em problemas de polinômios intratáveis em $\mathbb{C}$ e associar subcorpos de $\mathbb{C}$. Antes de nos aventurarmos ainda mais com esta teoria, consolidaremos nossa posição ilustrando a teoria aqui discutida para uma extensão de corpo em particular e seu Grupo de Galois.

Capítulo 11

Um exemplo prático

O Teorema Fundamental da Teoria de Galois é um tanto quanto "demais" para ser entendido em uma única vez, portanto, é válido gastarmos um bom tempo pensando nele. Nós, analisaremos, assim, a Correspondência de Galois através de um exemplo entendido.

O exemplo é o Grupo de Galois do corpo de decomposição de t^4-2 sobre $\mathbb{Q}$. E faremos a discussão em pequenos pedaços para ser mais fácil digerí-la.

1. Seja $f(t) = t^4 - 2 = (t^2 - \sqrt{2})(t^2 + \sqrt{2}) = (t + \sqrt[4]{2})(t - \sqrt[4]{2})(t^2 + \sqrt{2}) = (t + \sqrt[4]{2})(t - \sqrt[4]{2})(t - i\sqrt[4]{2})(t + i\sqrt[4]{2})$ sobre $\mathbb{Q}$; e seja K o corpo de decomposição para f tal que $K \subseteq \mathbb{C}$. Podemos, pelo acima visto, fatorar f como segue:

$$f(t) = (t - \xi)(t + \xi)(t - i\xi)(t + i\xi),$$

em que, $\xi = \sqrt[4]{2}$ é real e positivo. Portanto, $K = \mathbb{Q}(i, \xi)$. Como K é um corpo de decomposição, $K : \mathbb{Q}$ é finita e normal (Teorema 8.2.3). Estamos trabalhando em $\mathbb{C}$, portanto, a separabilidade é automática.

2. Encontremos o grau de $K : \mathbb{Q}$. Pela Lei das Torres:

$$[K : \mathbb{Q}] = [\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}].$$

O polinômio minimal de i sobre $\mathbb{Q}(\xi)$ é $t^2 + 1$, como $t^2 + 1 = 0$, mas $i \notin \mathbb{R} \supseteq \mathbb{Q}(\xi)$. Temos que, $[\mathbb{Q}(\xi, i) : \mathbb{Q}(\xi)] = 2$. Agora, como ξ é um zero sobre $\mathbb{Q}$, e f é irredutível pelo Critério de Eisenstein, Teorema 3.4.1, temos que, f é o polinômio minimal de ξ sobre $\mathbb{Q}$. Assim, $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$. Portanto,

$$[K : \mathbb{Q}] = 2 \cdot 4 = 8.$$

3. Devemos encontrar os elementos do Grupo de Galois de $K : \mathbb{Q}$. Por uma checagem

direta, ou Corolário 5.3.3, há um $\mathbb{Q}$-automorfismo σ de K tal que,

$$\sigma(i) = i \quad \text{e} \quad \sigma(\xi) = i\xi,$$

e outro τ, tal que

$$\tau(i) = i \quad \text{e} \quad \tau(\xi) = \xi.$$

Produtos destes geram 8 distintos $\mathbb{Q}$-automorfismos de K, como seguem:

Automorfismo	Efeitos em ξ	Efeitos em i
1	ξ	i
σ	$i\xi$	i
$\sigma^2 = \sigma \circ \sigma$	$-\xi$	i
σ^3	$-i\xi$	i
τ	ξ	$-i$
$\sigma\tau$	$i\xi$	$-i$
$\sigma^2\tau$	$-\xi$	$-i$
$\sigma^3\tau$	$-i\xi$	$-i$

Tabela 11.1: $\mathbb{Q}$-automorfismos de K.

Notemos que $\sigma^4 = 1, \tau^2 = 1, \tau\sigma = \sigma^3\tau, \tau\sigma^2 = \sigma^2\tau$ e $\tau\sigma^3 = \sigma\tau$.

Agora, qualquer $\mathbb{Q}$-automorfismo de K leva i em algum zero de t^2+1, então $i \mapsto \pm i$; similarmente, ξ é mapeado em $\xi, i\xi, -\xi$ ou $-i\xi$. Todas as possibilidades de combinação destes oito números aparecem na lista acima, logo, estes são precisamente os $\mathbb{Q}$-automorfismos de K.

4. A estrutura abstrata do Grupo de Galois pode ser encontrada. A relação geradora mostra,

$$G = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle,$$

isto é, G é o grupo dihedral de ordem 8, que escrevemos como D_8 (na verdade são isomorfos de acordo com o Teorema do Isomorfismo).

O grupo D_8 tem uma interpretação geométrica como o grupo de simetrias do quadrado. De fato, podemos rotular os quatro vértices do quadrado, com os zeros de $t^4 - 2$ de modo que as simetrias geométricas são precisamente as permutações dos zeros que ocorrem no Grupo de Galois (veja Figura 11.1).

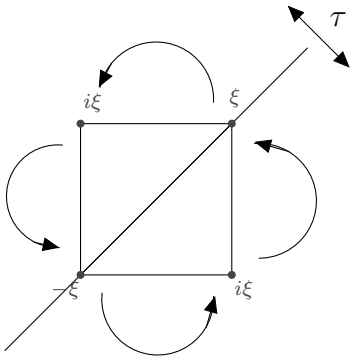

Figura 11.1: O grupo de Galois de D_8 interpretado como grupo de simetrias do quadrado.

5. É fácil encontrarmos os subgrupos de G. Como usualmente, deixamos $\mathbb{Z}_n$ denotar o grupo cíclico de ordem n e $\times$ o produto direto, então, os subgrupos de G são os que seguem:

$$\begin{array}{lcl}
\text{Ordem } 8: & G & G \cong D_8 \\
\text{Ordem } 4: & \{1, \sigma, \sigma^2, \sigma^3\} & S \cong \mathbb{Z}_4 \\
 & \{1, \sigma^2, \tau, \sigma^3\} & T \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \\
 & \{1, \sigma^2, \sigma\tau, \sigma^3\tau\} & U = \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\text{Ordem } 2: & \{1, \sigma^2\} & A \cong \mathbb{Z}_2 \\
 & \{1, \tau\} & B \cong \mathbb{Z}_2 \\
 & \{1, \sigma\tau\} & C \cong \mathbb{Z}_2 \\
 & \{1, \sigma^2\tau\} & D \cong \mathbb{Z}_2 \\
 & \{1, \sigma^3\tau\} & E \cong \mathbb{Z}_2 \\
\text{Ordem } 1: & \{1\} & I \cong 1.
\end{array}$$

6. As relações de inclusão entre os subgrupos de G podem ser somadas pelo diagrama de entrelaçamento. Em tal diagrama, Figura 11.2, $X \subseteq Y$ se há uma sequência de linhas de inclinação positiva de X a Y.

7. Através da Correspondência de Galois obtemos os corpos intermediários. Como a correspondência inverte as inclusões, obtemos o diagrama de linhas ilustrado na Figura 11.3.

8. Descrevemos, agora, os elementos destes corpos intermediários. Existem três subcorpos óbvios de K de grau 2 sobre $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i\sqrt{2})$. Estes são corpos fixos de

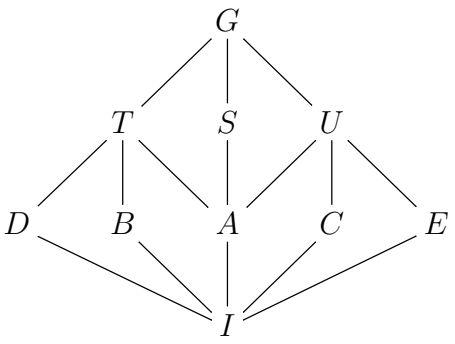

Figura 11.2: Reticulado de subgrupos.

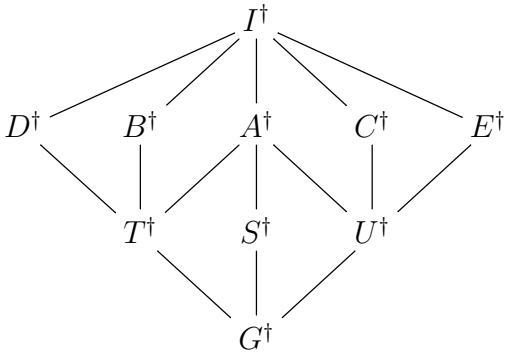

Figura 11.3: Reticulado de corpos intermediários.

$S^\dagger, T^\dagger$ e $U^\dagger$, respectivamente. Os outros corpos fixos são menos óbvios. Para mostrarmos uma possível aproximação, devemos encontrar $C^\dagger$. Notemos que qualquer elemento de K pode ser expresso unicamente na forma,

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3,$$

onde, $a_0, \ldots, a_7 \in \mathbb{Q}$. Então,

$$\begin{aligned} \sigma\tau(x) &= a_0 + a_1 i\xi - a_2\xi^2 - a_3 i\xi^3 - a_4 i + a_5(-i)i\xi - a_6 i(i\xi)^2 - a_7 i(i\xi)^3 \\ &= a_0 + a_5\xi - a_2\xi^2 - a_7\xi^3 - a_4 i + a_1 i\xi + a_6 i\xi^2 - a_3 i\xi^3 \end{aligned}$$

Ora, o elemento x é fixado por $\sigma\tau$ (e, portanto, por C) se, e somente se,

$$\begin{gathered} a_0 = a_0 \quad a_1 = a_5 \quad a_2 = -a_2 \quad a_3 = -a_7 \\ a_4 = -a_4 \quad a_5 = a_1 \quad a_6 = a_6 \quad a_7 = -a_3 \end{gathered}$$

Portanto, a_0 e a_6 são arbitrários, enquanto

$$a_2 = 0 = a_4 \quad a_1 = a_5 \quad a_3 = -a_7.$$

Segue que,

$$\begin{aligned} x &= a_0 + a_1(1+i)\xi + a_6 i\xi^2 + a_3(1-i)\xi^3 \\ &= a_0 + a_1[(1+i)\xi] + \frac{a_6}{2}[(1+i)\xi]^2 - \frac{a_3}{[(1+i)]\xi^3}, \end{aligned}$$

o que mostra que,

$$C^\dagger = \mathbb{Q}((1+i)\xi).$$

Similarmente,

$$A^\dagger = \mathbb{Q}(i, \sqrt{2}),\ B^\dagger = \mathbb{Q}(\xi),\ D^\dagger = \mathbb{Q}(i\xi),\ E^\dagger = \mathbb{Q}((1-i)\xi).$$

9. Os subgrupos normais de G são G, S, T, U, A, I. Pelo Teorema Fundamental da Teoria de Galois (Teorema 10.1.2), $G^\dagger, S^\dagger, T^\dagger, U^\dagger, A^\dagger, I^\dagger$ devem ser as únicas extensões normais de $\mathbb{Q}$ que estão contidas em K. Como estes são corpos de decomposição de $\mathbb{Q}$ para os polinômios, $t, t^2+1, t^2-2, t^2+2, t^4-t^2-2$ (provém de $(t^2+1)(t^2-2) = t^4-t^2-2$), t^4-2 (respectivamente), elas são extensões normais de $\mathbb{Q}$ (Teorema 8.2.3).

   Por outro lado, $B^\dagger : \mathbb{Q}$ não é normal, uma vez que t^4-2 tem um zero, ξ, em $B^\dagger$, mas não se fatora linearmente em $B^\dagger$. Similarmente, $C^\dagger, D^\dagger, E^\dagger$ não são extensões normais de $\mathbb{Q}$.

10. De acordo com o Teorema Fundamental da Teoria de Galois (Teorema 10.1.2), o Grupo de Galois de $A^\dagger : \mathbb{Q}$ é isomorfo a $\frac{G}{A}$. Agora, como $\frac{G}{A}$ é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ calcularemos diretamente o Grupo de Galois de $A^\dagger : \mathbb{Q}$. Como $A^\dagger = \mathbb{Q}(i, \sqrt{2})$, há 4 $\mathbb{Q}$-automorfismos:

Automorfismo	Efeito em i	Efeito em $\sqrt{2}$
1	i	$\sqrt{2}$
α	i	$-\sqrt{2}$
β	$-i$	$\sqrt{2}$
$\alpha\beta$	$-i$	$-\sqrt{2}$

Tabela 11.2: $\mathbb{Q}$-automorfismos de $A^\dagger$.

Notemos que: $\alpha^2 = \beta^2 = 1$ e $\alpha\beta = \beta\alpha$, como em $\mathbb{Z}_2 \times \mathbb{Z}_2$.

11. Notemos que o diagrama de linhas para $\mathcal{F}$ e $\mathcal{G}$ não se parecem, exceto que um é o outro de ponta cabeça. Portanto, não existe uma correspondência preservando as relações de inclusão. Isto parece um pouco ímpar, que a Correspondência de Galois reverta inclusões, mas, de fato, isto é inteiramente natural, e um tanto mais útil do que aquelas que preservam as inclusões.

Capítulo 12

Solubilidade e Simplicidade

Com o intuito de aplicar a Correspondência de Galois, precisamos ter em mãos um número de conceitos teóricos de grupos e teoremas. Assumimos familiaridade com a Teoria Elementar de Grupos: subgrupos, subgrupos normais, grupos quociente, conjugados, permutações (decomposição cíclica); e a estes, adicionaremos agora Teoremas de Isomorfismos.

Começaremos definindo Grupos Solúveis e provando algumas propriedades básicas. Estes, são importantes para a teoria de solução de equações por radicais. Em seguida, discutiremos sobre Grupos Simples, em que o principal objetivo é provar a simplicidade de grupos alternantes de grau maior ou igual a 5. Terminaremos o capítulo provando o Teorema de Cauchy: Se um primo p divide a ordem de um grupo finito, então o grupo tem um elemento de ordem p.

12.1 Grupos Solúveis

Grupos Solúveis foram primeiramente definidos e estudados (não do jeito abstrato corrente) por Galois no seu trabalho com solução de equações por radicais. Eles têm se mostrado extremamente importantes em muitos ramos da matemática.

Na definição a seguir, e daí em diante, a notação $H \triangle G$ significará que H é um subgrupo normal do grupo G. Relembremos que um grupo abeliano (ou comutativo) é aquele em que $gh = hg$ quaisquer que sejam os elementos g, h neste.

Definição 12.1.1. *Um grupo G é solúvel se este tem uma sequência finita de subgrupos,*

$$1 \subseteq G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G, \tag{12.1}$$

tais que,

1. $G_i \triangle G_{i+1}$, *para* $i = 0, \ldots, n-1$;
2. $\frac{G_{i+1}}{G_i}$ *é abeliano para* $i = 0, \ldots, n-1$.

A condição 1 não implica que $G_i \triangle G$, como também, $G_i \triangle G_{i+1} \triangle G_{i+2}$ não implica $G_i \triangle G_{i+2}$.

Exemplos 12.1.2. *1. Todo grupo abeliano G é solúvel, com a sequência $1 \triangle G$.*

2. *O grupo simétrico $\mathcal{S}_3$ de grau 3 é solúvel, pois tem um grupo cíclico normal de ordem 3 gerado pelo ciclo (123), cujo quociente é cíclico de ordem 2. Todos os grupos cíclicos são abelianos.*

3. *O grupo dihedral D_8 de ordem 8 é solúvel. No capítulo anterior, vimos que este tem um subgrupo normal S de ordem 4, cujo quociente tem ordem 2, e S é abeliano.*

4. *O grupo simétrico $\mathcal{S}_4$ de grau 4 é solúvel, com a sequência*

$$1 \triangle V \triangle \mathcal{A}_4 \triangle \mathcal{S}_4,$$

em que, $\mathcal{A}_4$ é o grupo alternante de ordem 12, e V é o quarto grupo de Klein (grupo consistido das permutações $1, (12)(34), (13)(24), (14)(23)$ e portanto, um produto direto de dois grupos cíclicos de ordem 2). Os grupos quocientes são:

$$\frac{V}{1} \cong V \text{ abeliano de ordem } 4;$$

$$\frac{\mathcal{A}_4}{V} \cong \mathbb{Z}_3 \text{ abeliano de ordem } 3;$$

$$\frac{\mathcal{S}_4}{\mathcal{A}_4} \cong \mathbb{Z}_2 \text{ abeliano de ordem } 2.$$

5. *O grupo simétrico $\mathcal{S}_5$ de grau 5 não é solúvel. Segue do sequinte Lema (encontrado em [5]):*

   - *O grupo simétrico $\mathcal{S}_n$ tem um grupo quociente de ordem prima, se e somente se, $p = 2$, e $n \geq 2$, em cada caso, o núcleo é o grupo alternante $\mathcal{A}_n$;*
   - *O grupo alternante $\mathcal{A}_n$ tem um grupo quociente de ordem prima p se, e somente se, $p = 3$ e $n = 3, 4$;*

   e do Corolário 12.2.5.

Relembremos os Teoremas de Isomorfismos.

Lema 12.1.3. *Sejam G, H e A grupos.*

1. *Se $H \triangle G$ e $A \subseteq G$, então $H \cup A \triangle A$ e*

$$\frac{A}{H \cap A} \cong \frac{HA}{H}.$$

2. *Se* $H \triangle G$, *e* $H \subseteq A \triangle G$, *então* $H \triangle A$, $\frac{A}{H} \triangle \frac{G}{H}$ *e*

$$\frac{G/H}{A/H} \cong \frac{G}{A}.$$

Demonstração. Podemos encontrar uma demonstração devidamente detalhada em [3]. □

Teorema 12.1.4. *Sejam* G *um grupo,* H *um subgrupo de* G, *e* N *um subgrupo normal de* G, *assim,*

1. *Se* G *é solúvel, então* H *é solúvel.*

2. *Se* G *é solúvel, então* G/N *é solúvel.*

3. *Se* N *e* G/N *são solúveis, então* G *é solúvel.*

Demonstração. 1. Seja,

$$1 = G_0 \triangle G_1 \triangle \ldots \triangle G_r = G$$

uma sequência de subgrupos normais de G, com quocientes $\frac{G_{i+1}}{G_i}$ abeliano. Consideremos $H_i = G_i \cap H$.

Então, pelo primeiro item do Lema 12.1.3, H tem uma sequência

$$1 + H_0 \triangle \ldots \triangle H_r = H.$$

Mostraremos que os coeficientes são abelianos. Ora,

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i},$$

pelo primeiro Teorema do Isomorfismo. Mas, este último grupo é um subgrupo de $\frac{G_{i+1}}{G_i}$ que é abeliano. Portanto, $\frac{H_{i+1}}{H_i}$ é abeliano para todo i, e, assim, H é solúvel.

2. Definamos G_i como acima. Então, $\frac{G}{N}$ tem a sequência

$$\frac{N}{N} = \frac{G_0N}{N} \triangle \frac{G_1N}{N} \triangle \ldots \triangle \frac{G_rN}{N} = \frac{G}{N}.$$

Um quociente típico é

$$\frac{G_{i+1}N/N}{G_iN/N},$$

que pelo segundo Teorema do Isomorfismo é isomorfo a

$$\frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i},$$

um quociente dos grupos abelianos $\frac{G_{i+1}}{G_i}$, e, portanto, abeliano. Assim, $\frac{G}{N}$ é solúvel.

3. Sabemos que existem as duas sequências

$$1 = N_0 \triangle N_1 \triangle \ldots \triangle N_r = N$$

$$\frac{N}{N} = \frac{G_0}{N} \triangle \frac{G_1}{N} \triangle \ldots \triangle \frac{G_S}{N} = \frac{G}{N}$$

com coeficientes abelianos. Consideremos a sequência de G dada pela combinação delas:

$$1 = N_0 \triangle N_1 \triangle \ldots \triangle N_r = N = G_0 \triangle G_1 \triangle \ldots \triangle G_S = G.$$

Os quocientes são o $\frac{N_{i+1}}{N_i}$, abeliano, ou $\frac{G_{i+1}}{G_i}$, isomorfo a $\frac{G_{i+1}/N}{G_i/N}$, também abeliano. Portanto, G é solúvel.

□

Diremos que um grupo G é uma extensão de um grupo A por um grupo B, se G tem um subgrupo normal N isomorfo a A tal que $\frac{G}{N}$ é isomorfo a B. Assim, somando as três propriedades do teorema acima, dizemos que a classe dos grupos solúveis é fechada perante subgrupos, quocientes e extensões. A classe dos grupos abelianos é fechada diante subgrupos e quocientes, mas não extensões, e provavelmente por esta razão que Galois foi levado a definir grupo solúveis.

12.2 Grupos Simples

Trataremos agora de grupos que, em certo sentido, são opostos aos solúveis.

Definição 12.2.1. *Um grupo G é simples se seus subgrupos normais são 1 e G.*

Exemplo 12.2.2. *Todo grupo cíclico $\mathbb{Z}_p$ com p primo é simples, já que, este não tem subgrupos além de 1 e $\mathbb{Z}_p$. Em particular, não há outros subgrupos normais. Estes grupos são também abelianos, portanto, solúveis. Eles são de fato os únicos grupos simples solúveis.*

Teorema 12.2.3. *Um grupo solúvel é simples se, e somente se, é cíclico e de ordem prima.*

Demonstração. Suponhamos que G é um grupo solúvel, portanto, este tem uma sequência

$$1 = G_0 \triangle G_1 \triangle \ldots \triangle G_n = G,$$

na qual devemos assumir $G_{i+1} \neq G_i$. Assim, G_{n-1} é um subgrupo normal próprio de G. Entretanto, G é simples, logo $G_{n-1} = 1$ e $G_n/G_{n-1} = G$, que é abeliano. Como todo subgrupo de um grupo abeliano é normal, e todo elemento de G gera um subgrupo cíclico, G deve ser cíclico com subgrupos próprios não triviais. Logo, G tem ordem prima.

A recíproca é trivial. □

Grupos simples têm um papel importante na teoria de grupos finitos. Eles são, em certo sentido, as unidades fundamentais das quais todos os grupos finitos são feitos. De fato, o teorema de Jordan-Hölder, que não provamos ou provaremos, diz que todo grupo finito tem uma sequência de subgrupos como na Equação (12.1), cujos quocientes são simples, e estes grupos simples dependem somente do grupo e não da sequência escolhida.

Teorema 12.2.4. *Se $n \geq 5$, então, o grupo alternante $\mathcal{A}_n$, de grau n é simples.*

Demonstração. Suponhamos que $1 \neq N \triangle \mathcal{A}_n$. Nossa estratégia será a seguinte: observemos, primeiramente, que se N contém um 3-ciclo, então contém todos os 3-ciclos, e como os 3-ciclos geram o $\mathcal{A}_n$, devemos ter $N = \mathcal{A}_n$. Segundo, mostraremos que N deve conter um 3-ciclo. Neste momento, é que temos como essencial, o fato de que $n \geq 5$.

Suponhamos, então, que N contenha um 3-ciclo, sem perda de generalidade, N, contenha (123). Assim, para qualquer $k > 3$, o ciclo $(32k)$ é uma permutação par, e, portanto, pertence a $\mathcal{A}_n$. Logo,

$$(32k)^{-1}(123)(32k) = (1k2),$$

pertence a N. Portanto, N contém $(1k2)^2 = (12k)$ para todo $k \geq 3$. Afirmamos que $\mathcal{A}_n$ é gerado por todos os 3-ciclos da forma $(12k)$. Se $n = 3$, temos a afirmação verdadeira. Caso, $n > 3$, temos que para todos $a, b > 2$, a permutação $(1a)(1b)$ é par, portanto, pertence a $\mathcal{A}_n$, e assim $\mathcal{A}_n$, contém

$$((1a)(1b))^{-1}(12k)(1a)(1b) = (abk),$$

se $k \neq a, b$. Como, $\mathcal{A}_n$ é gerado por todos os 3-ciclos, segue que $N = \mathcal{A}_n$.

Resta deste modo, mostrarmos que N contém ao menos um 3-ciclo. Faremos isto pela análise dos casos:

1. Suponhamos que N contenha um elemento $x = abc\cdots$, em que $a, b, c, \cdots$ sejam ciclos disjuntos e,

   $$a = (a_1 \cdots a_m) \quad (m \geq 4).$$

   Consideremos $t = (a_1 a_2 a_3)$. Então, N contém $t^{-1}xt$. Como, t comuta com $b, c, \cdots$ (ciclos disjuntos), segue que,

   $$t^{-1}xt = (t^{-1}at)bc\cdots = z \quad (digamos),$$

   então, N contém,

   $$zx^{-1} = (a_1 a_3 a_m),$$

   que é um 3-ciclo.

2. Suponhamos, agora, que N contenha um elemento envolvendo ao menos dois 3-

ciclos. Sem perda de generalidade, N contém,

$$x = (123)(456)y,$$

em y é uma permutação fixando $1, 2, 3, 4, 5, 6$. Consideremos $t = (234)$. Então, N contém,

$$(t^{-1}xt)x^{-1} = (12436).$$

Assim, pelo caso anterior, N contém um 3-ciclo.

3. Suponhamos que N contenha um elemento de x da forma $(ijk)p$, em que, p é um produto de 2-ciclos disjuntos de (ijk). Então, N contém $x^2 = (ijk)$, que é um 3-ciclo.

4. Resta apenas, o caso em que todo elemento de N é um produto disjunto de 2-ciclos. (Isto ocorre na verdade quando $n = 4$, dado pelo quatro-grupo $\mathcal{V}$). Mas, como $n \geq 5$, podemos assumir que N contém,

$$x = (12)(34)p,$$

em que p fixa $1, 2, 3, 4$. Se considerarmos, $t = (234)$, teremos que N contém

$$(t^{-1}xt)^{-1}x^{-1} = (14)(23),$$

e se $u = (145)$, N contém,

$$u^{-1}(t^{-1}xtx^{-1})u = (45)(23),$$

assim, N contém,

$$(45)(23)(14)(23) = (145),$$

contradizendo o fato de termos assumido que todo elemento de N é um produto de 2-ciclos disjuntos.

Portanto, $\mathcal{A}_n$ é simples se $n \geq 5$. □

Na verdade, $\mathcal{A}_5$ é o menor grupo simples não-abeliano, resultado provado primeiramente por Galois.

Corolário 12.2.5. *O grupo simétrico $\mathcal{S}_n$ de grau n é não solúvel para $n \geq 5$.*

Demonstração. Se $\mathcal{S}_n$ fosse solúvel, teríamos que $\mathcal{A}_n$ seria solúvel (Teorema 12.1.4), simples (Teorema 12.2.4), e portanto, de ordem prima pelo Teorema 12.2.3. Mas, $|\mathcal{A}_n| = \frac{1}{2}(n!)$, e não é primo se $n \geq 5$. □

12.3 Teorema de Cauchy

Provaremos nesta seção o Teorema de Cauchy, que diz: se um primo p divide a ordem de um grupo finito, então o grupo tem um elemento de ordem p. Começaremos para tanto relembrando algumas ideias da teoria de grupos.

Definição 12.3.1. *Elementos a e b de um grupo G são conjugados em G, se existe $g \in G$, tal que, $a = g^{-1}bg$.*

Conjugação é uma relação de equivalência; as classes de equivalências são as classes conjugadas de G.

Se as classes de conjugação de G são $C_1, \ldots, C_n$, então uma delas, digamos C_1, contém apenas o elemento identidade de G. Portanto, $|C_1| = 1$. Como as classes de conjugação formam uma partição de G, temos

$$|G| = 1 + |C_2| + \ldots + |C_r|,$$

que é a equação de classes para G.

Definição 12.3.2. *Se G é um grupo e $x \in G$, então o centralizador $C_G(x)$ de x em G é o conjunto de todos $g \in G$ para os quais $xg = gx$. Este sempre é um subgrupo de G.*

Veremos agora uma conexão entre centralizadores e classes de conjugação.

Lema 12.3.3. *Se G é um grupo e $x \in G$, então o número de elementos na classe de conjugação de x é o indíce de $C_G(x)$ em G.*

Demonstração. A equação $g^{-1}xg = h^{-1}xh$ é válida se, e somente se, $hg^{-1}x = xhg^{-1}$, o que significa que $hg^{-1} \in C_G(x)$, isto é, h e g estão no mesmo coset de $C_G(x)$ em G. O número destes cosets é o índice de $C_G(x)$ em G, donde temos provado o Lema. □

Corolário 12.3.4. *O número de elementos em uma classe de conjugação de um grupo finito G divide a ordem do grupo G.*

Definição 12.3.5. *O centro $Z(G)$ de um grupo G é o conjunto de todos os elementos $x \in G$, tal que, $xg = gx$ para todo $g \in G$.*

Exemplo 12.3.6. *O centro de G é um subgrupo normal de G. Muitos grupos têm um centro trivial, por exemplo, $Z(\mathcal{S}_3) = 1$. Grupos abelianos vão a outro extremo e têm $Z(G) = G$.*

Lema 12.3.7. *Se A é um grupo finito abeliano cuja ordem é divisível por um primo p, então, A tem um elemento de ordem p.*

Demonstração. Usaremos indução na $|A|$. Se $|A|$ é primo, temos que o resultado segue. Caso contrário, consideremos M um subgrupo próprio de A, cuja ordem m é maximal. Se p divide m, estamos nas hipóteses de indução. Então, suponhamos que p não divide m. Seja b um elemento de A, mas não de M, e seja B o subgrupo cíclico gerado por b. Então, MB é um subgrupo de A, maior do que M, e pela maximalidade $A = MB$.

Do Teorema do Isomorfismo temos,

$$|MB| = |M||B|/|M \cap B|,$$

e então, p divide a ordem r de B. Como B é cíclico, o elemento $b^{\frac{r}{p}}$ tem ordem p. □

Deste resultado, conseguimos um teorema mais geral:

Teorema 12.3.8 (Teorema de Cauchy)**.** *Se um primo p divide a ordem de um grupo finito G, então G tem um elemento de ordem p.*

Demonstração. Provaremos o teorema por indução na ordem de $|G|$. Os casos mais simples, $|G| = 1, 2, 3$ são triviais.

Para o passo de indução, começaremos com a equação de classes

$$|G| = 1 + |C_2| + \ldots + |C_r|.$$

Como $p \mid |G|$, devemos ter $p \nmid |C_j|$ para algum $j \geq 2$. Se $x \in C_j$, segue que $p \mid |C_G(x)|$, já que, $|C_j| = |G|/|C_G(x)|$.

Se $C_G(x) \neq G$, então, por indução, $C_G(x)$ contém um elemento de ordem p, e este elemento também pertence a G.

Caso $C_G(x) = G$, temos que $x \in Z(G)$, e escolhendo $x \neq 1$, conseguimos, $Z(G) \neq 1$.

Assim, $p \mid |Z(G)|$ ou $p \nmid |Z(G)|$. No primeiro caso, a demonstração é reduzida ao caso abeliano, Lema 12.3.7. No segundo caso, por indução, existe $x \in G$ tal que a imagem $\overline{x} \in G/Z(G)$ tem ordem p. Isto é, $x^p \in Z(G)$, mas, $x \notin Z(G)$. Seja X o grupo cíclico gerado por x. Agora, $XZ(G)$ é abeliano e tem ordem divisível por p, então, pelo Lema 12.3.7 sabemos que existe um elemento de ordem p no mesmo, e, novamente, este elemento pertence a G.

Isto completa o passo de indução e assim conclui a demonstração. □

Capítulo 13

Solução por radicais

O objetivo deste capítulo é usar a Correspondência de Galois para "derivar" uma condição que deva ser satisfeita por qualquer equação polinomial para que esta seja solúvel por radicais, digamos: o Grupo de Galois associado deve ser um Grupo Solúvel. Nós, então, construiremos uma equação polinomial quíntica cujo Grupo de Galois não seja solúvel, uma equação de desconcertante aparência simples, $t^5 - 6t + 3 = 0$, que mostra que a equação quíntica não pode ser resolvida por radicais.

13.1 Extensões Radicais

Algum cuidado é necessário na formalização da ideia de solubilidade por radicais. Começaremos do ponto de vista de Extensões de Corpos.

Informalmente, uma Extensão radical é obtida por uma sequência de adjunções de raízes n-ésimas, para vários n. Por exemplo, a expressão a seguir é radical:

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}}. \tag{13.1}$$

Para encontrarmos uma extensão de $\mathbb{Q}$ que contenha este elemento, deveremos adicionar, gradualmente, os elementos

$$\alpha = \sqrt[3]{11},\ \beta = \sqrt{3},\ \gamma = \sqrt[5]{\frac{(7+\beta)}{2}},\ \delta = \sqrt[3]{4},\ \epsilon = \sqrt[4]{1+\delta}.$$

Assim, por sugestão, temos a seguinte definição.

Definição 13.1.1. *Uma extensão $L : K$ em $\mathbb{C}$ é radical se $L = K(\alpha_1, \ldots, \alpha_m)$, onde para cada $j = 1, \ldots, m$ existe um inteiro n_j tal que*

$$\alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1}) \quad (j \geq 2).$$

Os elementos α_j formam uma sequência radical para $L : K$. O grau radical do radical α_j

é n_j.

Exemplo 13.1.2. *A expressão em* (13.1) *está contida em uma extensão radical da forma* $\mathbb{Q}(\alpha, \beta, \gamma, \delta, \epsilon)$ *de* $\mathbb{Q}$*, em que* $\alpha^3 = 11$, $\beta^2 = 3$, $\gamma^5 = \frac{(7+\beta)}{2}$, $\delta^3 = 4$ *e* $\epsilon^4 = 1 + \delta$.

É claro que qualquer expressão radical está contida em alguma extensão radical.

Um polinômio deveria ser considerado solúvel por radicais se todos os seus zeros são expressões radicais sobre o corpo base, assim temos a definição:

Definição 13.1.3. *Seja f um polinômio sobre um subcorpo K de $\mathbb{C}$, e seja $Gal(f, K)$ o corpo de decomposição de f sobre K. Dizemos que f é solúvel por radicais se existe um corpo M contendo $Gal(f, K)$, tal que $M : K$ seja uma extensão radical.*

Enfatizamos que na definição não exigimos que a extensão ao corpo de decomposição $Gal(f, K) : K$ seja radical. Há um motivo para tal. Queremos que tudo no corpo de decomposição $Gal(f, K)$ seja expresso por radicais, mas é desenxabido esperar que tudo expresso pelos mesmos radicais esteja dentro do corpo de decomposição. Se $M : K$ é radical e L é um corpo intermediário, então $L : K$ não precisa ser radical.

Observemos também que requeremos que todos os zeros de f sejam expressos por radicais. É possível que alguns zeros sejam expressos por radicais, enquanto outros não; simplesmente tomemos o produto de dois polinômios, um solúvel por radicais e outro não. Entretanto, se um polinômio irredutível f tem um zero expresso por radicais, então todos os zeros devem ser expressos, por um simples argumento baseado no Corolário 5.3.3.

O principal teorema deste capítulo exige algumas preliminares. Portanto, faremos alguns lemas, e o tal em seguida.

Lema 13.1.4. *Se $L : K$ é uma extensão radical em $\mathbb{C}$ e M é o fecho normal de $L : K$, então $M : K$ é radical.*

Demonstração. Seja $L = K(\alpha_1, \ldots, \alpha_r)$ com $\alpha_1^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ ($L : K$ é por hipótese uma extensão radical). Seja f_i o polinômio minimal de α_i sobre K. Então, $M \supseteq L$ é claramente o corpo de decomposição de $\prod_{i=1}^{r} f_i$. Para todo zero β_{ij} de f_i em M, existe um isomorfismo $\sigma : K(\alpha_i) \to K(\beta_{ij})$ pelo Corolário 5.3.3. Assim, temos que pela Proposição 9.1.4, σ estende a um K-automorfismo $\tau : M \to M$. Como α_i é radical sobre K, então o é β_{ij}, e portanto, o é M. □

Mostraremos, agora, a partir de dois lemas, que certos Grupos de Galois são abelianos.

Lema 13.1.5. *Seja K um subcorpo de $\mathbb{C}$ e seja L o corpo de decomposição para $t^p - 1$ sobre K, onde p é primo. Então, o Grupo de Galois de $L : K$ é abeliano.*

Demonstração. A derivada de $t^p - 1$ é pt^{p-1}, que é primo a $t^p - 1$. Logo, pelo Lema 8.3.5, o polinômio não tem zeros múltiplos em L. Claramente, seus zeros formam um grupo sob multiplicação; este grupo tem ordem prima p, e como os zeros são distintos, ele é cíclico.

Seja ϵ um gerador deste grupo. Então, $L = K(\epsilon)$, e qualquer K-automorfismo de L é determinado por seu efeito em ϵ.

Além disso, K-automorfismos permutam os zeros de $t^p - 1$. Portanto, qualquer K-automorfismo de L é da forma,

$$\alpha_j : \epsilon \to \epsilon^j,$$

e é unicamente determinado por esta condição. Mas, então $\alpha_i\alpha_j$ e $\alpha_j\alpha_i$ levam, ambos, ϵ em ϵ^{ij}, portanto, o Grupo de Galois é abeliano. □

Lema 13.1.6. *Seja K um subcorpo de $\mathbb{C}$ em que $t^n - 1$ se decompõe linearmente. Sejam $a \in K$ e L um corpo de decomposição para $t^n - a$ sobre K. Então, o Grupo de Galois de $L : K$ é abeliano.*

Demonstração. Seja α um zero qualquer de $t^n - a$. Como $t^n - 1$ se decompõe linearmente em K, o zero geral de $t^n - a$ é ϵ_a onde ϵ é um zero de $t^n - 1$ em K. Como $L = K(\alpha)$, qualquer K-automorfismo de L é determinado por seu efeito em α. Dados dois K-automorfismos:

$$\Phi : \alpha \mapsto \epsilon\alpha \quad \text{e} \quad \Psi : \alpha \mapsto \eta\alpha,$$

onde, ϵ e $\eta \in K$, então

$$\Phi\Psi(\alpha) = \epsilon\eta\alpha = \eta\epsilon\alpha = \Psi\Phi(\alpha).$$

E, como anteriormente, o Grupo de Galois é abeliano. □

Lema 13.1.7. *Se K é um subcorpo de $\mathbb{C}$ e $L : K$ é normal e radical, então $Gal(L : K)$ é solúvel.*

Demonstração. Suponha que $L = K(\alpha_1, \ldots, \alpha_n)$ com $\alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1})$. Pela seguinte Proposição: Se existe uma torre finita de subcorpos, podemos refinar (se for necessário aumentar o comprimento) de modo a fazermos todos os n_j primos (vide [5]); devemos assumir que n_j é primo para todo j. Em particular, existe um primo p tal que $\alpha_1^p \in K$.

Provamos o resultado por indução em n, usando a hipótese adicional de que todos os n_j são primos. O caso $n = 0$ é trivial, donde começa a indução.

Se $\alpha_1 \in K$, então $L = K(\alpha_2, \ldots, \alpha_n)$ e $Gal(L : K)$ é solúvel por indução.

Podemos, portanto, assumir que $\alpha_1 \notin K$. Seja f o polinômio minimal de α_1 sobre K. Como $L : K$ é normal, f se decompõe linearmente em L, pois $K \subseteq \mathbb{C}$, e f não tem zeros repetidos em L. Como $\alpha_1 \notin K$, o grau de f é no mínimo 2. Seja β um zero de f diferente de α_1, e consideremos $\epsilon = \frac{\alpha_1}{\beta}$. Então, $\epsilon^p = 1$ e $\epsilon \neq 1$. Portanto, ϵ tem ordem p no grupo multiplicativo de L, logo, os elementos $1, \epsilon, \epsilon^2, \ldots, \epsilon^{p-1}$ são raízes p-ésimas distintas da unidade em L. Portanto, $t^p - 1$ se decompõe linearmente em L.

Seja $M \subseteq L$ o corpo de decomposição de $t^p - 1$ sobre K, isto é, $M = K(\epsilon)$. Consideremos a cadeia de subcorpos $K \subseteq M \subseteq M(\alpha_1) \subseteq L$. Podemos ilustrar o resto da demonstração pelo seguinte diagrama:

L		
$\vert$	$\leftarrow$	$Gal(L : M(\alpha_1))$ solúvel por indução
$M(\alpha_1)$		
$\vert$	$\leftarrow$	$Gal(M(\alpha_1) : M)$ abeliano pelo Lema 13.1.6
M		
$\vert$	$\leftarrow$	$Gal(M : K)$ abeliano pelo Lema 13.1.5
K		

Tabela 13.1: Estratégia da demonstração.

Observemos que $L : K$ é finita e normal, portanto, também o é $L : M$; assim, o Teorema 10.1.2 se aplica à $L : K$ e à $L : M$.

Como $t^p - 1$ se decompõe linearmente em M e $\alpha_1^p \in M$, a demonstração do Lema 13.1.6 implica que $M(\alpha_1)$ é um corpo de decomposição para $t^p - \alpha_1^p$ sobre M. Portanto, $M(\alpha_1) : M$ é normal, e pelo Lema 13.1.6 $Gal(M(\alpha_1) : M)$ é abeliano. Apliquemos o Teorema 10.1.2 à $L : M$ para deduzirmos que

$$Gal(M(\alpha_1) : M) \cong \frac{Gal(L : M)}{Gal(L : M(\alpha_1))}.$$

Agora,

$$L = M(\alpha_1)(\alpha_2, \ldots, \alpha_n),$$

e, então, $L : M(\alpha_1)$ é uma extensão normal radical. Por indução, $Gal(L : M(\alpha_1))$ é solúvel. Portanto, pelo terceiro item do Teorema 12.1.4, $Gal(L : M)$ é solúvel.

Como M é o corpo de decomposição para $t^p - 1$ sobre K, a extensão $M : K$ é normal. Temos pelo Lema 13.1.5 que $Gal(M : K)$ é abeliano. O Teorema 10.1.2 aplicado à $L : K$ garante que

$$Gal(M : K) \cong \frac{Gal(L : K)}{Gal(L : M)}.$$

Por fim, o Teorema 10.1.2 mostra que $Gal(L : K_0)$ é solúvel, completando o passo de indução. □

Teorema 13.1.8. *Se K é um subcorpo de $\mathbb{C}$ e $K \subseteq L \subseteq M$, onde $M : K$ é uma extensão radical, então o Grupo de Galois de $L : K$ é solúvel.*

Demonstração. Seja K_0 um corpo fixo de $Gal(L : K)$, e $N : M$ o fecho normal de $M : K_0$. Então,

$$K \subseteq K_0 \subseteq L \subseteq M \subseteq N.$$

Como $M : K_0$ é radical, o Lema 13.1.4 implica que $N : K_0$ é uma extensão normal radical. Donde, pelo Lema 13.1.7, $Gal(N : K_0)$ é solúvel.

A partir do Teorema 9.3.10, conseguimos que a extensão $L : K_0$ é normal. E assim,

pela Correspondência de Galois (Teorema 10.1.2),

$$Gal(L : K_0) \cong \frac{Gal(N : K_0)}{Gal(N : L)}.$$

O Teorema 10.1.2 implica que $Gal(L : K_0)$ é solúvel. Mas, $Gal(L : K) = Gal(L : K_0)$, concluimos, portanto, que $Gal(L : K)$ é solúvel. □

A ideia desta demonstração é simples: uma extensão radical é uma série de extensões por raízes n-ésimas. Tais extensões possuem Grupos de Galois abelianos, então o Grupo de Galois de uma extensão radical é obtido a partir de uma adjunção de grupos abelianos. Infelizmente, há problemas técnicos ao longo da demonstração, e nós temos de escrevê-la em termos das raízes da unidade, e mais, temos de criar várias extensões normais antes de usarmos a Correspondência de Galois.

Agora, voltaremos a trabalhar com polinômios, e assim retornarmos ao que, de fato, Galois trabalhou.

Definição 13.1.9. *Seja f um polinômio sobre K (um subcorpo de $\mathbb{C}$), com corpo de decomposição $Gal(f, K)$ sobre K. O Grupo de Galois de f sobre K é o grupo $Gal(Gal(f, K) : K)$.*

Seja G o Grupo de Galois de um polinômio f sobre K, e seja $\partial f = n$. Se $\alpha \in Gal(f, K)$ é um zero de f, então, $f(\alpha) = 0$, e assim, para qualquer $g \in G$,

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

Portanto, cada elemento $g \in G$ induz uma permutação g' do conjunto de raízes de f em $Gal(f, K)$. Elementos distintos de G induzem permutações distintas, como $Gal(f, K)$ é gerado pelos zeros de f. Segue facilmente que $g \mapsto g'$ é um monomorfismo de grupo de G no grupo de $\mathcal{S}_n$ de todas as permutações de zeros de f. Isto, de fato, era como Galois pensava o grupo de Galois, e por muitos anos seguidos, os grupos de permutações e os grupos de transformações de variáveis eram os únicos grupos considerados pelos matemáticos.

Estamos agora em condições de reescrever o Teorema 13.1.8:

Teorema 13.1.10. *Seja f um polinômio sobre um subcorpo K de $\mathbb{C}$. Se f é solúvel por radicais, então o Grupo de Galois de f sobre K é solúvel.*

Portanto, para encontrarmos um polinômio não solúvel por radicais, é suficiente encontrarmos um, em que o Grupo de Galois não seja solúvel. Há duas maneiras de fazê-lo. Uma é olhar para o polinômio geral de grau n (o que não é uma boa abordagem), e a outra é exibir um polinômio específico com coeficientes racionais onde o Grupo de Galois seja não solúvel.

13.2 Uma quíntica insolúvel

Lema 13.2.1. *Seja p um primo, e seja f um polinômio irredutível de grau p sobre $\mathbb{Q}$. Suponhamos que f tenha precisamente dois zeros não reais em $\mathbb{C}$. Então, o Grupo de Galois de f sobre $\mathbb{Q}$ é isomorfo ao grupo simétrico $\mathcal{S}_p$.*

Demonstração. Pelo Teorema Fundamental da Álgebra, $\mathbb{C}$ contém o corpo de decomposição $Gal(f, \mathbb{Q})$. Seja G o Grupo de Galois de f sobre $\mathbb{Q}$, considerado como o grupo de permutação nos zeros de f. Estes, são distintos pela Proposição 8.3.6, logo, G é (isomorfo a) um subgrupo de $\mathcal{S}_p$. Quando construímos o corpo de decomposição de f, primeiro nós adicionamos um elemento de grau p, então $[Gal(f, \mathbb{C}) : \mathbb{Q}]$ é divisível por p. Pelo Teorema 10.1.2, p divide a ordem de G. Pelo Teorema de Cauchy, Teorema 12.3.8, G tem um elemento de ordem p. Mas, os únicos elementos de $\mathcal{S}_p$ de ordem p são os p-ciclos. Portanto, G contém um p-ciclo.

Como Conjugação dos Complexos é um $\mathbb{Q}$-automorfismo de $\mathbb{C}$, temos a indução de um $\mathbb{Q}$-automorfismo de $Gal(f, \mathbb{C})$. Isto, deixa $p-2$ zeros reais de f fixados, enquanto transpõe os zeros não reais. Assim, G contém um 2-ciclo.

Pela escolha da notação para zeros e, se necessário, tomando potências do p-ciclo, devemos assumir que G contém o 2-ciclos (12) e o p-ciclo $(12\ldots p)$. Afirmamos que estes geram todo o conjunto $\mathcal{S}_p$, o que completará a demonstração. Para provarmos a afirmação, consideremos $c = (12\ldots p)$, $t = (12)$, e G o grupo gerado por c e t. Então, G contém $c^{-1}tc = (23)$, e, portanto, $c^{-1}(23)c = (34), \ldots$ e assim todas as transposições $(m, m+1)$. Então, G contém

$$(12)(23)(12) = (13) \quad (13)(34)(13) = (14),$$

e daí por diante, portanto, contém todas as transposições $(1m)$. Finalmente, G contém todos os produtos $(1m)(1r)(1m) = (mr)$. Mas, todo elemento de $\mathcal{S}_n$ é um produto de transposições, então $G = \mathcal{S}_p$. □

Teorema 13.2.2. *O polinômio $t^5 - 6t + 3$ sobre $\mathbb{Q}$ não é solúvel por radicais.*

Demonstração. Seja $f(t) = t^5 - 6t + 3$. Pelo Critério de Eisenstein, f é irredutível sobre $\mathbb{Q}$. Devemos mostrar que f tem precisamente três zeros reais, cada um com multiplicidade 1, e portanto, têm dois zeros não reais. Como 5 é primo, pelo Lema 13.2.1, o Grupo de Galois de f sobre $\mathbb{Q}$ é $\mathcal{S}_5$. Pelo Corolário 12.2.5. $\mathcal{S}_5$ não é solúvel. Logo, pelo Teorema 13.1.10, $f(t) = 0$ é não solúvel por radicais.

Resta mostrarmos que f tem exatamente três zeros reais, cada um de multiplicidade 1. Ora, $f(-2) = -17$, $f(-1) = 8, f(0) = 3, f(1) = -2$, e $f(2) = 23$. Uma breve olhada no gráfico de $y = f(x)$ nos mostra isto (olhar Figura 13.2). Assim, pelo Teorema de Rolle, os zeros de f são separados pelos zeros de Df. Além disso, $Df = 5t^4 - 6$, que tem como zeros $\pm\sqrt[4]{\frac{6}{5}}$. Claramente, f e Df são coprimos, então f não têm zeros repetidos (segue também por irredutibilidade), e então, f tem no máximo três zeros reais. Mas,

certamente f tem no mínimo três zeros reais, já que uma função contínua definida nos reais não muda de sinal, exceto se passar pelo zero. Portanto, f tem precisamente três zeros reais, e o resultado segue.

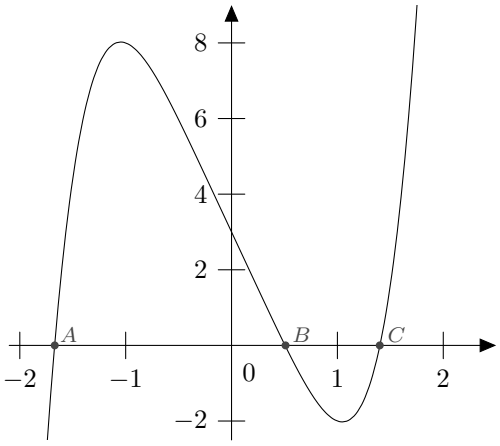

Figura 13.1: Gráfico da polinomial $t^5 - 6t + 3$.

□

Capítulo 14

O Polinômio Geral

14.1 Graus Transcendentes

Até o presente momento não trabalhamos com as extensões transcendentes; ao invés disto assumimos a finitude das extensões como foco central da teoria. Considereramos agora esta classe maior de extensões.

Definição 14.1.1. *Uma extensão $L : K$ é finitamente gerada se $L = K(\alpha_1, \ldots, \alpha_n)$, em que, n é finito.*

Notemos que os α_j podem ser algébricos ou transcendentes sobre K.

Definição 14.1.2. *Se $t_1, \ldots, t_n$ são elementos transcendentes sobre um corpo K, todos em alguma extensão L de K, então eles são independentes se há um polinômio não trivial p sobre K (em n indeterminadas) tal que $p(t_1, \ldots, t_n) = 0$ em L.*

Exemplo 14.1.3. *Se t é transcendente sobre K e u é transcendente sobre $K(t)$, então $K(t, u)$ é uma extensão finitamente gerada de K, e t, u são independentes. Por outro lado, t e $u = t^2 + 1$ são ambos transcendentes sobre K, mas estão relacionados pela equação polinomial $t^2 + 1 - u = 0$, logo, não são independentes.*

O próximo Lema descreve a estrutura de uma extensão finitamente gerada.

Lema 14.1.4. *Se $L : K$ é finitamente gerada, então, existe um corpo intermediário M tal que,*

1. *$M = K(\alpha_1, \ldots, \alpha_r)$, em que, os α_i são elementos transcendentes e independentes sobre K.*

2. *$L : M$ é uma extensão finita.*

Demonstração. Sabemos que $L = K(\beta_1, \ldots, \beta_n)$, pois $L : K$ é finitamente gerada. Se todos os β_j são algébricos sobre K, então $L : K$ é finita pelo Lema 6.1.9 (generalizado) e, devemos considerar $M = K$. Caso contrário, algum dos β_i é transcendente sobre

K. Chamemos este de α_1. Se $L : K(\alpha_1)$ não é finita, existe algum β_k transcendente sobre $K(\alpha_1)$. Chamemos o mesmo de α_2. Continuamos este processo até conseguirmos $M = K(\alpha_1, \ldots, \alpha_r)$ de tal modo que $L : M$ é finita. Logo, por construção, os α_j são elementos transcendentes independentes sobre K. □

Lema 14.1.5 (Lema de Steinitz da Troca)**.** *Com a mesma notação do Lema 14.1.4, se existir outro corpo intermediário de $N = K(\beta_1, \ldots, \beta_s)$, tal que, $\beta_1, \ldots, \beta_s$ são elementos transcendentes independentes sobre K e $L : N$ seja finita, devemos ter $r = s$.*

Demonstração. Como $[L : M]$ é finito, temos pelo Lema 6.1.9 que β_1 é algébrico sobre M. Portanto, existe uma equação polinomial

$$p(\beta_1, \alpha_1, \ldots, \alpha_r) = 0.$$

Assim, algum α_j, sem perda de generalidade, α_1, na verdade aparece na equação. Então, α_1 é algébrico sobre $K(\beta_1, \alpha_2, \ldots, \alpha_r)$ e $L : K(\beta_1, \alpha_2, \ldots, \alpha_r)$ é finita. Indutivamente, conseguimos substituir α_j por β_j, e deste modo,

$$L : K(\beta_1, \ldots, \beta_r)$$

é finita. Se $s > r$, temos que β_{r+1} deve ser algébrico sobre $K(\beta_1, \ldots, \beta_r)$, o que é uma contradição. Portanto, $s \leq r$. Analogamente, conseguimos perceber que $r \leq s$. E assim, temos a demonstração do Lema. □

Definição 14.1.6. *O inteiro definido no Lema 14.1.4 é o grau de transcendência de $L : K$. Pelo Lema 14.1.5, o valor de r é bem definido.*

Exemplo 14.1.7. *Consideremos $K(t, \alpha, u) : K$, em que, t é transcendente sobre K, $\alpha^2 = t$, e u é transcendente sobre $K(t, \alpha)$. Assim, $M = K(t, u)$, em que, t e u são elementos transcendentes independentes sobre K, e, portanto,*

$$K(t, \alpha, u) : M = M(\alpha) : M$$

é finita. Deste modo, vemos que o grau de transcendência é dois.

Proposição 14.1.8. *Uma extensão finitamente gerada $L : K$ tem grau de transcendência r se, e somente se, existe um corpo intermediário M tal que L é uma extensão finita de M e $M : K$ é isomorfa a $K(t_1, \ldots, t_r) : K$.*

Demonstração. Suponhamos que $L : K$ seja finitamente gerada. Assim, pelo Lema 14.1.4, temos que existe M, corpo intermediário, ou seja, $K \subseteq M \subseteq L$, e elementos $t_1, \ldots, t_r$ transcendentes e independentes, tais que $M = K(t_1, \ldots, t_r)$, e $L : M$ é finita. Neste caso, r é o grau de transcendência de $L : K$.

Suponhamos agora, que $L : K$ é finitamente gerada, M é corpo intermediário de L e K, $L : M$ seja uma extensão finita e $M : K$ é isomorfa a $K(t_1, \ldots, t_r) : K$. Assim, consideremos φ o isomorfismo de M em $K(t_1, \ldots, t_r)$, logo $M \supseteq K(\beta_1, \ldots, \beta_r)$. Seja $\beta \in M \setminus K(\beta_1, \ldots, \beta_r)$, logo, existe $\alpha = \varphi(\beta) \in K(t_1, \ldots, t_r)$.

Se α é algébrico, então $\alpha \in K$, logo $\beta \in K$, o que é um absurdo.

Portanto, α é transcendente, ou seja, existe algum polinômio não constante, tal que $\alpha = f(t_1, \ldots, t_r)$. Assim, $\beta = (\varphi^{-1}f)(\beta_1, \ldots, \beta_r) \in K(\beta_1, \ldots, \beta_r)$. Portanto, $M = K(\beta_1, \ldots, \beta_r)$, e pelo Lema 14.1.5, r é o grau de transcendência de $L : K$. □

14.2 Polinômios Elementares Simétricos

Geralmente é nos dado um polinômio e desejamos encontrar os seus zeros. Mas, também é possível trabalhar na direção contrária, isto é, dados os zeros e as suas respectivas multiplicidades, reconstruirmos o polinômio (problema incrivelmente mais simples do que o primeiro, ao qual concentraremos nossa atenção).

Consideremos um polinômio de grau n e seus n zeros com as respectivas multiplicidades. Isto é,

$$f(t) = k(t - \alpha_1) \cdot \ldots \cdot (t - \alpha_n),$$

em que, $k \in K$ e α_j são os zeros em K (não necessariamente distintos). Suponhamos que

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n.$$

Se expandirmos o primeiro produto e compararmos os coeficientes com os da segunda expressão, temos o seguinte resultado:

$$\begin{aligned} a_n &= k \\ a_{n-1} &= -k(\alpha_1 + \ldots + \alpha_n) \\ a_{n-2} &= k(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n) \\ &\ldots \\ a_0 &= k(-1)^n \alpha_1\alpha_2 \cdot \ldots \cdot \alpha_n \end{aligned}$$

A expressão em $\alpha_1, \ldots, \alpha_n$ do lado direito é o polinômio elementar simétrico, porém, agora, estão sendo interpretados como elementos de $K(t_1, \ldots, t_n)$, em que, K pode ser qualquer corpo. Além disso, os polinômios elementares simétricos aqui calculados como $t_j = \alpha_j$, para $1 \leq j \leq n$.

Os polinômios elementares simétricos são simétricos no sentido de que eles não se alteram através de uma permutação das indeterminadas t_j. Esta propriedade nos sugere:

Definição 14.2.1. *Um polinômio $q \in K(t_1, \ldots, t_n)$ é simétrico se*

$$q(t_{\sigma(1)}, \ldots, t_{\sigma(n)}) = q(t_1, \ldots, t_n),$$

para todas a permutações $\sigma \in \mathcal{S}_n$.

Existem outros polinômios simétricos além dos polinômios simétricos elementares, como por exemplo, $t_1^2 + \ldots + t_n^2$. Mas, estes, podem ser expressos em termos dos primeiros, como acima discutido. Assim, temos o seguinte teorema:

Teorema 14.2.2. *Sobre o corpo K, qualquer polinômio simétrico em $t_1, \ldots, t_n$ pode ser expresso como um polinômio de grau menor ou igual em termos dos polinômios elementares $s_r(t_1, \ldots, t_n)$, com $r = 0, \ldots, n$.*

14.3 O Polinômio Geral

Seja K um corpo qualquer, e sejam $t_1, \ldots, t_n$ os elementos transcendentes sobre K. O grupo simétrico $\mathcal{S}_n$ pode atuar como um grupo de K-automorfismos de $K(t_1, \ldots, t_n)$ (uso de uma transformação linear), definindo,

$$\sigma(t_i) = t_{\sigma(i)},$$

para todo $\sigma \in \mathcal{S}_n$. Podemos extendê-lo a qualquer expressão racional Φ pela definição,

$$\sigma(\Phi(t_1, \ldots, t_n)) = \Phi(t_{\sigma(1)}, \ldots, t_{\sigma(n)}).$$

Conseguimos, assim, provar que σ, extendido deste modo, é um K-automorfismo.

Exemplo 14.3.1. *Se $n = 4$ e σ é a permutação*

$$\begin{pmatrix} 1234 \\ 2431 \end{pmatrix},$$

temos então, $\sigma(t_1) = t_2, \sigma(t_2) = t_4, \sigma(t_3) = t_3$ e $\sigma(t_4) = t_1$. Além disto, como um caso típico,

$$\sigma\left(\frac{{t_1}^5 t_4}{{t_2}^4 - 7t_3}\right) = \frac{{t_2}^5 t_1}{{t_4}^4 - 7t_3}.$$

Claramente, elementos distintos de $\mathcal{S}_n$ originam K-automorfismos distintos.

O corpo fixo F de $\mathcal{S}_n$ obviamente contém todos os polinômios simétricos em t_i, e, em particular, os polinômios elementares simétricos $s_r = s_r(t_1, \ldots, t_n)$. Devemos mostrar que estes geram F.

Lema 14.3.2. *Com a notação acima, $F = K(s_1, \ldots, s_n)$.*

Demonstração. Primeiro mostraremos que

$$[K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)] \leq n!,$$

por indução em n. Consideremos a extensão dupla,

$$K(t_1, \ldots, t_n) \supseteq K(s_1, \ldots, s_n, t_n) \supseteq K(s_1, \ldots, s_n).$$

Agora, $f(t_n) = 0$, em que,

$$f(t) = t^n - s_1 t^{n-1} + \ldots + (-1)^n s_n,$$

e, tal que,

$$[K(s_1, \ldots, s_n, t_n) : K(s_1, \ldots, s_n)] \leq n.$$

Se considerarmos $s'_1, \ldots, s'_{n-1}$ o polinômio elementar simétrico em $t_1, \ldots, t_{n-1}$, e definirmos $s'_0 = 1$, então

$$s_j = t_n s'_{j+1} + s'_j,$$

e, portanto,

$$K(s_1, \ldots, s_n, t_n) = K(t_n, s'_1, \ldots, s'_{n-1}).$$

Por indução,

$$[K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n, t_n)] = [K(t_n)(t_1, \ldots, t_{n-1}) : K(t_n)(s'_1, \ldots, s'_{n-1})] \leq (n-1)!$$

e assim, pela Lei das Torres (generalizada) o passo de indução segue.

Agora, $K(s_1, \ldots, s_n)$ é claramente um corpo fixo F de $\mathcal{S}_n$. Pelo Teorema referido na demonstração de 9.3.8 (generalizado),

$$[K(t_1, \ldots, t_n) : F] = |\mathcal{S}_n| = n!,$$

e assim pelo discutido acima $F = K(s_1, \ldots, s_n)$. □

Corolário 14.3.3. *Todo polinômio simétrico em $t_1, \ldots, t_n$ sobre K pode ser escrito como uma expressão racional em $s_1, \ldots, s_n$.*

Demonstração. Ora, polinômios simétricos estão no corpo fixo F. □

Lema 14.3.4. *Com a notação acima, $s_1, \ldots, s_n$ são elementos transcendentes independentes sobre K.*

Demonstração. Como $K(t_1, \ldots, t_n)$ é uma extensão finita de $K(s_1, \ldots, s_n)$, temos que ambos têm o mesmo grau de transcendência sobre K, digamos, n. Portanto, os s_j são independentes, pois, caso contrário o grau de transcendência de $K(s_1, \ldots, s_n) : K$ seria menor do que n. □

Definição 14.3.5. *Seja K um corpo e sejam $s_1, \ldots, s_n$ elementos transcendentes sobre K. O polinômio geral de grau n sobre K é o polinômio,*

$$t^n - s_1 t^{n-1} + s_2 t^{n-2} - \ldots + (-1)^n s_n$$

sobre o corpo $K(s_1, \ldots, s_n)$.

Teorema 14.3.6. *Sejam K um corpo qualquer, g um polinômio geral de grau n sobre K (na realidade sobre $K(s_1, \ldots, s_n)$), e $Gal(g, K(s_1, \ldots, s_n))$ o corpo de decomposição de g sobre $K(s_1, \ldots, s_n)$. Então, os zeros $t_1, \ldots, t_n$ de g em $Gal(g, K(s_1, \ldots, s_n))$ são elementos independentes transcendentes sobre K, e o grupo de Galois de $Gal(g, K(s_1, \ldots, s_n)) : K(s_1, \ldots, s_n)$ é simétrico ao grupo $\mathcal{S}_n$.*

Demonstração. A extensão $Gal(g, K(s_1, \ldots, s_n)) : K(s_1, \ldots, s_n)$ é finita pelo Teorema 8.2.3, portanto, o grau de transcendência de $Gal(g, K(s_1, \ldots, s_n)) : K$ é igual ao, de $K(s_1, \ldots, s_n) : K$, digamos, n. Como $Gal(g, K(s_1, \ldots, s_n)) = K(t_1, \ldots, t_n)$, os t_j são elementos transcendentes independentes sobre K, já que, qualquer relação algébrica entre eles diminuiria o grau de transcendência. Os s_j são agora os polinômios elementares simétricos em $t_1, \ldots, t_n$ pelo Teorema 14.2.2. Como acima, $\mathcal{S}_n$ age como um grupo de automorfismos de $Gal(g, K(s_1, \ldots, s_n))$ e pelo Lema 14.3.2 o corpo fixo é $K(s_1, \ldots, s_n)$. Temos então, pelo Teorema 9.3.10, que, $Gal(g, K(s_1, \ldots, s_n)) : K(s_1, \ldots, s_n)$ é separável e normal (normalidade também segue da definição de $Gal(g, K(s_1, \ldots, s_n))$ como corpo de decomposição), agora, pelo Teorema que aparece na demonstração do Teorema 9.3.8, seu grau é $|\mathcal{S}_n| = n!$. Logo, pelo Teorema Fundamental da Teoria de Galois, o grupo de Galois tem ordem $n!$, e está contido em $\mathcal{S}_n$, portanto,temos que este é igual a $\mathcal{S}_n$. □

Teorema 14.3.7. *Se K é um corpo de característica zero e $n \geq 5$, então a polinomial geral de grau n sobre K (na verdade sobre $K(s_1, \ldots, s_n)$) é não solúvel por radicais.*

Demonstração. A demonstração segue do Teorema 13.1.10 e do Corolário 12.2.5. □

14.4 Extensões Cíclicas

Nesta seção, mostraremos que Extensões Cíclicas - extensões com Grupo de Galois cíclicos - estão extremamente relacionadas com Extensões Radicais.

Definição 14.4.1. *Consideremos $L : K$ uma extensão normal e finita com Grupo de Galois G. A norma de um elemento $a \in L$ é*

$$N(a) = \tau_1(a)\tau_2(a) \cdots \tau_n(a),$$

em que, $\tau_1, \ldots, \tau_n$ são elementos de G.

Temos que $N(a)$ pertence ao corpo fixo de G (Ora, temos um lema que dita: Se G é um grupo com os elementos distintos $g_1, \ldots, g_n$, e se, $g \in G$, então, como j varia de 1 a n, os elementos gg_j cobrem G e ocorrem precisamente uma única vez - vide [5]),e, se a extensão é também separável, temos que $N(a) \in K$.

Teorema 14.4.2 (Teorema 90 de Hilbert)**.** *Seja $L : K$ uma extensão normal finita com Grupo de Galois cíclico G gerado por um elemento τ. Então, $a \in L$ tem norma $N(a) = 1$ se, e somente se,*

$$a = \frac{b}{\tau(b)},$$

para algum $b \in L$, em que $b \neq 0$.

Demonstração. Consideremos $|G| = n$. Se $a = \frac{b}{\tau(b)}$ e $b \neq 0$, então

$$\begin{aligned} N(a) &= a\tau(a)\tau^2(a)\cdots\tau^{n-1}(a) \\ &= \frac{b}{\tau(b)}\frac{\tau(b)}{\tau^2(b)}\frac{\tau^2(b)}{\tau^3(b)}\cdots\frac{\tau^{n-1}}{\tau^n(b)} \\ &= 1, \end{aligned}$$

já que, $\tau^n = 1$.

Reciprocamente, suponhamos que $N(a) = 1$. Consideremos $c \in L$, e definamos

$$\begin{aligned} d_0 &= a_0 \\ d_1 &= (a\tau(a))\tau(c) \\ &\cdots \\ d_j &= [a\tau(a)\cdots\tau^j(a)]\tau^j(c), \end{aligned}$$

para $0 \leq j \leq n-1$. Então,

$$d_{n-1} = N(a)\tau^{n-1}(c) = \tau^{n-1}(c).$$

E mais,

$$d_{j+1} = a\tau(d_j) \quad (0 \leq j \leq n-2).$$

Definamos,

$$b = d_0 + d_1 + \ldots + d_{n-1}.$$

Afirmamos que podemos escolher c de modo a tornarmos $b \neq 0$. Suponhamos por absurdo, que não consigamos isto, ou seja, $b = 0$ para todas as escolhas de c. Assim, para $c \in L$,

$$\lambda_0\tau^0(c) + \lambda_1\tau(c) + \ldots + \lambda_{n-1}\tau^{n-1}(c) = 0,$$

em que,

$$\lambda_j = a\tau(a)\cdots\tau^j(a),$$

pertence a L. Logo, os τ^j automorfismos distintos são linearmente dependentes sobre L, contrariando o Lema de Dedekind (vide [5]).

Assim, podemos escolher c tal que $b \neq 0$. Deste modo,

$$\begin{aligned} \tau(b) &= \tau(d_0) + \ldots + \tau(d_{n-1}) \\ &= \left(\frac{1}{a}\right)(d_1 + \ldots + d_{n-1}) + \tau^n(c) \\ &= \left(\frac{1}{a}\right)(d_0 + \ldots + d_{n-1}) \\ &= \frac{b}{a}. \end{aligned}$$

Portanto, $a = \frac{b}{\tau(b)}$, como afirmamos. □

Teorema 14.4.3. *Suponhamos que $L : K$ seja uma extensão normal finita cujo Grupo de Galois, G, é cíclico, de ordem p, gerado por τ. Assumamos que a característica de K é 0 ou, prima a p, e que $t^p - 1$ se decompõe linearmente sobre K. Então, $L = K(\alpha)$, em que α é um zero de um polinômio irredutível $t^p - a$ sobre K para algum $a \in K$.*

Demonstração. Os p zeros de $t^p - 1$ de um grupo H, grupo este, que deve, ser cíclico (já que, qualquer grupo de ordem prima é cíclico). Sabemos que um grupo cíclico consiste de potências de um único elemento, assim, os zeros de $t^p - 1$ são potências de algum $\epsilon \in K$, em que, $\epsilon^p = 1$. Logo,

$$N(\epsilon) = \epsilon \cdots \epsilon = 1,$$

uma vez que, $\epsilon \in K$, e, portanto, $\tau^i(\epsilon) = \epsilon$, para todo i. Pelo Teorema 14.4.2, temos que $\epsilon = \frac{\alpha}{\tau(\alpha)}$ para algum $\alpha \in L$. Assim,

$$\tau(\alpha) = \epsilon^{-1}\alpha \quad \tau^2(\alpha) = \epsilon^{-2}\alpha \quad \ldots \quad \tau^j(\alpha) = \epsilon^{-j}\alpha,$$

e $a = \alpha^p$ é fixado por G. Logo, está em K. Agora, como $K(\alpha)$ é o corpo de decomposição para $t^p - a$ sobre K. Os K-automorfismos $1, \tau, \ldots, \tau^{p-1}$ mapeiam α em elementos distintos, então, eles são os p distintos K-automorfismos de $K(\alpha)$. Pelo Teorema Fundamental da Teoria de Galois, o grau de $[K(\alpha) : K] \geq p$. Mas, $[L : K] = |G| = p$, então $L = K(\alpha)$.

Portanto, $t^p - a$ é o polinômio minimal de α sobre K, caso contrário, deveríamos ter $[K(\alpha) : K] < p$. Sendo um polinômio minimal, $t^p - a$ é irredutível sobre K. □

Teorema 14.4.4. *Sejam K um corpo de característica 0, e $L : K$ uma extensão normal finita com Grupo de Galois solúvel G. Então, existe uma extensão R de L tal que $R : K$ é radical.*

Demonstração. Todas as extensões são separáveis já que K tem característica 0. Usaremos indução na $|G|$. O resultado é claro quando $|G| = 1$. Se $|G| \neq 1$, tomamos o máximo subgrupo normal H de G, este existe, já que, G é um grupo finito. Então, $\frac{G}{H}$ é simples, e

como H é maximal, temos que este é também solúvel pelo segundo item do Teorema 12.1.4. Pelo Teorema 12.2.3, $\frac{G}{H}$ é cíclico e de ordem prima p. Seja N o corpo de decomposição de $t^p - 1$ sobre L. Então, $N : K$ é normal, e pelo Teorema 8.2.3, L é um corpo de decomposição sobre K para algum polinômio f, assim, N é o corpo de decomposição sobre L de $(t^p - 1)f$, o que implica que, $N : K$ é normal pelo Teorema 8.2.3.

O Grupo de Galois de $N : L$ é abeliano pelo Lema 13.1.6, e, pelo Teorema Fundamental da Teoria de Galois, $Gal(L : K)$ é isomorfo a $\frac{Gal(N:K)}{Gal(N:L)}$. Pelo Teorema 12.1.4 (generalizado), $Gal(N : K)$ é solúvel. Seja M o subcorpo de N gerado por K e os zeros de $t^p - 1$. Então, $N : M$ é normal. Agora, $M : K$ é claramente radical, e como $L \subseteq N$, temos que o resultado desejado providenciará uma extensão R de N, tal que, $R : M$ é radical.

Afirmamos que, o Grupo de Galois de $N : M$ é isomorfo a um subgrupo de G. Mapeemos qualquer M - automorfismo τ de N em sua restrição $\tau|_L$. Como $L : K$ é normal, $\tau|_L$ é um K-automorfismo de L, e existe um homomorfismo de grupos

$$\Phi : Gal(N : M) \to Gal(L : K).$$

Se $\tau \in ker(\Phi)$, então τ fixa todos os elementos de M e L, o que gera N. Portanto, $\tau = 1$, e assim, Φ é um monomorfismo, o que implica que $Gal(N : M)$ é isomorfo a um subgrupo J de $Gal(L : K)$.

Se $J = \Phi(Gal(N : M))$ é um subgrupo próprio de G, então por indução, existe uma extensão R de N, tal que $R : M$ é radical.

A única possibilidade restante é que $J = G$. Então, podemos encontrar um subgrupo $I \triangle Gal(N : M)$ de índice p, digamos, $I = \Phi^{-1}(H)$. Consideremos P o corpo fixo de $I^{\dagger}$. Então, $[P : M] = p$ pelo Teorema Fundamental da Teoria de Galois, $P : M$ é normal, e ainda pelo mesmo teorema, $t^p - 1$ se decompõe linearmente em M. Pelo Teorema 14.4.3 (generalizado), $P = M(\alpha)$, em que $\alpha^p = a \in M$. Mas, $N : P$ é uma extensão normal com Grupo de Galois Solúvel de ordem menor do que $|G|$, e então, por indução existe uma extensão R de N tal que $R : P$ é radical. Ora, $R : M$ é radical e o teorema está provado. □

Terminaremos este Trabalho de Conclusão de Curso com o seguinte Teorema:

Teorema 14.4.5. *Sobre um corpo de característica zero, um polinômio é solúvel por radicais se, e somente se, este tem Grupo de Galois solúvel.*

Demonstração. A demonstração deste teorema segue dos Teoremas 13.1.10 e 14.4.4. □

.

Referências Bibliográficas

[1] EDWARDS, H. M. **Galois Theory**. New York: Springer, 3ª ed., 1998.

[2] EVES, H. **Introdução à história da matemática**; tradução: Hygino H. Domingues. Campinas: Editora Unicamp, 5ª ed., 2011.

[3] GONÇALVES, A. **Introdução à Álgebra**. Rio de Janeiro: IMPA, 1977.

[4] MONTEIRO, J. L. H. **Fundamentos de Álgebra**. Rio de Janeiro: IMPA, 1969.

[5] STEWART, I. **Galois Theory**. Chapman & Hall/CRC, 3ª ed., 2004.

Índice Remissivo