Gabriela Alexandra da Cruz Barreiros

GRUPOS E EXTENSÕES DE GALOIS

Departamento de Matemática Pura
Faculdade de Ciências da Universidade do Porto
2005

O presidente do júri,

António Machado

Gabriela Alexandra da Cruz Barreiros

GRUPOS E EXTENSÕES DE GALOIS

Tese submetida à Faculdade de Ciências da Universidade do Porto para obtenção do grau de Mestre em Matemática – Ensino da Matemática.

Departamento de Matemática Pura

Faculdade de Ciências da Universidade do Porto

Setembro, 2005

Conteúdo

Em 1830, Galois associa um grupo, o qual é hoje conhecido como sendo o grupo de Galois, a uma dada equação polinomial $f(x) = 0$. Dado $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$, com coeficientes $a_0, a_1, ..., a_{n-1} \in \mathbb{K}$ e raízes $\alpha_1, ..., \alpha_n$ nalguma extensão de $\mathbb{K}$, formamos um corpo Δ tal que Δ é o menor corpo que contém $\mathbb{K}$ e $\alpha_1, ..., \alpha_n$. Assim construído, a Δ dá-se o nome de corpo de decomposição de $f(x)$. O grupo de Galois de f sobre $\mathbb{K}$ é o grupo de todos os $\mathbb{K}$-automorfismos de Δ e nota-se por $G(\Delta : \mathbb{K})$. Mostra-se que é, a menos de isomorfismo, um subgrupo de S_n, o grupo simétrico em n elementos.

Um grupo é simples se não tem subgrupos normais. Um subgrupo H de um grupo G é normal se para todo $g \in G$, $gHg^{-1} = H$. Nota-se por $H \leq G$ o facto de H ser subgrupo de G e por $H \trianglelefteq G$ o facto de H ser subgrupo normal de G. Todo o grupo finito pode ser expresso da forma

$$id = H_1 \trianglelefteq H_2 \trianglelefteq ... \trianglelefteq H_r = G,$$

onde cada H_i/H_{i-1} é simples. Se cada um dos grupos quocientes simples obtidos for cíclico, então G diz-se solúvel. Se para G tomarmos o grupo $G(\Delta : \mathbb{K})$, onde Δ e f são como acima, dizemos que equação

$$f(x) = 0$$

é resolúvel por radicais se é possível calcular os zeros de $f(x)$ a partir dos coeficientes de $\mathbb{K}$ através um números finito de adições, diferenças, produtos, quocientes e extracções de raízes. Galois demonstra que a equação $f(x) = 0$ é resolúvel por radicais se e só se $G(\Delta : \mathbb{K})$ é um grupo solúvel. Galois observa que o grupo simétrico S_5 não tem essa propriedade, o que explica o facto de a equação geral do 5° grau não ser resolúvel por radicais, ou, por outras palavras, de não existir uma fórmula resolvente geral com radicais para as equações do 5° grau. A teoria dos grupos, criada por Galois no decurso da sua investigação sobre a resolubilidade de equações, teve posteriormente enorme desenvolvimento noutras áreas. Também a teoria dos corpos e das suas extensões se veio a revelar fundamental noutras áreas da matemática.

A dificuldade em calcular o grupo de Galois de certos polinómios é um dos aspectos desta teoria que se mantém insatisfatório. Assim, a correspondência entre equações polinomiais de grau n e subgrupos de S_n só é viável para valores muito pequenos de n. Como é impossível compreender completamente esta correspondência, para todo n, é natural levantar a seguinte questão: Será que todos os subgrupos de S_n ocorrem, pelo menos uma vez, nesta correspondência, isto é, será que todo o subgrupo de S_n corresponde a algum

polinómio de grau n? Esta questão é uma formulação do Problema Inverso da Teoria de Galois. Hilbert foi pioneiro no estudo deste problema. Ele começou por mostrar, através do seu teorema da irredutibilidade, que é suficiente que grupos ocorram como grupos de Galois de polinómios sobre o corpo $\mathbb{Q}(x)$. O facto de existirem várias extensões de Galois de determinado tipo não isomorfas leva à introdução do conceito de rigidez. Este garante-nos que, sob determinadas condições, um dado grupo finito ocorre como grupo de Galois sobre $\mathbb{Q}$, e que a extensão de Galois associada é única, a menos de isomorfismo.

Começamos no capítulo 1, por rever alguns conceitos básicos sobre polinómios, extensões e teoria de Galois necessários para o desenvolvimento do trabalho. A maioria das demonstrações será omitida.

No capítulo 2, será demonstrado que, para todo o inteiro positivo n, existe um polinómio em $\mathbb{Q}$ cujo grupo de Galois é isomorfo a S_n. Neste capítulo será essencial a utilização do Teorema de Hilbert. Este permite-nos, dado um polinómio irredutível $f(x_1, x_2, ..., x_n, y)$ em $n+1$ variáveis sobre $\mathbb{Q}$, concluir que existem valores racionais para $x_1, x_2, ..., x_n$ para os quais o polinómio resultante em y seja irredutível sobre $\mathbb{Q}$.

Os números construtíveis são a base do capítulo 3. Um número real α diz-se construtível se existe um segmento de comprimento $|\alpha|$ obtido a partir de um segmento de recta unitário num número finito de passos usando apenas uma régua não graduada e um compasso. Veremos que, sendo α um real construtível, então o seu grau sobre $\mathbb{Q}$, $\deg_{\mathbb{Q}} \alpha$, é uma potência de 2. No entanto, também será visto que esta não é uma condição suficiente, uma vez que existem reais α tais que $\deg_{\mathbb{Q}} \alpha$ é uma potência de 2 e α não é construtível. A demonstração deste teorema assentará no Teorema demonstrado no capítulo 2.

No capítulo 4 será dada uma condição necessária e suficiente para um dado polinómio ser resolúvel por radicais. Mostra-se também que, para todo $n \geq 5$, existem polinómios em que nenhuma das suas raízes pode ser exprimível por radicais.

No capítulo 5 começamos por introduzir o conceito de pontos de ramificação e de classes de conjugação de uma dada extensão de Galois. Introduzimos à custa destes conceitos certas classes de equivalência, formadas por um grupo de Galois, os pontos de ramificação e o conjunto das classes de conjugação associadas aos pontos de ramificação, e demonstra-se que, a menos de isomorfismo, para cada classe de equivalência dada, existe uma única extensão de Galois finita de $\mathbb{C}(x)$. A existência de tais extensões é-nos garantida

pelo teorema de Riemann, o qual será apenas enunciado, não se conhecendo demonstração algébrica.

Capítulo 1

Preliminares

Começamos por relembrar alguns conceitos importantes para o trabalho. Neste capítulo muitas das demonstrações serão omitidas. Os resultados podem ser encontrados em [3], [4] e [8].

1.1 Polinómios

Todos os anéis considerados neste trabalho são unitários e associativos. Um anel comutativo A diz-se um **domínio de integridade** se, para todo $a, b \in A$, sempre que $ab = 0$ então $a = 0$ ou $b = 0$.

Relembramos agora o conceito de característica.

Definição 1.1.1 *Seja A um anel. Consideremos o conjunto*

$$A_n = \{a \in A : na = 0\},$$

*para cada $n \in \mathbb{N}$. Se para qualquer natural n, se tem $A_n \neq A$, diz-se que A tem **característica zero** e escrevemos $car(A) = 0$. Caso contrário, se existe algum natural n tal que $A_n = A$, então a **característica de A** é o menor natural n_0 tal que $A_{n_0} = A$ e escrevemos $car(A) = n_0$.*

Definição 1.1.2 *Dizemos que $\mathbb{K}$ é um **corpo** se $\mathbb{K}$ é um anel comutativo onde $\mathbb{K} \setminus \{0\}$ é não vazio e $(\mathbb{K} \setminus \{0\}, \cdot)$ é um grupo abeliano.*

Definição 1.1.3 *Seja A um anel comutativo com identidade. Designamos por **polinómio** em A na incógnita x a expressão*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 = \sum_{i=i}^{n} a_i x^i,$$

onde $a_i \in A$ *e* $n \in \mathbb{N}$. *Aos elementos* a_i $(i = 0, 1, ..., n)$ *chamamos* ***coeficientes*** *de* $f(x)$. *Ao maior expoente de* x *que tem coeficiente não nulo em* $f(x)$ *chamamos o* ***grau*** *de* $f(x)$ *e escrevemos* ***deg f(x)*** *para designar este grau. Dizemos que o polinómio nulo tem grau* $-\infty$. *Seja* n *o maior inteiro tal que* $a_n \neq 0$. *Ao elemento* a_n *chamamos* ***coeficiente principal***. *Se* $a_n = 1$, *dizemos que* $f(x)$ *é um* ***polinómio mónico***.

É fácil verificar que o conjunto de todos os polinómios com coeficientes num anel A numa incógnita x forma um anel, o qual notaremos por $A[x]$, o **anel de polinómios** em x com coeficientes em A.

Dado D um domínio de integridade, $D[x]$ também o é. O seu **corpo das fracções** é

$$D(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in D[x], g(x) \neq 0 \right\}.$$

O teorema seguinte permite-nos a divisão de polinómios semelhante à divisão conhecida para os naturais.

Teorema 1.1.4 (Teorema da Divisão) *Sejam* $\mathbb{K}$ *um corpo e* $f(x), g(x) \in \mathbb{K}[x]$, *com* $f(x) \neq 0$. *Então existem polinómios únicos* $q(x), r(x) \in \mathbb{K}[x]$, *com* $\deg r(x) < \deg f(x)$ *tais que*

$$g(x) = q(x)f(x) + r(x).$$

Demonstração [3, Teoema I.2.5] □

Definição 1.1.5 *Sejam* $\mathbb{K}$ *um corpo e* $f(x), g(x) \in \mathbb{K}[x]$.

(a) Dizemos que $f(x)$ ***divide*** $g(x)$ *se existe* $q(x) \in \mathbb{K}[x]$ *tal que* $g(x) = q(x)f(x)$. *Neste caso escrevemos* $f(x) \mid g(x)$; *caso contrário,* $f(x) \nmid g(x)$.

(b) Dizemos que $d(x)$ *é um* ***máximo divisor comum*** *em* $\mathbb{K}[x]$ *de* $f(x)$ *e de* $g(x)$ *se* $d(x)$ *divide* $f(x)$, $d(x)$ *divide* $g(x)$ *e, se, sempre que algum* $h(x) \in \mathbb{K}[x]$ *divida* $f(x)$ *e* $g(x)$, *então* $h(x)$ *divide* $d(x)$. *Neste caso, escrevemos* ***m.d.c(f(x),g(x)) = d(x)***.

(c) Dizemos que $f(x)$ *e* $g(x)$ *são* ***primos entre si*** *se* 1 *é o máximo divisor comum de* $f(x)$ *e* $g(x)$, *isto é, se* $m.d.c(f(x), g(x)) = 1$.

Definição 1.1.6 *Sejam A um anel comutativo com identidade e $f(x) \in A[x]$ tal que $\deg f(x) \geq 1$. Dizemos que $f(x)$ é um* ***polinómio irredutível*** *em $A[x]$ se não existem $g(x), h(x) \in A[x]$ tais que $\deg g(x), \deg h(x) < \deg f(x)$ e $f(x) = g(x)h(x)$.*

Relembramos que se $f(x) \in D[x]$ for um polinómio mónico sobre um domínio de integridade D de grau ≥ 1, $f(x)$ é irredutível em $D[x]$ se e só se é irredutível em $F[x]$ onde F é o corpo das fracções de D.

Definição 1.1.7 *Sejam $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x]$. Dizemos que um elemento $\alpha \in \mathbb{K}$ é uma* ***raiz*** *de $f(x)$ em $\mathbb{K}$ se $f(\alpha) = 0$.*

Lema 1.1.8 *Sejam $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x]$. Um elemento $\alpha \in \mathbb{K}$ é uma raiz de $f(x)$ se e só se $x - \alpha$ divide $f(x)$.*

Demonstração Suponhamos que $x - \alpha$ divide $f(x)$. Então,

$$f(x) = (x - \alpha)g(x),$$

para algum $g(x) \in \mathbb{K}[x]$. Assim,

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0,$$

isto é, α é raiz de $f(x)$.

Por outro lado, suponhamos que $f(\alpha) = 0$. Pelo Teorema da Divisão (Teorema 1.1.4) existem polinómios únicos $q(x), r(x) \in \mathbb{K}[x]$, tais que

$$f(x) = q(x)(x - \alpha) + r(x)$$

com $\deg r(x) < \deg(x - \alpha) = 1$. Logo, $r(x)$ é um polinómio constante em $\mathbb{K}[x]$, digamos r. Assim,

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

Portanto $r = 0$, de onde concluímos que $x - \alpha$ divide $f(x)$. □

Definição 1.1.9 *Dizemos que α é uma raiz de* ***multiplicidade*** *m de $f(x)$ se $(x - \alpha)^m \mid f(x)$ mas $(x - \alpha)^{m+1} \nmid f(x)$. Se α for raiz de multiplicidade m onde $m \geq 2$, dizemos que α é uma* ***raiz múltipla*** *de $f(x)$.*

Definição 1.1.10 *Dizemos que um corpo $\mathbb{K}$ é* ***algebricamente fechado*** *se todo o polinómio $f(x) \in \mathbb{K}[x]$ de grau positivo admite uma raiz em $\mathbb{K}$.*

O teorema que se segue será de maior importância no próximo capítulo; se um polinómio em $n+1$ variáveis sobre $\mathbb{Q}$ for irredutível então podemos construir a partir deste um polinómio irredutível em $\mathbb{Q}[x]$. A demonstração é feita por indução em n e será omitida; pode no entanto ser encontrada em [7, Teorema 36].

Teorema 1.1.11 (Hilbert) *Seja $f(t_1, t_2, ..., t_n, x)$ um polinómio irredutível sobre $\mathbb{Q}$ em $n+1$ variáveis. Então, existe um número infinito de conjuntos de valores racionais $\alpha_1, \alpha_2, ..., \alpha_n$ tais que $f(\alpha_1, \alpha_2, ..., \alpha_n, x)$ é irredutível em $\mathbb{Q}[x]$.*

Recorde-se que um **domínio de factorização única** (**DFU**) é um domínio de integridade, no qual todo o elemento não nulo e que não seja invertível pode ser escrito como produto de primos a menos do produto por uma unidade e que esta decomposição é única a menos da ordem dos factores. Relembramos agora um critério importante que nos garante a irredutibilidade de alguns polinómios.

Teorema 1.1.12 (Critério de Eisenstein) *Seja $\mathbb{K}$ um corpo quociente de um domínio de factorização única A e $p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ um polinómio sobre A de grau n. Se existe um primo $p \in A$ tal que*

1. *p não divide a_n,*
2. *p divide $a_0, a_1, ..., a_{n-1}$,*
3. *p^2 não divide a_0*

então $p(x)$ é um polinómio irredutível sobre $\mathbb{K}$.

Demonstração [14, Teorema 37.5] □

1.2 Extensões de Corpos

Neste parágrafo revemos conceitos da teoria de corpos que serão necessários.

Definição 1.2.1 *Sejam* $\mathbb{K}$, $\mathbb{L}$ *corpos. Dizemos que* $\mathbb{L}$ *é uma* ***extensão*** *de* $\mathbb{K}$ *se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{L}$. *O símbolo* $\mathbb{L}/\mathbb{K}$ *designa a extensão* $\mathbb{L}$ *de* $\mathbb{K}$.

O lema seguinte é óbvio atendendo à definição de característica:

Lema 1.2.2 *Seja* $\mathbb{K}$ *um corpo de característica zero. Então qualquer extensão* $\mathbb{L}$ *de* $\mathbb{K}$ *também tem característica zero.*

Definição 1.2.3 *Sejam* $\mathbb{K}$, $\mathbb{L}$ *corpos tais que* $\mathbb{L}$ *é uma extensão de* $\mathbb{K}$. *O grau da extensão* $\mathbb{L}/\mathbb{K}$ *é a* ***dimensão*** *de* $\mathbb{L}$ *quando considerado como espaço vectorial sobre* $\mathbb{K}$ *e escrevemos* $[\mathbb{L} : \mathbb{K}]$ *para designar este grau. Dizemos que* $\mathbb{L}$ *é uma* ***extensão finita*** *de* $\mathbb{K}$ *se o grau* $[\mathbb{L} : \mathbb{K}]$ *for finito. Caso contrário, dizemos que* $\mathbb{L}$ *é uma* ***extensão infinita*** *de* $\mathbb{K}$.

Dados $\mathbb{K}$ e $\mathbb{F}$ subcorpos de um corpo $\mathbb{E}$ tais que $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ e $v_1, v_2, ..., v_n$ uma base de $\mathbb{E}$ sobre $\mathbb{K}$ e $u_1, u_2, ..., u_m$ uma base de $\mathbb{K}$ sobre $\mathbb{F}$, facilmente se demonstra que

$$\{u_i v_j : i = 1, 2, ..., m;\ j = 1, 2, ...n\}$$

é base de $\mathbb{E}$ sobre $\mathbb{F}$. Temos assim que :

Teorema 1.2.4 *Sejam* $\mathbb{K}$ *e* $\mathbb{F}$ *subcorpos de um corpo* $\mathbb{E}$ *tais que* $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$. *Se* $\mathbb{E}$ *é uma extensão finita de* $\mathbb{K}$ *e* $\mathbb{K}$ *é uma extensão finita de* $\mathbb{F}$, *então*

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}]\,[\mathbb{K} : \mathbb{F}]\,.$$

Demonstração [3, Teorema II.1.5] □

Definição 1.2.5 *Seja* $\mathbb{L}$ *uma extensão do corpo* $\mathbb{K}$ *e seja* $\lambda \in \mathbb{L}$. *Dizemos que* λ *é* ***algébrico*** *sobre* $\mathbb{K}$ *se* λ *é raiz de algum polinómio não nulo* $p(x) \in \mathbb{K}[x]$; *caso contrário, dizemos que* λ *é* ***transcendente*** *sobre* $\mathbb{K}$.

Definição 1.2.6 *Seja* $\mathbb{L}$ *uma extensão do corpo* $\mathbb{K}$. *Dizemos que* $\mathbb{L}$ *é uma* ***extensão algébrica*** *de* $\mathbb{K}$ *se todo o elemento de* $\mathbb{L}$ *é algébrico sobre* $\mathbb{K}$. *Caso contrário, dizemos que* $\mathbb{L}$ *é uma* ***extensão transcendente*** *de* $\mathbb{K}$.

Proposição 1.2.7 *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$ e seja $\alpha \in \mathbb{L}$ um elemento algébrico sobre $\mathbb{K}$. Existe um e um só polinómio irredutível mónico $f(x) \in \mathbb{K}[x]$ tal que $f(\alpha) = 0$, ou seja, tal que α é raiz de $f(x)$. Tem-se ainda que qualquer polinómio de $\mathbb{K}[x]$ que admita a raiz α é múltiplo de $f(x)$, isto é, $f(x)$ é o polinómio de grau mínimo entre os polinómios que admitem a raiz α.*

Definição 1.2.8 *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$ e seja $\alpha \in \mathbb{L}$ um elemento algébrico sobre $\mathbb{K}$. O **polinómio mínimo** de α sobre $\mathbb{K}$ é o único polinómio mónico $m_\alpha(x) \in \mathbb{K}[x]$ de grau mínimo de α sobre $\mathbb{K}$.*

Definição 1.2.9 *Seja $m_\alpha(x) \in \mathbb{K}[x]$ o polinómio mínimo de α sobre $\mathbb{K}$. Define-se **grau de α sobre $\mathbb{K}$** como sendo o grau de $m_\alpha(x)$, isto é,*

$$\deg_{\mathbb{K}} \alpha := \deg_{\mathbb{K}} m_\alpha(x)$$

Dado um corpo e uma sua extensão construímos agora subcorpos intermédios.

Definição 1.2.10 *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$ e S um subconjunto de $\mathbb{L}$. Ao menor subcorpo de $\mathbb{L}$ que contém $\mathbb{K} \cup S$ dá-se o nome de subcorpo de $\mathbb{L}$ gerado por $\mathbb{K} \cup S$ e representa-se por $\mathbb{K}(S)$.*

Definição 1.2.11 *Seja $\alpha \in \mathbb{L} \supset \mathbb{K}$ e uma aplicação $\psi : \mathbb{K}[x] \longrightarrow \mathbb{L}$ dada por $\psi(p(x)) = p(\alpha)$. Então designamos $\psi(\mathbb{K}[x])$ por $\mathbb{K}[\alpha]$.*

A aplicação introduzida na definição 1.2.11 é um homomorfismo de anéis. Como $\mathbb{K}[\alpha]$ é, por definição, a imagem de $\mathbb{K}[x]$ por um homomorfismo de anéis, $\mathbb{K}[\alpha]$ é um anel. Mais, podemos demonstrar que $\mathbb{K}[\alpha]$ é o menor anel que contém $\mathbb{K} \cup \{\alpha\}$.

Definição 1.2.12 *Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. Dizemos que $\mathbb{L}$ é uma **extensão simples** de $\mathbb{K}$ se existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$.*

Teorema 1.2.13 *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$ e seja $\alpha \in \mathbb{L}$. Então*

$$\mathbb{K}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{K}[x]\}$$

e

$$\mathbb{K}(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} : p(\alpha), q(\alpha) \in \mathbb{K}[x], q(\alpha) \neq 0 \right\}.$$

Tem-se também que $\mathbb{K}(\alpha)$ é o corpo das fracções de $\mathbb{K}[\alpha]$.

Demonstração A imagem da aplicação

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

é um subanel de $\mathbb{L}$. Seja R um subanel de $\mathbb{L}$ que contém $\mathbb{K}$ e α. Então, por ser fechado para a adição e para a multiplicação, $f(\alpha) \in R$, para todo $f(x) \in \mathbb{K}[x]$. Deste modo, $\{f(\alpha) : f(x) \in \mathbb{K}[x]\}$ está contido em todos os subanéis de $\mathbb{L}$ que contêm $\mathbb{K}$ e α. Como $\mathbb{K} \subseteq \operatorname{Im}\psi$ e $\alpha \in \operatorname{Im} f$, $\mathbb{K}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{K}[x]\}$. O corpo das fracções de $\mathbb{K}[\alpha]$ é o conjunto $\left\{\frac{p(\alpha)}{q(\alpha)} : p(\alpha), q(\alpha) \in \mathbb{K}[x], q(\alpha) \neq 0\right\}$, que está contido em qualquer subcorpo de $\mathbb{L}$ que contenha $\mathbb{K}[\alpha]$, logo é igual a $\mathbb{K}(\alpha)$. □

A proposição seguinte dá-nos uma descrição de $\mathbb{K}(\alpha)$ quando $\alpha \in \mathbb{L} \supseteq \mathbb{K}$ é um elemento algébrico sobre $\mathbb{K}$.

Proposição 1.2.14 *Seja $\alpha \in \mathbb{L} \supset \mathbb{K}$ um elemento algébrico sobre $\mathbb{K}$, $\alpha \notin \mathbb{K}$ e $m_\alpha(x)$ o seu polinómio mínimo sobre $\mathbb{K}$. Então:*

(a) $\mathbb{K}(\alpha)$, o subcorpo de $\mathbb{L}$ gerado por $\mathbb{K}$ e α, é isomorfo ao corpo das fracções $\mathbb{K}[x]/\langle m_\alpha(x)\rangle$;

(b) $\mathbb{K}(\alpha) \simeq \mathbb{K}[\alpha]$;

(c) $\mathbb{K}(\alpha)$ é o conjunto dos elementos da forma $a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_o$, onde n é o grau de $m_\alpha(x)$.

Proposição 1.2.15 *Se $\mathbb{L}$ é uma extensão de $\mathbb{K}$ e $\alpha \in \mathbb{L}$ é transcendente sobre $\mathbb{K}$, então $\mathbb{K}(\alpha) \simeq \mathbb{K}[x]$ como anéis.*

A proposição seguinte indica-nos o grau de uma extensão simples e algébrica:

Proposição 1.2.16 *Seja $\mathbb{K}(\alpha)$ uma extensão simples do corpo $\mathbb{K}$, onde α é algébrico com polinómio mínimo $m_\alpha(x)$ sobre $\mathbb{K}$. Então, $\{1, \alpha, \alpha^2, ..., \alpha^{n-2}, \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$ e $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg m_\alpha(x)$.*

Demonstração [3, Corolário II.2.5] □

Relacionamos agora o conceito de extensão algébrica com o de extensão finita.

Proposição 1.2.17 *Toda a extensão finita é algébrica.*

Demonstração Seja $\mathbb{L}/\mathbb{K}$ uma extensão finita. Então, por definição de extensão finita, $[\mathbb{L} : \mathbb{K}] = n < \infty$, isto é, $\mathbb{L}$ tem dimensão finita quando visto como espaço vectorial sobre $\mathbb{K}$. Assim, o conjunto de quaisquer $n+1$ vectores não nulos é linearmente dependente. Seja $\alpha \in \mathbb{L}$ e consideremos $1, \alpha, \alpha^2, ..., \alpha^n$. Então, existem $c_0, c_1, ..., c_n \in \mathbb{K}$, não todos nulos, tais que $\sum c_i \alpha^i = 0$. Deste modo, α é raiz do polinómio não nulo $f(x) = \sum c_i x^i$. Logo α é algébrico sobre $\mathbb{K}$. □

Observação 1.2.18 *O recíproco da Proposição 1.2.17 é falso.*

Tem-se que toda a extensão finita é algébrica. Extensões da forma $\mathbb{K}(\alpha_1, \alpha_2, ..., \alpha_n)$ onde os α_i's são algébricos sobre $\mathbb{K}$ são finitas.

Proposição 1.2.19 *Se $\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2, ..., \alpha_n)$ onde os α_i's são algébricos sobre $\mathbb{K}$ então $[\mathbb{L} : \mathbb{K}]$ é finita.*

Demonstração [3, Lema II.2.6] □

Combinando as Proposições 1.2.17 e 1.2.19 obtém-se:

Proposição 1.2.20 *A extensão $\mathbb{L}/\mathbb{K}$ é finita se e só se $\mathbb{L}$ é algébrico sobre $\mathbb{K}$ e existem $n \in \mathbb{N}$ e $\alpha_1, ..., \alpha_n \in \mathbb{L}$ tais que $\mathbb{L} = \mathbb{K}(\alpha_1, ..., \alpha_n)$.*

Demonstração [3, Lema II.2.6] □

Definição 1.2.21 *Seja $\mathbb{K}$ uma extensão de $\mathbb{F}$. Dizemos que $\mathbb{K}$ é um* ***fecho algébrico*** *de $\mathbb{F}$ se*

(i) *$\mathbb{K}/\mathbb{F}$ é uma extensão algébrica, e*

(ii) *$\mathbb{K}$ é algebricamente fechado.*

Neste caso, escrevemos $\mathbb{K} = \overline{\mathbb{F}}$.

A existência dos fechos algébricos é-nos garantida por [4, Corolário 7.3.5], sendo que a existência das extensões algebricamente fechadas de $\mathbb{F}$ são asseguradas por [4, Teorema 7.3.4].

Mostramos agora que, dado um elemento algébrico α sobre um corpo $\mathbb{K}$, raiz de um polinómio $f(x) \in \mathbb{K}[x]$, podemos construir um novo polinómio cujos coeficientes pertencem ao anel gerado pelos coeficientes de $f(x)$, mónico, que admite uma raiz do tipo $a_n\alpha$ que gera a mesma extensão simples que α.

Lema 1.2.22 *Seja α algébrico sobre um corpo $\mathbb{L}$ e $f(x) = \sum_{i=0}^{n} a_i x^i$ um polinómio sobre $\mathbb{L}$ de grau $n > 0$ tal que $f(\alpha) = 0$. Então*

$$g(x) = x^n + \sum_{i=0}^{n-1} a_i a_n^{n-i-1} x^i$$

é um polinómio mónico de grau n tal que $g(a_n\alpha) = 0$. Tem-se que ainda que:

a) $\mathbb{L}(\alpha) = \mathbb{L}(a_n\alpha)$;

b) se f for irredutível, g também o é.

Demonstração Seja α algébrico sobre $\mathbb{L}$, e f e g tais como na hipótese do Lema. Uma vez que

$$\begin{aligned} g(a_n\alpha) &= a_n^n\alpha^n + \sum_{i=0}^{n-1} a_i a_n^{n-i-1+i}\alpha^i \\ &= a_n^n\alpha^n + a_n^{n-1}\sum_{i=0}^{n-1} a_i\alpha^i \\ &= a_n^{n-1} f(\alpha), \end{aligned}$$

$g(a_n\alpha) = 0$. Como $a_n \in \mathbb{L}$ e $\alpha \in \mathbb{L}(\alpha)$, $\mathbb{L}(a_n\alpha) \subseteq \mathbb{L}(\alpha)$. Como $\alpha = a_n^{-1}a_n\alpha$, por argumento análogo tem-se a restante inclusão. Se f for irredutível, α é algébrico sobre $\mathbb{L}$ de grau n, logo

$$n = [\mathbb{L}(\alpha) : \mathbb{L}].$$

Como $\mathbb{L}(\alpha) = \mathbb{L}(a_n\alpha)$, $n = [\mathbb{L}(a_n\alpha) : \mathbb{L}]$, isto é, $a_n\alpha$ tem grau n sobre $\mathbb{L}$. Como $g(x)$ é de grau n sobre $\mathbb{L}$, é mónico e $g(a_n\alpha) = 0$, g é irredutível sobre $\mathbb{L}$. □

Introduzimos agora um novo conceito necessário:

Definição 1.2.23 *(a) Dizemos que um polinómio irredutível $f(x) \in \mathbb{K}[x]$ é **separável** quando não tem raízes múltiplas em qualquer corpo de decomposição.*

*(b) Dizemos que um **polinómio** qualquer é **separável** sobre $\mathbb{K}$ quando todos os seus factores irredutíveis o são.*

*(c) Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos. Um **elemento** $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ diz-se **separável** sobre $\mathbb{K}$ quando o seu polinómio mínimo o é.*

*(d) Uma **extensão** algébrica $\mathbb{L}$ diz-se **separável** sobre $\mathbb{K}$ quando todos os seus elementos são separáveis sobre $\mathbb{K}$.*

Teorema 1.2.24 *Seja $\mathbb{K}$ um corpo de característica zero e $f(x)$ um qualquer polinómio irredutível sobre $\mathbb{K}[x]$. Então $f(x)$ não tem raízes múltiplas em qualquer extensão de $\mathbb{K}$.*

Demonstração Suponhamos que $f(x)$ tem uma raiz múltipla α. Então, numa certa extensão de $\mathbb{K}$, poderíamos escrever

$$f(x) = (x - \alpha)^2 q(x),$$

para algum polinómio $q(x)$ com coeficientes nessa extensão. Assim, a derivada do polinómio $f(x)$,

$$f'(x) = 2(x - \alpha)q(x) + (x - \alpha)^2 q'(x),$$

admite α como raiz. Seja $p(x)$ o polinómio mínimo de α sobre $\mathbb{K}$. Dado que α é raiz de $f(x)$ e de $f'(x)$, $p(x)$ divide ambos os polinómios. Ora, sendo $f(x)$ irredutível, assim como $p(x)$, temos que $p(x) = \epsilon f(x)$, para algum $\epsilon \in \mathbb{K}\setminus\{0\}$ e, deste modo, $f(x) \mid f'(x)$. No entanto, $f'(x)$ tem grau inferior a $f(x)$, logo $f'(x) = 0$. Considerando

$$f(x) = c_0 + c_1 x + \ldots + c_n x^n,$$

com $c_n \neq 0$, temos que

$$f'(x) = c_1 + 2c_2x + ... + nc_nx^{n-1}.$$

Então, $nc_n = 0$ com $n \in \mathbb{N}$. Como $\mathbb{K}$ tem característica zero e qualquer sua extensão também a tem, chegamos a uma contradição. Portanto, $f(x)$ não pode ter raízes múltiplas. □

Uma vez que o corpo $\mathbb{Q}$ tem característica zero, o corolário seguinte é consequência imediata do Teorema anterior:

Corolário 1.2.25 *Seja $f(x)$ um polinómio irredutível em $\mathbb{Q}[x]$. Então, $f(x)$ não tem raízes múltiplas em qualquer extensão de $\mathbb{Q}$.*

Demonstramos agora que uma extensão finita e separável é uma extensão simples:

Teorema 1.2.26 (Teorema do Elemento Primitivo) *Seja $\mathbb{E}$ uma extensão finita de um corpo $\mathbb{F}$ de característica zero. Então, existe $\alpha \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(\alpha)$.*

Demonstração Seja $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_n)$. Para demonstrar que $\mathbb{E}$ é uma extensão simples de $\mathbb{F}$ usaremos indução em n. Se $n = 1$, $\mathbb{E} = \mathbb{F}(\alpha_1)$, logo não há nada a provar. Suponhamos que $\mathbb{E}_1 = \mathbb{F}(\alpha_1, ..., \alpha_{n-1})$. Por hipótese de indução podemos admitir que $\mathbb{E}_1$ é uma extensão simples de $\mathbb{F}$, isto é, que $\mathbb{E}_1 = \mathbb{F}(\beta)$, para algum $\beta \in \mathbb{E}_1$. Então, $\mathbb{E} = \mathbb{E}_1(\alpha_n) = \mathbb{F}(\beta, \alpha_n)$. A demonstração fica assim reduzida ao caso em que $n = 2$. Digamos que $\mathbb{E}$ é gerado por dois elementos α e β. Sejam $f(x)$ e $g(x)$ os polinómios sobre $\mathbb{F}$ irredutíveis que admitem as raízes α e β, respectivamente, e seja $\mathbb{E}'$ o corpo de decomposição destes polinómios. Sejam $\alpha = \alpha_1, ...\alpha_m$ e $\beta = \beta_1, ..., \beta_n$ as suas raízes. Pelo Teorema 1.2.24, as raízes α_i's são todas distintas. Consideremos as seguintes equações em x

$$\alpha_i + x\beta_j = \alpha + x\beta,$$

com $1 \leq i \leq m$ e $2 \leq j \leq n$. Estas equações têm exactamente uma solução em $\overline{\mathbb{F}}$,

$$x = \frac{\alpha - \alpha_i}{\beta_j - \beta}.$$

Seja k um elemento de $\mathbb{F}$ que não seja solução destas equações e tomemos $\gamma = \beta + k\alpha$. Demonstramos de seguida que a extensão $\mathbb{E}$ é gerada pelo elemento $\gamma = \beta + k\alpha$, isto é, vamos ver que $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. Ora, uma vez que $\gamma \in \mathbb{F}(\alpha, \beta)$, temos que $\mathbb{F}(\gamma) \subset \mathbb{F}(\alpha, \beta)$. Para mostrar que $\mathbb{F}(\alpha, \beta) \subset \mathbb{F}(\gamma)$ basta mostrar que $\alpha, \beta \in \mathbb{F}(\gamma)$. Comecemos por ver que $\beta \in \mathbb{F}(\gamma)$. Para tal, iremos ver que α é raiz de um polinómio de grau 1 sobre $\mathbb{F}(\gamma)$. Consideremos os polinómios $f(x)$ e $g(x)$ como anteriormente. Temos que $f(x)$ e $h(x) = g(\gamma - kx)$ são polinómios sobre $\mathbb{F}(\gamma)$ (note-se que $g(x) \in \mathbb{F}[x] \subset \mathbb{F}(\gamma)[x]$). Dada a forma como k, $g(x)$ e $h(x)$ foram escolhidos, α é raiz de ambos os polinómios. Assim, o máximo divisor comum destes polinómios é divisível pelo factor $x - \alpha$ em $\overline{\mathbb{F}}[x]$, admitindo portanto a raiz α. Como $f(x)$ não tem raízes múltiplas, o seu máximo divisor comum também não as tem, ou seja, a raiz α aparece apenas uma vez. Mas, pela escolha de k, os polinómios $f(x)$ e $g(\gamma - kx)$ não têm outra raiz em comum, dado que as raízes de $f(x)$ são da forma α_i, com $1 \leq i \leq m$, e $\gamma - k\alpha_i \neq \beta_j$, para todo o j. Portanto, o máximo divisor comum de $f(x)$ e $g(\gamma - kx)$ tem grau 1. Mas, o máximo divisor comum é um polinómio sobre $\mathbb{F}(\gamma)$, o corpo dos coeficientes de $f(x)$ e $g(\gamma - kx)$. Portanto, α é a raiz de um polinómio de grau 1 sobre $\mathbb{F}(\gamma)$, ou seja, $\alpha \in \mathbb{F}(\gamma)$. Como $\mathbb{F}(\gamma)$ é um corpo e $\beta = \gamma - k\alpha$, $\beta \in \mathbb{F}(\gamma)$. Portanto, $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. □

Definição 1.2.27 *Seja $\mathbb{L}$ um corpo. Dizemos que o polinómio $f(x) \in \mathbb{L}[x]$ se **decompõe** em $\mathbb{L}$ se $f(x) = \lambda(x-\alpha_1)...(x-\alpha_n)$, para alguns $\lambda, \alpha_1, ..., \alpha_n \in \mathbb{L}$.*

Definição 1.2.28 *Seja $f(x)$ um polinómio com coeficintes num corpo $\mathbb{K}$. Um **corpo de decomposição** de f(x) é uma extensão $\mathbb{L}$ de $\mathbb{K}$ em que:*

(a) $f(x)$ se decompõe em $\mathbb{L}$ num produto de termos de grau 1, e

(b) $\mathbb{L} = \mathbb{K}(\alpha_1, ..., \alpha_n)$ onde $\alpha_1, ..., \alpha_n$ são as raízes de $f(x)$ em $\mathbb{L}$.

O teorema seguinte garante-nos a existência de um corpo de decomposição de um polinómio $f(x) \geq \mathbb{K}[x]$ de grau $n \geq 1$, onde $\mathbb{K}$ é um corpo.

Teorema 1.2.29 *Seja $\mathbb{K}$ um corpo e $f(x)$ um polinómio de grau $n \geq 1$. Existe uma extensão $\mathbb{L}$ de $\mathbb{K}$ que é um corpo de decomposição de $f(x)$.*

Demonstração [4, Teorema 7.3.1] □

Os corpos de decomposição de polinómios sobre corpos $\mathbb{K}$ não são necessariamente únicos, no entanto, quaisquer corpos de decomposição de um mesmo polinómio sobre um corpo são isomorfos.

Proposição 1.2.30 *Seja $f(x)$ um polinómio sobre um corpo $\mathbb{K}$. Dois corpos de decomposição de $f(x)$ são isomorfos.*

Demonstração [4, Teorema 7.4.3] □

Pela Proposição 1.2.20 concluímos que dado um polinómio $f(x)$ sobre um corpo $\mathbb{K}$ o seu corpo de decomposição é uma extensão finita de $\mathbb{K}$. A proposição seguinte diz-nos que o grau dessa extensão é necessariamente inferior a $n!$, onde n é o grau do polinómio.

Proposição 1.2.31 *Seja $\mathbb{K}$ um corpo e seja $\mathbb{L}$ um corpo de decomposição sobre $\mathbb{K}$ do polinómio $f(x) \in \mathbb{K}[x]$. Então, $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ e $[\mathbb{L} : \mathbb{K}] \leq (\deg f)!$*

Demonstração [3, Lema III. 1.4] □

Definição 1.2.32 *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$. Dizemos que $\mathbb{L}/\mathbb{K}$ é uma **extensão normal** se cada polinómio irredutível $f(x) \in \mathbb{K}[x]$ que tem pelo menos uma raiz em $\mathbb{L}$ se decompõe em $\mathbb{L}$.*

O teorema seguinte caracteriza algumas extensões normais.

Teorema 1.2.33 *A extensão $\mathbb{L}/\mathbb{K}$ é finita e normal se e só se $\mathbb{L}$ é um corpo de decomposição de algum polinómio sobre $\mathbb{K}$.*

Demonstração [3, Teorema III.1.10] □

Proposição 1.2.34 *Seja $\mathbb{L}$ uma extensão finita e normal de um corpo $\mathbb{K}$ e $\mathbb{M}$ um corpo intermédio. Então $\mathbb{L}$ é uma extensão finita e normal de $\mathbb{M}$.*

Demonstração Pelo Teorema 1.2.33, $\mathbb{L}$ é o corpo de decomposição de algum polinómio em $\mathbb{K}[x]$, $f(x)$. Mas $f(x) \in \mathbb{M}[x]$, pois $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$. Assim, $\mathbb{L}$ é o corpo de decomposição de $f(x) \in \mathbb{M}[x]$. □

Introduzimos agora a noção de discriminante de um polinómio sobre $\mathbb{K}$. Este conceito dá-nos uma forma de verificar se o polinómio tem raízes múltiplas.

Definição 1.2.35 *Dado $p(x) \in \mathbb{K}[x]$ de grau n e mónico com raízes $r_1, ..., r_n$ nalguma extensão de $\mathbb{K}$, define-se o* ***discriminante*** *de $p(x)$ como sendo o produto*

$$D_{p(x)} = \prod_{i<j} (r_i - r_j)^2$$

A proposição seguinte é óbvia atendendo à definição de discriminante:

Proposição 1.2.36 *Seja $\mathbb{K}$ um corpo, $p(x) \in \mathbb{K}[x]$ um polinómio irredutível e $\alpha_1, ..., \alpha_n$ as raízes de $p(x)$ em alguma extensão de $\mathbb{K}$. Então $D_{p(x)} = 0$ se e só se $p(x)$ tem raízes múltiplas.*

Note-se que a Proposição anterior é equivalente a dizer que $D_{p(x)} = 0$ se e só se $p(x)$ não é um polinómio separável.

Introduzimos agora o conceito de polinómio simétrico.

Definição 1.2.37 *Dizemos que um polinómio em n variáveis $f(x_1, x_2, ..., x_n) \in \mathbb{K}[x_1, x_2, ..., x_n]$ é* ***simétrico*** *se se mantém invariante através das $n!$ permutações das suas variáveis.*

Existem polinómios simétricos fáceis de identificar: os polinómios simétricos elementares.

Definição 1.2.38 *Seja D um domínio de integridade e $x_1, x_2, ..., x_n$ n variáveis sobre D. Chamamos* ***polinómios simétricos elementares*** *nas incógnitas $x_1, x_2, ..., x_n$ aos polinómios $e_i \in D[x_1, x_2, ..., x_n]$ definidos do seguinte modo*

$$\begin{aligned}
e_1(x_1, x_2, ..., x_n) &= x_1 + x_2 + ... + x_n, \\
e_2(x_1, x_2, ..., x_n) &= x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_{n-1}x_n, \\
&\vdots \\
e_n(x_1, x_2, ..., x_n) &= x_1x_2...x_n.
\end{aligned}$$

Dado um domínio de integridade D, podemos, em $D[x_1, x_2, ..., x_n]$, escrever todos os polinómios simétricos à custa dos elementares definidos antes:

Teorema 1.2.39 (Teorema Fundamental de Polinómios Simétricos) *Seja D um domínio de integridade. Então cada polinómio simétrico em $D[x_1, x_2, ..., x_n]$ pode ser escrito como um polinómio sobre D nos polinómios simétricos elementares $e_1, e_2, ..., e_n$.*

Demonstração [3, Teorema I.6.3] □

Lema 1.2.40 *Seja $\mathbb{K}$ um corpo e seja $f(x) = x^n + a_1 x^{n-1} + ... + a_n \in \mathbb{K}[x]$. Sejam $\alpha_1, \alpha_2, ..., \alpha_n$ as raízes de $f(x)$ numa extensão $\mathbb{L}$ de $\mathbb{K}$, pelo que $f(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n) \in \mathbb{L}[x]$. Então,*

$$a_i = (-1)^i e_i(\alpha_1, \alpha_2, ..., \alpha_n),$$

onde as funções $e_1(\alpha_1, \alpha_2, ..., \alpha_n)$ representam o i-ésimo polinómio simétrico elementar nas incógnitas $\alpha_1, \alpha_2, ..., \alpha_n$.

Proposição 1.2.41 *Seja $f(x)$ um polinómio sobre $\mathbb{F}$ de grau n com raízes $\alpha_1, \alpha_2, ..., \alpha_n$. Se $f(x_1, x_2, ..., x_n)$ é um polinómio simétrico sobre $\mathbb{F}$ em n variáveis, então $f(\alpha_1, \alpha_2, ..., \alpha_n)$ é um elemento de $\mathbb{F}$.*

Demonstração Pelo Teorema 1.2.39, o polinómio $f(\alpha_1, \alpha_2, ..., \alpha_n)$ pode ser escrito como um polinómio sobre $\mathbb{F}$ nos polinómios simétricos elementares. Se $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$, então demonstra-se facilmente pelo Lema 1.2.40 que

$$e_i(\alpha_1, ..., \alpha_n) = \pm a_{n-i}/a_n \in \mathbb{F}.$$

Consequentemente, $f(\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{F}$. □

Usando o Lema 1.2.40, o Teorema Fundamental de Polinómios simétricos e um raciocínio da demonstração da Proposição 1.2.41 pode-se demonstrar que:

Proposição 1.2.42 *Seja $\mathbb{K}$ um corpo e $p(x) \in \mathbb{K}[x]$ de grau n. Tem-se que $D_{p(x)} \in \mathbb{K}$. Mais, se $\mathbb{K}$ for o corpo de fracções de um domínio de integridade R e $p(x) \in R[x]$, então $D_{p(x)} \in R$.*

Demonstração [14, página 567] □

1.3 Teoria de Galois

Neste parágrafo revemos alguns resultados bem conhecidos da teoria de Galois. A partir de extensões de corpos formamos grupos; os grupos de Galois associados a uma extensão. As propriedades dos grupos de Galois dependem das propriedades das extensões.

Definição 1.3.1 *Sejam* $\mathbb{L}$ *e* $\mathbb{M}$ *duas extensões de um corpo* $\mathbb{K}$. *Um* $\mathbb{K}$*-isomorfismo de* $\mathbb{M}$ *para* $\mathbb{L}$ *é um isomorfismo de corpos* $\varphi : \mathbb{M} \to \mathbb{L}$ *tal que* $\varphi(k) = k$, *para todo* $k \in \mathbb{K}$. *Um* $\mathbb{K}$***-automorfismo*** *de* $\mathbb{L}$ *é um* $\mathbb{K}$*-isomorfismo* $\varphi : \mathbb{L} \to \mathbb{L}$.

Duas extensões $\mathbb{F}$ *e* $\mathbb{F}'$ *de* $\mathbb{K}$ *dizem-se isomorfas se existir um* $\mathbb{K}$*-isomorfismo entre elas.*

Consideramos agora o conjunto de todos os $\mathbb{K}$-automorfismos de uma extensão $\mathbb{L}$ do corpo $\mathbb{K}$.

Teorema 1.3.2 *Seja* $\mathbb{L}$ *uma extensão de um corpo* $\mathbb{K}$. *O conjunto de todos os* $\mathbb{K}$*-automorfismos de* $\mathbb{L}$ *é um grupo, relativamente à operação de composição de aplicações.*

Definição 1.3.3 *O grupo constituído por todos os* $\mathbb{K}$*-automorfismos de* $\mathbb{L}$ *é designado por* ***grupo de Galois*** *da extensão* $\mathbb{L}$ *de* $\mathbb{K}$, *e será denotado por* $G(\mathbb{L} : \mathbb{K})$.

Definição 1.3.4 *Seja* G *um grupo de automorfismos de um corpo* $\mathbb{K}$. *O conjunto de elementos de* $\mathbb{K}$ *que ficam fixos por todos os automorfismos de* G *formam um subcorpo, chamado o* ***corpo fixo de*** G. *Este corpo fixo será denotado por* $\mathbb{K}^G$:

$$\mathbb{K}^G = \{\alpha \in \mathbb{K} : \varphi(\alpha) = \alpha, \text{ para todo } \varphi \in G\}.$$

Definição 1.3.5 *Seja* $f(x)$ *um polinómio sobre* $\mathbb{F}$ *e* $\mathbb{E}$ *o seu corpo de decomposição sobre* $\mathbb{F}$. *Dizemos que* $G(\mathbb{E} : \mathbb{F})$ *é o* ***grupo de Galois de*** f ***sobre*** $\mathbb{F}$.

Definição 1.3.6 *Seja* $\mathbb{L}$ *uma extensão do corpo* $\mathbb{K}$. *Dizemos que* $\mathbb{L}/\mathbb{K}$ *é uma* ***extensão de Galois*** *se for uma extensão finita, normal e separável sobre* $\mathbb{K}$.

A proposição seguinte relaciona extensões de Galois, corpos de decomposição e corpos fixos:

Proposição 1.3.7 *Seja* $\mathbb{L}$ *uma extensão de* $\mathbb{K}$ *e* G *o grupo de* $\mathbb{K}$*-automorfismos de* $\mathbb{L}$*. As seguintes afirmações são equivalentes:*

1. $\mathbb{L}$ *é uma extensão de Galois de* $\mathbb{K}$*;*
2. $\mathbb{L}$ *é um corpo de decomposição de um polinómio separável sobre* $\mathbb{K}$*;*
3. $\mathbb{L}^G = \mathbb{K}$.

Se qualquer uma destas condições se verifica, então $|G(\mathbb{L} : \mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.

Demonstração [4, Proposição 7.7.4] □

Proposição 1.3.8 *Seja* $f(x) \in \mathbb{K}[x]$ *um polinómio de grau* n*. Então, o seu grupo de Galois é isomorfo a um subgrupo de* S_n.

Demonstração [3, Proposição V.1.6] □

A seguir enunciamos a correspondência existente entre subgrupos de determinadas extensões de um corpo $\mathbb{K}$, as de Galois, e os corpos intermédios dessa mesma extensão. A bijecção existente permite-nos caracterizar corpos intermédios que são extensões normais de $\mathbb{K}$ em função dos subgrupos de alguns grupos de Galois.

Teorema 1.3.9 (Teorema da Correspondência de Galois) *Seja* $\mathbb{L}/\mathbb{K}$ *uma extensão de Galois e consideremos*

$S(G(\mathbb{L} : \mathbb{K})) = \{G : G \leq G(\mathbb{L} : \mathbb{K})\}$, *o conjunto dos subgrupos de* $G(\mathbb{L} : \mathbb{K})$

e

$CI(\mathbb{L}/\mathbb{K}) = \{\mathbb{M} : \mathbb{K} \subset \mathbb{M} \subset \mathbb{L}\}$, *o conjunto dos corpos intermédios entre* $\mathbb{K}$ *e* $\mathbb{L}$.

Considerem-se também as aplicações

$$\begin{array}{rccl} G(\mathbb{L} : \ ) : & CI(\mathbb{L}/\mathbb{K}) & \longrightarrow & S(G(\mathbb{L} : \mathbb{K})) \\ & \mathbb{M} & \mapsto & G(\mathbb{L} : \mathbb{M}), \quad \forall M : \mathbb{K} \subset \mathbb{M} \subset \mathbb{L} \end{array}$$

e

$$\begin{array}{rccl} fix() : & S(G(\mathbb{L}/\mathbb{K})) & \longrightarrow & CI(\mathbb{L}/\mathbb{K}) \\ & G & \mapsto & fix(G), \quad \forall G : G \leq G(\mathbb{L} : \mathbb{K}). \end{array}$$

(a) *As aplicações são bijecções, cada uma inversa uma da outra, que invertem inclusões.*

(b) *Tem-se que* $|G(\mathbb{L}:\mathbb{K})| = [\mathbb{L}:\mathbb{K}]$ *e* $|G| = |\mathbb{L}:fix(G)|$, $\forall M \in CI(\mathbb{L}/\mathbb{K}), \forall G \in S(G(\mathbb{L}:\mathbb{K}))$.

1. *Tem-se que* $G \trianglelefteq G(\mathbb{L}:\mathbb{K})$ *se e só se a extensão* $fix(G)/\mathbb{K}$ *é normal; e*
2. *Tem-se que a extensão* $\mathbb{M}/\mathbb{K}$ *é normal se e só se* $G(\mathbb{L}:\mathbb{M}) \trianglelefteq G(\mathbb{L}:\mathbb{K})$.

(c) *Se a extensão* $\mathbb{M}/\mathbb{K}$ *for normal então* $G(\mathbb{L}:\mathbb{K})/G(\mathbb{L}:\mathbb{M}) \simeq G(\mathbb{M}:\mathbb{K})$.

Demonstração [3, Teorema V.2.6] □

Teorema 1.3.10 (Artin) *Seja* $\mathbb{K}$ *um corpo e seja* G *um grupo finito de automorfismos de* $\mathbb{K}$*, de ordem* n*. Seja* $\mathbb{L} = \mathbb{K}^G$ *o corpo fixo de* G*. Então* $\mathbb{K}/\mathbb{L}$ *é uma extensão de Galois e o seu grupo de Galois é* G*. Tem-se que* $[\mathbb{K}:\mathbb{L}] = n$.

Demonstração [8] □

Como aplicação da teoria de Galois podemos demonstrar propriedades do discriminante de um dado polinómio sobre um corpo $\mathbb{K}$.

Proposição 1.3.11 *Seja* $\mathbb{K}$ *um corpo e* $p(x) \in \mathbb{K}[x]$ *um polinómio separável e irredutível. Sejam* $\alpha_1, ..., \alpha_n$ *as raízes de* $p(x)$ *num corpo de decomposição* $\mathbb{E}$ *de* $p(x)$*. Então* $D_{p(x)} \in \mathbb{K}$.

Demonstração Seja $\sigma \in G = G(\mathbb{E}:\mathbb{K})$. Note-se que $\sigma\left(D_{p(x)}\right) = D_{p(x)}$, logo $D_{p(x)} \in \mathbb{E}^G$. Como $\mathbb{E}$ é corpo de decomposição de um polinómio separável sobre $\mathbb{K}$, pela Proposição 1.3.7, $\mathbb{E}^G = \mathbb{K}$, deduzindo-se o pretendido. □

Proposição 1.3.12 *Seja* $\mathbb{K}$ *um corpo e* $p(x) \in \mathbb{K}[x]$ *um polinómio separável e irredutível. Sejam* $\alpha_1, ..., \alpha_n$ *as raízes de* $p(x)$ *num corpo de decomposição* $\mathbb{E}$*. Então* $D_{p(x)}$ *é um quadrado perfeito em* $\mathbb{K}$ *se e só se o grupo de Galois de* $p(x)$*,* $G(\mathbb{E}:\mathbb{K})$*, é um subgrupo de* A_n.

Demonstração Seja $\sigma \in G = G(\mathbb{E} : \mathbb{K})$ e $d = \sqrt{D_{p(x)}} = \prod_{i<j} (r_i - r_j)$. Pela Proposição 1.3.8 podemos pensar em σ como sendo uma permutação do conjunto dos zeros de $p(x)$. Tal como na demonstração da Proposição 1.3.11, $\mathbb{E}^G = \mathbb{K}$. Tem-se então que $d \in \mathbb{K}$ se e só se $d \in \mathbb{E}^G$, isto é, se e só se $\sigma(d) = d$. Mas tal só acontece se σ for uma permutação par, logo, G é um subgrupo de A_n. □

Capítulo 2

S_n como grupo de Galois

Neste capítulo demonstramos que dado $n \in \mathbb{N}$ e S_n, o grupo simétrico em n elementos, existe um polinómio em $\mathbb{Q}[x]$ cujo grupo de Galois é isomorfo a S_n (Teorema 2.3.5).

Começamos por verificar na secção 1 que dado um corpo $\mathbb{K}$, se o grupo de Galois de um polinómio $f(x) \in \mathbb{K}[x]$ de grau n é isomorfo a S_n, então f é irredutível sobre $\mathbb{K}$. Na secção 2 estudamos elementos $\alpha_1, ..., \alpha_n$ algebricamente independentes sobre $\mathbb{Q}$. Mostramos que dado n elementos algebricamente independentes sobre $\mathbb{Q}$, as suas $n!$ permutações induzem $\mathbb{Q}$-automorfismos na extensão gerada por estes elementos. Finalmente na secção 3 tomamos elementos $\alpha_1, ...\alpha_n$ algebricamente independentes sobre $\mathbb{Q}$ e à custa destes definimos $f(x)$ e $b_1, ..., b_n \in \mathbb{Q}(\alpha_1, ..., \alpha_n)$ que permitirão demonstrar o resultado pretendido.

2.1 Preliminares

Sabemos pela Proposição 1.3.8 que o grupo de Galois de um polinómio f de grau n sobre um corpo $\mathbb{K}$ é isomorfo a um subgrupo de S_n. Por definição, o corpo de decomposição de f não é mais que $\Lambda = \mathbb{K}(\alpha_1, ...\alpha_n)$ onde $\alpha_1, ..., \alpha_n$ são as raízes de $f(x)$. Sabemos também que zeros de factores irredutíveis de $f(x)$ são transformados sob acção de elementos de $G(\Lambda : \mathbb{K})$ em zeros desses mesmos factores. Note-se ainda que os automorfismos de $G(\Lambda : \mathbb{K})$ são determinados pelas imagens das raízes de $f(x)$.

Definição 2.1.1 *Seja $\mathbb{E}$ uma extensão algébrica de um corpo $\mathbb{F}$. Dois elementos $\alpha_1, \alpha_2 \in \mathbb{E}$ dizem-se* ***conjugados*** *se são zeros do mesmo polinómio*

irredutível de $\mathbb{F}[x]$.

Proposição 2.1.2 *Seja* $f(x)$ *um polinómio de grau n sobre um corpo* $\mathbb{K}$ *cujo grupo de Galois é isomorfo a* S_n. *Então f é irredutível sobre* $\mathbb{K}$.

Demonstração Seja $f(x)$ um polinómio nas condições do enunciado e suponhamos, por redução ao absurdo, que $f(x)$ não é irredutível, isto é, que se pode escrever como produto de dois polinómios distintos não constantes. Assim, podemos tomar num corpo de decomposição do polinómio duas raízes, a_i e a_j, que pertencem a factores irredutíveis distintos, não sendo portanto conjugadas. Consequentemente, o grupo de Galois de $f(x)$ sobre $\mathbb{K}$ não conteria nenhum automorfismo que envia a_i em a_j, uma vez que este envia raízes de factores irredutíveis em raízes desses mesmos factores. Deste modo não poderia conter todas as permutações dos zeros de $f(x)$, logo não seria isomorfo a S_n. □

2.2 Elementos algebricamente independentes sobre $\mathbb{Q}$

Na secção 1.2. introduzimos a definição de elemento algébrico. Dada $\mathbb{F}$ extensão de $\mathbb{Q}$ e $\alpha \in \mathbb{F}$, dizemos que α é algébrico sobre $\mathbb{Q}$ se existir $p(x) \in \mathbb{Q}[x]$, não nulo, tal que $p(\alpha) = 0$. Podemos agora demonstrar que o conjunto dos elementos algébricos sobre $\mathbb{Q}$ é numerável, isto é, que existe uma bijecção entre este conjunto e $\mathbb{N}$.

Proposição 2.2.1 *O conjunto dos números algébricos sobre* $\mathbb{Q}$ *é numerável.*

Demonstração Notemos que todo o número algébrico é a raiz de algum polinómio de coeficientes inteiros. Comecemos por ver que o conjunto de tais polinómios é numerável. Consideremos a sequência de primos $p_1, p_2, p_3, \ldots$. A cada polinómio $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ não trivial associamos o racional positivo $p_1^{a_0}\, p_2^{a_1}\, p_3^{a_2} \ldots p_{n+1}^{a_n}$. Atendendo à decomposição dos naturais como produto de potências de primos, estabelecemos uma bijecção entre os racionais positivos diferentes de 1 e o conjunto dos polinómios sobre $\mathbb{Q}$. Como o conjunto dos racionais positivos diferentes de 1 é numerável, o conjunto dos polinómios com coeficientes inteiros é numerável, podendo os polinómios ser

listados como $f_1, f_2, f_3, \ldots$. Para obter o conjunto dos números algébricos em $\mathbb{Q}$, basta listar as raízes de f_1, de f_2, e assim sucessivamente, obtendo-se no final um conjunto numerável. □

Definição 2.2.2 *Dizemos que n elementos $a_1, a_2, ..., a_n$ são* ***algebricamente independentes*** *sobre $\mathbb{Q}$ se não existe um polinómio $p(x_1, x_2, ..., x_n) \in \mathbb{Q}[x_1, x_2, ..., x_n]$ tal que*

$$p(a_1, a_2, ..., a_n) = 0,$$

ou seja, se não existe uma relação algébrica entre eles.

Lema 2.2.3 *Para todo o n, existem n elementos algebricamente independentes sobre $\mathbb{Q}$.*

Demonstração Comecemos por reparar que, pelo Lema 2.2.1, o conjunto dos números algébricos sobre $\mathbb{Q}$ é numerável. Uma vez que $\mathbb{C}$ não é numerável, sabemos que existe um número a_1 transcendente sobre $\mathbb{Q}$, isto é, tal que a_1 não é raiz de qualquer polinómio de $\mathbb{Q}[x]$.

Note-se que $\mathbb{Q}(a_1) = \left\{ \frac{f(a_1)}{g(a_1)} : f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0 \right\}$ e $f(a_1), g(a_1) \neq 0$ uma vez que a_1 é transcendente sobre $\mathbb{Q}$. Assim, cada elemento é da forma

$$\frac{\alpha_n a_1^n + \alpha_{n-1} a_1^n + ... + \alpha_0}{\beta_m a_1^m + \beta_{m-1} a_1^{m-1} + ... + \beta_0}$$

Logo, $\mathbb{Q}(a_1)$ é um conjunto numerável.

Portanto, tal como anteriormente, podemos escolher um elemento a_2 transcendente sobre $\mathbb{Q}(a_1)$; de seguida um elemento a_3 transcendente sobre $\mathbb{Q}(a_1, a_2)$ e assim sucessivamente, até obtermos uma sequência a_1, a_2, ..., a_n, onde a_n é transcendente sobre $\mathbb{Q}(a_1, a_2, ..., a_{n-1})$.

Vejamos agora, por redução ao absurdo, que os elementos encontrados são algebricamente independentes sobre $\mathbb{Q}$. Para tal, suponhamos que existe um polinómio em $\mathbb{Q}[x_1, x_2, ..., x_n]$ tal que $p(a_1, a_2, ..., a_n) = 0$. Seja k o maior índice que aparece nesta relação ($1 \leq k \leq n$). Então, a_k seria algébrico sobre $\mathbb{Q}(a_1, a_2, ..., a_{k-1})$, o que é uma contradição, atendendo à escolha dos a_i's. Portanto $a_1, a_2, ..., a_n$ são algebricamente independentes sobre $\mathbb{Q}$ como se pretendia demonstrar. □

Mostramos agora, de que modo permutações de elementos algebricamente independentes sobre $\mathbb{Q}$ originam automorfismos das extensões geradas por esses elementos.

Lema 2.2.4 *Sejam a_1, a_2, ..., a_n n elementos algebricamente independentes sobre $\mathbb{Q}$ e $\mathbb{E} = \mathbb{Q}(a_1, a_2, ..., a_n)$. Então, cada uma das n! permutações do conjunto a_1, a_2, ..., a_n induz um automorfismo em $\mathbb{E}$ que mantém fixo $\mathbb{Q}$.*

Demonstração Note-se que toda a permutação $(a_1\ a_2\ ...\ a_n)$ se pode escrever como uma sequência de transposições $(a_1\ a_n)(a_1\ a_{n-1})...(a_1\ a_2)$.

Como a composição de automorfismos é um automorfismo, basta mostrar que toda a transposição (c, d) do conjunto $\{a_1, ..., a_n\}$ induz um automorfismo de $\mathbb{Q}(c, d)$ que mantém $\mathbb{Q}$ fixo.

Note-se que a extensão $\mathbb{E}$ obtida de $\mathbb{Q}$ se mantém invariante, quando trocamos a ordem dos a_i's. Consideremos a transposição que permuta a_i e a_j, e $\mathbb{K}$ a extensão de $\mathbb{Q}$ gerada por todos os outros a_i's, isto é, $\mathbb{K} = \mathbb{Q}(a_1, ..., a_{i-1}, a_{i+1}, ..., a_{j-1}, a_{j+1}, ..., a_n)$. Assim, $\mathbb{E} = \mathbb{K}(a_i, a_j)$.

Sejam $c = a_i$ e $d = a_j$. Então $\mathbb{E}$ ($= \mathbb{K}(c, d)$) pode ser representado por

$$\left\{ \frac{p(c,d)}{q(c,d)} : p, q \in \mathbb{K}[x_1, x_2]; q \neq 0 \right\}.$$

O candidato natural para o automorfismo induzido pela transposição que permuta os elementos c e d é a aplicação

$$\begin{array}{rccc} \phi: & \mathbb{K}(c,d) & \longrightarrow & \mathbb{K}(c,d) \\ & \frac{p(c,d)}{q(c,d)} & \longmapsto & \frac{p(d,c)}{q(d,c)}. \end{array}$$

Verificamos agora que esta aplicação está bem definida, que é bijectiva, que preserva a adição e a multiplicação e que mantém os elementos de $\mathbb{Q}$ invariantes.

Com vista a mostrar que ϕ está bem definida, consideramos

$$\frac{p_1(c,d)}{q_1(c,d)} = \frac{p_2(c,d)}{q_2(c,d)} \in \mathbb{K}. \tag{1}$$

Queremos ver que as imagens por ϕ destas duas representações são iguais, isto é, que

$$\frac{p_1(d,c)}{q_1(d,c)} = \frac{p_2(d,c)}{q_2(d,c)}. \tag{2}$$

Da equação (1) tem-se que $x = c$ e $y = d$ é solução da equação polinomial

$$p_1(x,y)q_2(x,y) - p_2(x,y)q_1(x,y) = 0$$

Como (c, d) são algebricamente independentes, não poderá existir um polinómio não trivial $p \in \mathbb{K}[x_1, x_2]$ tal que $p(c, d) = 0$. Portanto,

$$p_1(x, y)q_2(x, y) - p_2(x, y)q_1(x, y)$$

terá de coincidir com o polinómio nulo. Assim, qualquer par ordenado é solução desta equação. Em particular, (d, c) também é solução deste polinómio, ou seja, $p_1(d, c)q_2(d, c) - p_2(d, c)q_1(d, c) = 0$, deduzindo-se assim a equação (2).

Para mostrar que ϕ é injectiva, isto é, que

$$\phi\left(\frac{p_1(c,d)}{q_1(c,d)}\right) = \phi\left(\frac{p_2(c,d)}{q_2(c,d)}\right) \Longrightarrow \frac{p_1(c,d)}{q_1(c,d)} = \frac{p_2(c,d)}{q_2(c,d)}$$

ou seja, que

$$\frac{p_1(d,c)}{q_1(d,c)} = \frac{p_2(d,c)}{q_2(d,c)} \Longrightarrow \frac{p_1(c,d)}{q_1(c,d)} = \frac{p_2(c,d)}{q_2(c,d)},$$

basta usar um argumento análogo ao anterior.

Atendendo à forma como ϕ está definida, ϕ é obviamente sobrejectiva.

Sejam $\frac{p_1(c,d)}{q_1(c,d)}, \frac{p_2(c,d)}{q_2(c,d)} \in \mathbb{K}$ quaisquer. Tem-se que

$$\begin{aligned}
\phi\left(\tfrac{p_1(c,d)}{q_1(c,d)} + \tfrac{p_2(c,d)}{q_2(c,d)}\right) &= \phi\left(\tfrac{p_1(c,d)q_2(c,d)+p_2(c,d)q_1(c,d)}{q_1(c,d)q_2(c,d)}\right) \\
&= \tfrac{p_1(d,c)q_2(d,c)+p_2(d,c)q_1(d,c)}{q_1(d,c)q_2(d,c)} \\
&= \tfrac{p_1(d,c)}{q_1(d,c)} + \tfrac{p_2(d,c)}{q_2(d,c)}
\end{aligned}$$

e que

$$\begin{aligned}
\phi\left(\tfrac{p_1(c,d)}{q_1(c,d)} \times \tfrac{p_2(c,d)}{q_2(c,d)}\right) &= \phi\left(\tfrac{p_1(c,d)p_2(c,d)}{q_1(c,d)q_2(c,d)}\right) \\
&= \tfrac{p_1(d,c)p_2(d,c)}{q_1(d,c)q_2(d,c)} \\
&= \tfrac{p_1(d,c)}{q_1(d,c)} \times \tfrac{p_2(d,c)}{q_2(d,c)},
\end{aligned}$$

assim ϕ preserva a adição e a multiplicação.

Para concluir apenas notamos que esta aplicação mantém os elementos de $\mathbb{Q}$ invariantes uma vez que só impõe transformações a c e d, que são elementos de $\mathbb{E}\backslash\mathbb{Q}$. $\square$

2.3 Polinómios cujo grupo de Galois é S_n

Consideremos n elementos a_1, a_2, ..., a_n algebricamente independentes sobre $\mathbb{Q}$ e seja $f(x)$ o polinómio definido do seguinte modo

$$\begin{aligned} f(x) &= \prod_{i=1}^{n} (x - a_i) \\ &= x^n + b_1 x^{n-1} + ... + b_n, \end{aligned}$$

onde os b_i's são dados por:

$$\begin{aligned} b_1 &= -(a_1 + ... + a_n) \\ b_2 &= a_1 a_2 + ... + a_{n-1} a_n \\ &\vdots \\ b_i &= (-1)^i \times \text{(soma de todos os produtos de } i \text{ diferentes } a_i\text{'s)} \\ &\vdots \\ b_n &= (-1)^n a_1 a_2 ... a_n, \end{aligned}$$

isto é,

$$b_i = (-1)^i e_i(a_1, ..., a_n)$$

onde e_i é a i-ésima função simétrica de n variáveis.

Então:

Lema 2.3.1 *O polinómio $f(x)$ definido antes é irredutível sobre $\mathbb{Q}(b_1, b_2, ..., b_n)$. O grupo de Galois de $f(x)$ sobre $\mathbb{Q}(b_1, b_2, ..., b_n)$ é isomorfo a S_n.*

Demonstração Seja $\mathbb{E} = \mathbb{Q}(a_1, a_2, ..., a_n)$ e $\mathbb{K} = \mathbb{Q}(b_1, b_2, ..., b_n)$. Note-se que, atendendo à definição de f e dos b_i's, $\mathbb{E}$ é o seu corpo de decomposição.

Pelo Lema 2.2.4, cada permutação dos a_i's induz um automorfismo de $\mathbb{E}$ que fixa todos os elementos $\mathbb{K} = \mathbb{Q}(b_1, b_2, ..., b_n)$, e portanto, induz um elemento de $G(\mathbb{E} : \mathbb{K})$, pelo que, $|G(\mathbb{E} : \mathbb{K})| \geq n!$. Uma vez que o grupo de Galois do polinómio f, de grau n, é isomorfo a um subgrupo de S_n (Proposição 1.3.8), temos que

$$G(\mathbb{E} : \mathbb{K}) \simeq S_n.$$

Pela Proposição 2.1.2, f é irredutível sobre $\mathbb{K}$. □

Como $\mathbb{E} = \mathbb{Q}(a_1, a_2, ..., a_n)$ é uma extensão finita de $\mathbb{K} = \mathbb{Q}(b_1, b_2, ..., b_n)$, $\mathbb{E}$ é uma extensão simples de $\mathbb{K}$. No próximo lema mostramos de forma simples tal facto.

Lema 2.3.2 *Sejam $a_1, a_2, ..., a_n$ algebricamente independentes sobre $\mathbb{Q}$ e $\mathbb{E} = \mathbb{Q}(a_1, a_2, ..., a_n)$. Então existem inteiros $m_1, m_2, ..., m_n$ tais que $\mathbb{E} = \mathbb{K}(m_1a_1 + m_2a_2 + ... + m_na_n)$.*

A soma $m_1a_1 + m_2a_2 + ... + m_na_n$ assume $n!$ valores distintos, que correspondem às $n!$ permutações possíveis dos a_i's, onde $\mathbb{K} = \mathbb{Q}(b_1, b_2, ..., b_n)$.

Demonstração Uma vez que $\mathbb{E}$ é corpo de decomposição do polinómio $f(x) \in \mathbb{K}[x]$, pela Proposição 1.3.7, $\mathbb{E}$ é extensão de Galois de $\mathbb{K}$, logo finita. Note-se que atendendo à definição dos b_i's, $\mathbb{E} = \mathbb{Q}(a_1, a_2, ..., a_n) = \mathbb{K}(a_1, a_2, ..., a_n)$. Pelo Teorema do Elemento Primitivo (Teorema 1.2.26), esta extensão pode ser escrita como uma extensão simples. No Teorema 1.2.26 demonstra-se que existem inteiros $m_1, ..., m_n$ tais que $\mathbb{E} = \mathbb{K}\left(\sum_{i=1}^{n} m_ia_i\right)$. Pelo Lema 2.3.1 e Teorema 1.3.9,

$$[\mathbb{E} : \mathbb{K}] = |G(\mathbb{E} : \mathbb{K})| = n!.$$

Assim, o grau de $\sum_{i=1}^{n} m_ia_i$ sobre $\mathbb{K}$ é $n!$, ou seja, o grau do menor polinómio sobre $\mathbb{K}$ do qual $\sum_{i=1}^{n} m_ia_i$ é raiz é $n!$. Então, $\sum_{i=1}^{n} m_ia_i$ terá $n!$ conjugados os quais não são mais do que imagens de $\sum_{i=1}^{n} m_ia_i$ pelos $n!$ automorfismos de $G(\mathbb{E} : \mathbb{K})$. Tais automorfismos associam a $\sum_{i=1}^{n} m_ia_i$ somas idênticas com os a_i's permutados. Estes conjugados são todos distintos, uma vez que são raízes de polinómios irredutíveis que, pelo Teorema 1.2.24, não podem ter raízes múltiplas. Portanto, todas estas somas são distintas. □

Denotemos por $c_1, c_2, ..., c_{n!}$ os $n!$ valores distintos obtidos de $\sum_{i=1}^{n} m_ia_i$ permutando os a_i's.

Seja $g(x) = \prod_{i=1}^{n!} (x - c_i)$. Note-se que as permutações dos a_i's correspondem a permutações dos c_i's, não alterando portanto $g(x)$. Portanto, os coeficientes de $g(x)$ são polinómios simétricos avaliados em $(a_1, a_2, ..., a_n)$. Como estes a_i's são raízes de um polinómio sobre $\mathbb{K}$, por 1.2.41, os coeficientes de $g(x)$ pertencem a $\mathbb{K}$. O corpo de decomposição de $g(x)$ será então $\mathbb{K}(c_1, ..., c_n)$. Pela demonstração do Lema 2.3.2, $\mathbb{K}(c_1, ..., c_n) = \mathbb{E}$, logo o grupo de Galois de $g(x)$ é $G(\mathbb{E} : \mathbb{K}) \simeq S_n$. Assim, pela Proposição 2.1.2, $g(x)$ é irredutível.

Lema 2.3.3 *O grupo de g(x) sobre* $\mathbb{K}$ *é isomorfo a* S_n *e o polinómio g(x) é irredutível sobre* $\mathbb{K} = \mathbb{Q}(b_1, b_2, ..., b_n)$.

Acábamos de ver que tanto o grupo de Galois de f como o de g sobre $\mathbb{K}$ são isomorfos a S_n.

Construímos agora dois polinómios $F(t_1, t_2, ..., t_n, x)$ e $G(t_1, t_2, ..., t_n, x)$ de $n+1$ variáveis sobre $\mathbb{Q}$. O grau de cada um destes polinómios será n e $n!$, respectivamente, tal como f e g.

Comecemos por tomar n variáveis $s_1, s_2, ..., s_n$ e definir n funções t_i do seguinte modo:

$$t_i = (-1)^i e_i(s_1, s_2, ..., s_n),$$

onde e_i corresponde ao i-ésimo polinómio simétrico de $(s_1, s_2, ..., s_n)$.

Definamos também $n!$ funções u_i da seguinte forma

$$u_i = \sum_{i=1}^{n} m_i s_i$$

e todas as somas obtidas permutando os s_i's.

Construímos agora F e G;

$$\begin{aligned} F(t_1, t_2, ..., t_n, x) &= x^n + t_1 x^{n-1} + ... + t_n \\ &= \prod_{i=1}^{n} (x - s_i) \end{aligned}$$

e

$$G(t_1, t_2, ..., t_n, x) = \prod_{i=1}^{n!} (x - u_i).$$

Enquanto que para a função F temos uma representação explícita em termos de $t_1, t_2, ..., t_n$ e x, para G não temos. Sabemos que os coeficientes das potências de x em G podem ser escritas como polinómios em s_i's e que são simétricos como funções dos s_i's. Assim, pelo Teorema Fundamental dos Polinómios Simétricos (Teorema 1.2.39) sabemos que G representa uma função nas variáveis $t_1, t_2, ..., t_n$ e x. Note-se que $F(b_1, b_2, ..., b_n, x) = f(x)$ e $G(b_1, b_2, ..., b_n, x) = g(x)$.

Lema 2.3.4 *Os polinómios* F *e* G *são irredutíveis em* $\mathbb{Q}$.

Demonstração Consideremos os polinómios $G(t_1, t_2, ..., t_n, x)$ e $F(t_1, t_2, ..., t_n, x)$ sobre $\mathbb{Q}$ definidos anteriormente.

Suponhamos que F não é irredutível sobre $\mathbb{Q}$, isto é, que existem polinómios R e S não triviais de coeficientes racionais tais que

$$F(t_1, t_2, ..., t_n, x) = R(t_1, t_2, ..., t_n, x)S(t_1, t_2, ..., t_n, x).$$

Esta factorização, a existir, seria válida para quaisquer valores de $t_1, t_2, ..., t_n$, em particular, para $t_i = b_i = (-1)^i e_i(a_1, a_2, ..., a_n)$. Tendo R e S graus em x não inferior a um, esta substituição resultaria numa factorização de f, contrariando o facto de, pelo Lema 2.3.1, f ser irredutível sobre $\mathbb{Q}(b_1, ..., b_n)$.

Suponhamos agora que S tem grau 0 em x. Neste caso,

$$S(t_1, t_2, ..., t_n, x) = s(t_1, t_2, ..., t_n).$$

Então, o coeficiente de x^n no produto RS será dado por $r(t_1, t_2, ..., t_n)s(t_1, t_2, ..., t_n)$, sendo $r(t_1, t_2, ..., t_n)$ o coeficiente de x^n de $R(t_1, t_2, ..., t_n, x)$. Mas como $F(t_1, t_2, ..., t_n, x)$ tem coeficiente de x^n igual a 1, o grau do polinómio $r(t_1, t_2, ..., t_n)s(t_1, t_2, ..., t_n)$ terá de ser nulo. Visto que o grau do produto de polinómios corresponde à soma dos graus de cada factor, concluimos que r e s têm ambos grau zero em qualquer uma das variáveis, ou seja, r e s reduzem-se a constantes não nulas. Mas, neste caso, S também é uma constante e portanto a factorização $F = RS$ é uma factorização trivial, ou seja, F é irredutível em $\mathbb{Q}$.

Um argumento análogo prova a irredutibilidade de G. □

Demonstramos agora o resultado principal deste capítulo.

Teorema 2.3.5 *Para todo o inteiro positivo n, existe um polinómio em $\mathbb{Q}$ cujo grupo de Galois é isomorfo a S_n.*

Demonstração Seja $n \in \mathbb{N}$ e $G(t_1, t_2, ..., t_n, x) = \prod_{i=1}^{n!} (x - u_i)$ o polinómio sobre $\mathbb{Q}$ construído antes. Pelo Teorema de Hilbert (Teorema 1.1.11), podemos escolher racionais $\beta_1, \beta_2, ..., \beta_n$ tais que o polinómio

$$\widetilde{G}(x) = G(\beta_1, \beta_2, ..., \beta_n, x)$$

é irredutível em $\mathbb{Q}[x]$.

Pretendemos demonstrar que o grupo de Galois de

$$\widetilde{F}(x) = F(\beta_1, \beta_2, ..., \beta_n, x) = x^n + \beta_1 x^{n-1} + ... + \beta_n$$

é isomorfo a S_n.

Sejam $\alpha_1, \alpha_2, ..., \alpha_n$ as raízes de $\widetilde{F}$. Então, $m_1\alpha_1 + m_2\alpha_2 + ... + m_n\alpha_n$ pertence ao corpo de decomposição de $\widetilde{F}$, $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$. Por definição de G e de F, $m_1\alpha_1 + m_2\alpha_2 + ... + m_n\alpha_n$ é um zero de G, o qual é um polinómio irredutível de grau $n!$ sobre $\mathbb{Q}$. Assim existe em $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ um elemento de ordem $n!$ sobre $\mathbb{Q}$. Logo $[\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n) : \mathbb{Q}] \geq n!$. Portanto, o grupo de Galois de $\widetilde{F}$ tem ordem não inferior a $n!$.

Como este grupo corresponde ao conjunto das permutações dos $\alpha_1, \alpha_2, ..., \alpha_n$, a sua ordem poderá ser, no máximo, $n!$.

Deste modo, o grupo de Galois de $\widetilde{F}$ terá, precisamente, ordem $n!$, ou seja, é isomorfo a S_n. □

Capítulo 3

Números Construtíveis

Um dos problemas da geometria clássica consistia no traçado de diversas figuras e na realização de diversas construções, tendo como únicos instrumentos uma régua (não graduada) e um compasso. Um número real α diz-se construtível se for possível construir um segmento de recta de comprimento $|\alpha|$ a partir de um segmento de recta unitário num número finito de passos usando apenas uma régua e um compasso. Nesta secção, sempre que usarmos o verbo "construir" estaremos a falar em construir usando apenas régua e compasso.

Neste capítulo demonstramos que dado um real α, para que ele seja construtível é necessário que o grau de α sobre $\mathbb{Q}$ seja uma potência de 2. A condição obtida não é no entanto suficiente tal como é demonstrado na proposição 3.2.7. Para tal consideramos um polinómio sobre $\mathbb{Q}$ cujo grupo de Galois é isomorfo a S_n. A existência deste polinómio é-nos garantida pelo Teorema 2.3.5.

3.1 Preliminares

Dada uma régua (não graduada) e um compasso as operações que podemos realizar com estes instrumentos são chamadas construções fundamentais e são:

1. Dados dois pontos, podemos traçar uma recta que passa pelos dois pontos e prolongá-la até ao infinito nas duas direcções;

2. Dados dois pontos podemos traçar o segmento de recta que une os dois pontos;

3. Dado um ponto e um segmento de recta, podemos traçar a circunferência com centro nesse ponto e raio igual ao comprimento do segmento de recta.

O lema seguinte diz-nos que a soma e o produto de números reais construtíveis ainda é um número construtível.

A sua demonstração será omitida mas demonstração análoga é feita em 3.1.3.

Lema 3.1.1 *Dados segmentos de comprimentos* 1, α *e* β, *com* $\alpha > \beta$ *e* $\beta \neq 0$, *é possível construir segmentos de comprimentos* $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ *e* α/β.

Definição 3.1.2 *Dizemos que um número real* α *é* ***construtível*** *se, dado um segmento de comprimento 1, é possível construir, num número finito de passos, um segmento de comprimento* $|\alpha|$.

Pelo Lema 3.1.1 podemos concluir que todos os números racionais são construtíveis.

A proposição seguinte é apenas uma reformulação deste Lema usando o conceito de números reais construtíveis:

Proposição 3.1.3 *Sejam* α *e* β *dois reais construtíveis. Então também*

$$\alpha + \beta, \alpha - \beta, \alpha\beta \text{ e } \alpha/\beta$$

são construtíveis.

Demonstração Consideremos dois reais construtíveis α e β, com $\alpha > \beta$. Traçamos sobre uma recta s um segmento $[AB]$ de comprimento α e um segmento de recta $[CD]$ de comprimento igual a β de modo que B coincida com C. Construa-se uma circunferência com centro em B e raio $\overline{CD}$. A circunferência intersecta a recta s nos pontos D e E tais que B está entre A e D e E está entre A e B. Então, o comprimento de $[AD]$, $\overline{AD}$, é $\alpha + \beta$ e o de $[AE]$ é $\alpha - \beta$, concluindo-se que $\alpha + \beta$ e $\alpha - \beta$ são construtíveis.

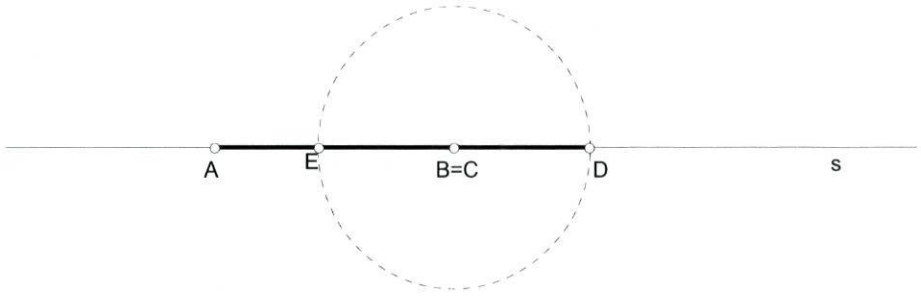

Figura 3.1: Construção da soma e da diferença de dois reais construtíveis

Com vista a demonstrar a segunda parte da Proposição, marcamos sobre uma recta dada s um segmento de recta $[AB]$ de comprimento igual a α. Por A, traçamos outra recta r, concorrente com a anterior. Em r marcamos a partir de A um segmento unitário, digamos $[AC]$, e o segmento $[AD]$ de comprimento igual a β. De seguida traçamos a recta t que contém os pontos B e C e construímos a recta t' paralela a t que passa por D. Seja P o ponto de intersecção das rectas t' e s.

Então o comprimento de $[AP]$, $\overline{AP} = \alpha\beta$, uma vez que, pelo Teorema de Tales,

$$\frac{\overline{AC}}{\overline{AD}} = \frac{\overline{AB}}{\overline{AP}}$$

isto é,

$$\frac{1}{\beta} = \frac{\alpha}{\overline{AP}}.$$

Concluímos assim que $\alpha\beta$ é construtível.

Nas mesmas condições do caso anterior, traçamos a recta t que contém os pontos B e D e construímos por C a recta t' paralela a t que intersecta a recta s no ponto Q.

Então $\overline{AQ} = \alpha/\beta$ uma vez que

$$\frac{\overline{AC}}{\overline{AD}} = \frac{\overline{AQ}}{\overline{AB}},$$

isto é,

$$\frac{1}{\beta} = \frac{\overline{AQ}}{\alpha}.$$

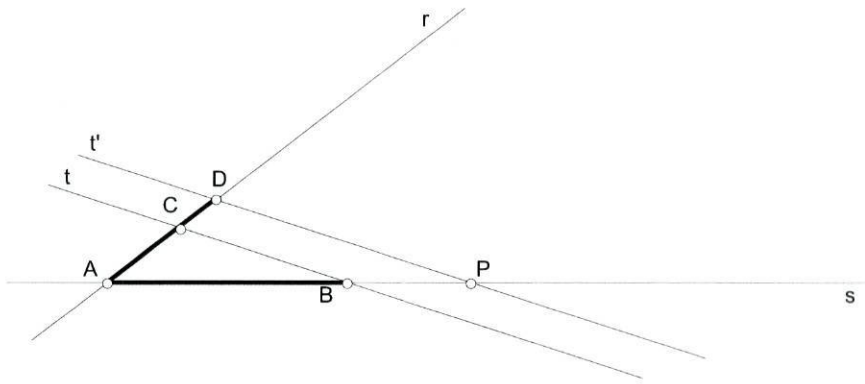

Figura 3.2: Construção do produto de dois reais construtíveis

□

Mostramos agora que se α é construtível, $\sqrt{\alpha}$ também o é.

Lema 3.1.4 *Dados segmentos de comprimentos* 1 *e* α *é possível construir um segmento de comprimento* $\sqrt{\alpha}$.

Demonstração Consideremos sobre uma recta s o segmento unitário $[AB]$ e o segmento $[BC]$ de comprimento $\overline{BC} = \alpha$. Seja M o ponto médio do segmento $[AC]$ e construa-se uma semicircunferência com centro em M e diâmetro $\overline{AC}$. De seguida construa-se a perpendicular s' a s pelo ponto B e seja D o ponto de intersecção da recta s' com a semicircunferência.

Então, $[BD]$ é um segmento de comprimento$\sqrt{\alpha}$ já que

$$\frac{\overline{BC}}{\overline{BD}} = \frac{\overline{BD}}{\overline{AB}},$$

isto é,

$$\frac{\alpha}{\overline{BD}} = \frac{\overline{BD}}{1},$$

concluindo-se o pretendido. □

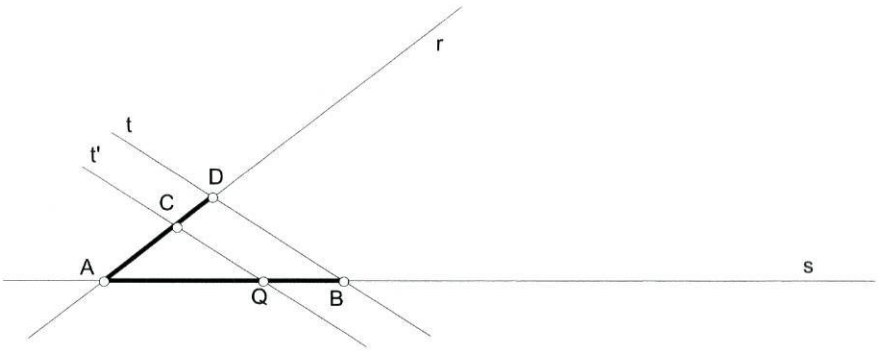

Figura 3.3: Construção do quociente de dois reais construtíveis

Definição 3.1.5 *Seja $\mathbb{F}$ um corpo. Designamos por* ***plano*** *de $\mathbb{F}$ o conjunto dos pares ordenados (x, y), com $x, y \in \mathbb{F}$.*

Entende-se por recta de $\mathbb{F}$ a recta que passa por dois pontos distintos do plano de $\mathbb{F}$ e por circunferência de $\mathbb{F}$ a circunferência cujo centro e algum ponto da circunferência pertencem ao plano de $\mathbb{F}$.

Lema 3.1.6 *Toda a recta do plano de $\mathbb{F}$ pode ser representada por uma equação do tipo*

$$ax + by + c = 0,$$

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

Toda a circunferência pode ser representada por uma equação do tipo

$$x^2 + y^2 + ax + by + c = 0,$$

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

3.2 Extensões quadráticas

Relacionamos agora o conceito de número construtível com a existência de certas extensões. Começamos por introduzir o conceito de extensão quadrática de um corpo.

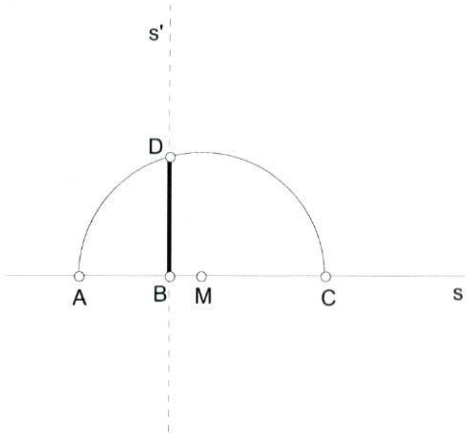

Figura 3.4: Extracção da raiz quadrada de um real construtível

Definição 3.2.1 *Seja $\mathbb{F}$ um corpo. Dizemos que $\mathbb{F}(k)$ é uma* ***extensão quadrática*** *de $\mathbb{F}$ se $k^2 \in \mathbb{F}$ e $k \notin \mathbb{F}$.*

Lema 3.2.2 *O ponto de intersecção de duas rectas de $\mathbb{F}$ pertence a $\mathbb{F}$. Os pontos de intersecção de uma recta com uma circunferência de $\mathbb{F}$, assim com os pontos de intersecção de duas circunferências de $\mathbb{F}$ pertencem ao plano de $\mathbb{F}$ ou ao plano de alguma extensão quadrática de $\mathbb{F}$.*

Demonstração O caso da intersecção das duas rectas de $\mathbb{F}$ equivale à solução das duas equações

$$\begin{aligned} a_1x + b_1y + c_1 &= 0 \\ a_2x + b_2y + c_2 &= 0, \end{aligned}$$

com a_1, a_2, b_1, b_2, c_1, $c_2 \in \mathbb{F}$ (Lema 3.1.6). É óbvio que a resolução deste sistema envolve operações racionais, estando as soluções x e y em $\mathbb{F}$, ou seja, (x, y) pertence ao plano de $\mathbb{F}$, $\{(x, y) : x, y \in \mathbb{F}\}$.

O caso da intersecção de uma recta com uma circunferência em $\mathbb{F}$ reduz-se à solução do sistema de equações em $\mathbb{F}$

$$\begin{cases} a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0, \end{cases}$$

com a_1, a_2, b_1, b_2, c_1, $c_2 \in \mathbb{F}$. Como os coeficientes a_1 e b_1 não podem ser simultâneamente zero, a primeira equação pode ser resolvida em ordem a qualquer uma das duas variáveis. Sem perda de generalidade consideremos a equação resolvida em ordem a y:

$$y = -\frac{c_1}{b_1} - \frac{a_1}{b_1}x.$$

Substituindo na segunda equação obtemos uma equação do segundo grau em x com coeficientes em $\mathbb{F}$. Sabemos que, utilizando a fórmula resolvente, obtemos soluções do tipo $A \pm B\sqrt{k}$, com A, B, $k \in \mathbb{F}$ e $k \geq 0$. Substituindo estas soluções na primeira equação obtemos uma solução para y do tipo $A' \pm B'\sqrt{k}$, com A', B', $k \in \mathbb{F}$. Assim, quando $\sqrt{k} \in \mathbb{F}$ os pontos pertencem a $\mathbb{F}$. Caso contrário, isto é, quando $\sqrt{k} \notin \mathbb{F}$, os pontos pertencem ao plano de $\mathbb{F}(\sqrt{k})$.

No caso da intersecção de duas circunferências, as equações:

$$\begin{aligned} x^2 + y^2 + a_1x + b_1y + c_1 &= 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 &= 0 \end{aligned}$$

podem ser subtraídas, obtendo-se uma equação linear com coeficientes em $\mathbb{F}$. A equação obtida pode ser resolvida em simultâneo com uma das equações da circunferência, reduzindo este caso ao caso anterior. □

Lema 3.2.3 *Seja $\mathbb{E}$ uma extensão quadrática de $\mathbb{F}$. Então $[\mathbb{E} : \mathbb{F}] = 2$.*

Demonstração Pela definição de extensão quadrática, $\mathbb{E} = \mathbb{F}(\sqrt{k})$, para algum $k \in \mathbb{F}$ tal que $\sqrt{k} \notin \mathbb{F}$. Uma vez que $\sqrt{k}$ e $-\sqrt{k}$ não pertencem a $\mathbb{F}$, o polinómio $x^2 - k$ é irredutível. Assim $\sqrt{k}$ é raiz de um polinómio irredutível de grau 2 sobre $\mathbb{F}$. Pela Proposição 1.2.16, $[\mathbb{E} : \mathbb{F}] = 2$. □

Lema 3.2.4 *Dado α, se existe uma sequência finita de corpos $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset ... \subset \mathbb{F}_N$, tal que $\alpha \in \mathbb{F}_N$, e tal que para todo o j, $0 \leq j \leq N-1$, $\mathbb{F}_{j+1}$ é uma extensão quadrática de $\mathbb{F}_j$, então α é construtível.*

Demonstração A demonstração faz-se por indução em N.

Se $N = 0$, $\mathbb{F}_0 = \mathbb{Q}$, α é racional e portanto construtível.

Suponhamos que a afirmação se verifica para um dado n. Queremos ver que então também se verifica para $n+1$. Se $\alpha \in \mathbb{F}_{n+1}$, como $\mathbb{F}_{n+1}$ é uma extensão quadrática de $\mathbb{F}_n$, α pode ser escrito na forma $a_n + b_n\sqrt{k_n}$, com $a_n, b_n, k_n \in \mathbb{F}_n$. Por hipótese de indução, a_n, b_n, k_n são construtíveis. Pelos Lemas 3.1.1 e 3.1.4, conclui-se que $\alpha = a_n + b_n\sqrt{k_n}$ é construtível como se desejava demonstrar. □

O resultado seguinte caracteriza os números construtíveis como sendo aqueles para os quais existe uma sequência finita de extensões quadráticas de $\mathbb{Q}$ (podemos chamar extensão multi-quadrática a uma extensão deste tipo).

Teorema 3.2.5 *Um número α é construtível se e só se existe uma sequência de corpos $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset ... \subset \mathbb{F}_N$, com $\alpha \in \mathbb{F}_N$, tal que para todo o j, $0 \leq j \leq N-1$, $\mathbb{F}_{j+1}$ é uma extensão quadrática de $\mathbb{F}_j$.*

Demonstração Consideremos os pontos $(0,0)$ e $(1,0)$ no plano cartesiano e α um número construtível. Por definição, pode ser construído um segmento de comprimento $|\alpha|$. É claro que podemos usar este segmento, o ponto $(0,0)$ e a recta que passa pelos pontos $(0,0)$ e $(1,0)$ para construir o ponto $P = (\alpha, 0)$. É portanto suficiente mostrar que o ponto P pertence ao plano de um corpo $\mathbb{F}_N$ que verifica as condições do enunciado, isto é, um corpo obtido a partir de $\mathbb{Q}$ através de uma sequência finita de extensões quadráticas.

A construção do ponto P envolve um número finito de passos de construções fundamentais, cada um dando origem a um número finito de pontos novos resultantes de intersecções. Listemos todos estes pontos segundo a ordem da sua construção. Se no i-ésimo passo da construção resultarem, pela primeira vez, mais do que um ponto, suponhamos m pontos, estes são listados na i-ésima, $i+1$-ésima, etc. posição por qualquer ordem. No $i+1$-ésimo passo da construção os pontos são listados começando agora na posição $i+m$.

Suponhamos que o ponto P se encontra na t-ésima posição. Temos então

$$P_1, P_2, ..., P_{t-1}, P_t = P.$$

Verificamos agora que existe um corpo $\mathbb{F}$, que se pode obter a partir de $\mathbb{Q}$ através de uma sequência de extensões quadráticas, tal que $P_1, P_2, ..., P_{t-1}, P_t$ pertencem ao plano de $\mathbb{F}$. Como P_1 e P_2 são os dois pontos de partida, $(0,0)$ e $(1,0)$, estes pertencem desde logo ao plano de $\mathbb{Q}$, estando a afirmação provada para $t = 1$ e $t = 2$. Suponhamos que um dado P_{t-1} construtível pertence a uma extensão quadrática. Para mostrar que a afirmação é válida

para qualquer t, recordemos que a construção de P_t apenas envolve figuras construídas usando os pontos $P_1, P_2, ..., P_{t-1}$, e portanto, por hipótese de indução, figuras que pertencem ao plano de algum corpo $\widetilde{\mathbb{F}}$ que pode ser obtido de $\mathbb{Q}$ através de uma sequência de extensões quadráticas. No entanto, pelo Lema 3.2.2, P_t pertence ao plano do corpo $\widetilde{\mathbb{F}}$ ou $\widetilde{\mathbb{F}}(\sqrt{k})$, para algum $k \in \widetilde{\mathbb{F}}$ e $\sqrt{k} \notin \widetilde{\mathbb{F}}$. Em cada um dos casos, P_t, assim como os outros P_i's, pertencem ao plano de um corpo do tipo pretendido.

Com o Lema 3.2.4 conclui-se o resultado. □

A partir da existência de extensões quadráticas de um dado número real construtível, demonstra-se que o grau desse número sobre $\mathbb{Q}$ será uma potência de 2.

Teorema 3.2.6 *Seja α um real construtível. Então $\deg_{\mathbb{Q}} \alpha$ é uma potência de 2.*

Demonstração Seja α um número construtível. Então, existe uma sequência de corpos

$$\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_N$$

tais que $\alpha \in \mathbb{F}_N$ e para cada j, $\mathbb{F}_{j+1}$ é uma extensão quadrática de $\mathbb{F}_j$. Deste modo, para cada j, $[\mathbb{F}_{j+1} : \mathbb{F}_j] = 2$. Aplicando sucessivamente o Teorema 1.2.4,

$$[\mathbb{F}_N : \mathbb{Q}] = 2^N.$$

Como $\alpha \in \mathbb{F}_N$, $\mathbb{Q}(\alpha) \subset \mathbb{F}_N$. Deste modo,

$$\begin{aligned} [\mathbb{F}_N : \mathbb{Q}] &= [\mathbb{F}_N : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] \\ 2^N &= [\mathbb{F}_N : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}]\,. \end{aligned}$$

Assim, nenhum dos factores do membro direito pode ter factores ímpares. Portanto, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é uma potência de 2, que pela Proposição 1.2.16 iguala a $\deg_{\mathbb{Q}} \alpha$. □

Usando o Teorema 2.3.5 podemos demonstrar que existe um número α cujo grau sobre $\mathbb{Q}$ é uma potência de 2 mas que não é construtível. Demonstra-se assim que o resultado obtido em 3.2.6 não é suficiente.

Proposição 3.2.7 *Para todo $m \geq 2$, existe um número α, tal que*

$$\deg_{\mathbb{Q}} \alpha = 2^m,$$

e tal que α não é construtível.

Demonstração Seja $n = 2^m$, para algum $m \in \mathbb{N} \setminus \{1\}$. Pelo Teorema 2.3.5, podemos considerar $f(x)$ um polinómio sobre $\mathbb{Q}$ cujo grupo de Galois é isomorfo a S_n. Pela Proposição 2.1.2, $f(x)$ é irredutível. Assim, pelo Teorema 1.2.24, $f(x)$ não tem raízes múltiplas de onde, cada uma das suas raízes tem grau $n = 2^m$ sobre $\mathbb{Q}$.

Suponhamos que todas estas raízes eram construtíveis. Então, todo o elemento do corpo de decomposição $\mathbb{E}$ de $f(x)$ seria construtível, uma vez que todos os elementos de $\mathbb{E}$ poderiam ser definidos através de combinações racionais das raízes de $f(x)$. O grau de $[\mathbb{E} : \mathbb{Q}]$ é $n!$, uma vez que é igual à ordem do grupo de Galois. Se escrevermos $\mathbb{E}$ como uma extensão simples de $\mathbb{Q}$, $\mathbb{E} = \mathbb{Q}(\alpha)$, então $\deg_{\mathbb{Q}} \alpha = n!$. Mas $m \geq 2$ pelo que $n \geq 4$. Assim, $n!$ contém o factor ímpar 3, ou seja, $n!$ não é uma potência de 2. Pelo Teorema 3.2.6, α não é construtível.

Portanto, pelo menos uma das raízes de f não é construtível. Seja α essa raiz. □

Capítulo 4

Polinómios com raízes não exprimíveis por radicais

As raízes de um polinómio $f(x) = ax^2 + bx + c$ de segundo grau com coeficientes reais são dadas pela fórmula $\left(-b \pm \sqrt{b^2 - 4ac}\right)/2a$. A mesma fórmula é válida para um polinómio $f(x) \in \mathbb{F}[x]$ onde $\mathbb{F}$ é um corpo de característica diferente de 2.

Sobre $\mathbb{Q}$, o polinómio $x^2 + 2x - 2 \in \mathbb{Q}[x]$ tem como raízes ou zeros $\frac{-2\pm\sqrt{4+4\cdot 2}}{2} \in \mathbb{Q}\left(\sqrt{2}\right)$. A questão que se pode pôr é se fórmulas análogas podem ser encontradas para polinómios de grau maior que 2 com coeficientes em $\mathbb{Q}$, isto é, fórmulas que envolvam uma sequência de operações racionais e extracções de raízes. A resposta é afirmativa para polinómios de terceiro e quarto grau com coeficientes em $\mathbb{Q}$. Já para polinómios de grau 5 tal nem sempre é possível. Mostrar-se-á que para cada $n \geq 5$, existem polinómios de grau n tais que nenhuma das suas raízes pode ser calculada da forma desejada.

4.1 Extensões por radicais

Começamos por formalizar a ideia de um elemento se conseguir obter de elementos de um dado corpo usando sequências finitas de somas, diferenças, produtos, quocientes e extracções de raízes.

Definição 4.1.1 *Um corpo $\mathbb{E}$ é uma **extensão por radicais** de um corpo $\mathbb{F}$ se existem elementos $\alpha_1, ..., \alpha_n \in \mathbb{E}$ e inteiros positivos $n_1, ..., n_j$ tais que:*

1. $\mathbb{E} = \mathbb{F}(\alpha_1, ..., \alpha_n)$

2. $\alpha_1^{n_1} \in \mathbb{F}$

3. $\alpha_i^{n_i} \in \mathbb{F}(\alpha_1, ..., \alpha_{i-1})$ *para* $1 < i < n$.

Um polinómio $f(x) \in \mathbb{F}[x]$ *diz-se* ***resolúvel por radicais*** *sobre* $\mathbb{F}$ *se o seu corpo de decomposição sobre* $\mathbb{F}$ *está contido numa extensão por radicais de* $\mathbb{F}$.

De acordo com a definição anterior um polinómio $f(x) \in \mathbb{F}[x]$ é resolúvel por radicais sobre $\mathbb{F}$ se conseguirmos obter todos os zeros de $f(x)$ usando uma sequência finita de somas, diferenças, produtos, quocientes e n-ésimas raízes começando o processo com elementos de $\mathbb{F}$.

Definição 4.1.2 *Um elemento* β *diz-se* ***exprimível por radicais*** *sobre* $\mathbb{F}$ *quando existem* $\alpha_1, ..., \alpha_m$ *tais que* $\mathbb{F}(\alpha_1, ..., \alpha_m, \beta)$ *é uma extensão radical de* $\mathbb{F}$.

Mostramos agora que relações existem entre um polinómio ser resolúvel por radicais e o grupo de Galois desse polinómio; demonstrar-se-á no fim desta secção que

Teorema 4.1.3 *Um polinómio é resolúvel por radicais se e só se o seu grupo de Galois for solúvel.*

Relembramos que um grupo G se diz solúvel se existir uma sequência de subgrupos $G = H_0 \supseteq H_1 \supseteq ... \supseteq H_N = \{id\}$ tal que cada H_{i+1} é um subgrupo normal de H_i, para cada $0 \leq i \leq N-1$ e $|H_i| / |H_{i+1}|$ é primo. A uma sequência como a indicada antes dá-se o nome de **série de decomposição** de G com factores primos.

Caso nada em contrário seja dito, nesta secção consideramos o polinómio $f(x)$, $\mathbb{F}$ o menor corpo que contém os coeficientes de $f(x)$ e $\mathbb{E}$ o seu corpo de decomposição.

Relembramos agora um resultado importante da teoria de grupos; demonstra-se que S_n, para $n \geq 5$, não é solúvel. Necessitamos porém do seguinte lema:

Lema 4.1.4 *Se* N *é um subgrupo normal de um grupo* H *com índice primo* p, *então para quaisquer elementos* $\phi, \psi \in H, \phi^{-1}\psi^{-1}\phi\psi \in N$.

Demonstração Sejam N, H, ϕ, ψ nas condições do enunciado do Lema.

Se $\phi \in N$, como $N \trianglelefteq H$, $\psi^{-1}\phi\psi \in N$. Como $\phi \in N$ e N é subgrupo de H, é fechado para o produto, logo $\phi^{-1}\psi^{-1}\phi\psi \in N$.

Se $\phi \notin N$, considere-se $\widetilde{N} = \left\{\phi^k n : n \in N, k \in \mathbb{Z}\right\}$. Facilmente se verifica que $\widetilde{N}$ é um subgrupo normal de H. Pelo Teorema de Lagrange, como $N \leq \widetilde{N}$, $|N|$ é divisor de $\left|\widetilde{N}\right|$, isto é,

$$\left|\widetilde{N}\right| = q\,|N|$$

para algum q. Mas $\left|\widetilde{N}\right| \mid |H|$ e $|H| = p\,|N|$. Logo $p\,|N| = aq\,|N|$, para algum a. Como p é primo, conclui-se que $q = 1$ ou $q = p$. Como $\phi \notin N$, $N \neq \widetilde{N}$ já que $\phi \in \widetilde{N}$. Logo $q \neq 1$. Portanto $q = p$ e $\widetilde{N} = H$. Podemos assim escrever $\psi \in H$ na forma

$$\psi = \phi^k n$$

para alguns $k \in \mathbb{Z}$ e $n \in N$. Mas então

$$\phi^{-1}\psi^{-1}\phi\psi = \phi^{-1}n^{-1}\phi^{-k}\phi\phi^k n = \phi^{-1}n^{-1}\phi n$$

e uma vez que $N \trianglelefteq H$, $\phi^{-1}n^{-1}\phi \in N$. Como $n \in N$, deduz-se que

$$\phi^{-1}n^{-1}\phi n \in N,$$

logo $\phi^{-1}\psi^{-1}\phi\psi \in N$. □

Proposição 4.1.5 *Se $n \geq 5$, então S_n não é solúvel.*

Demonstração Suponhamos, com vista a um absurdo, que S_n é solúvel. Assim, existe uma cadeia de subgrupos

$$S_n = G = H_0 \supset H_1 \supset \ldots \supset H_N = \{id\}$$

tal que para cada $j \in \{0, \ldots, N-1\}$, H_{j+1} é um subgrupo normal de índice primo de H_j. Mostrar-se-á, por indução em N, que para todo o j, H_j contém todos os ciclos de comprimento 3. Isto contraria o facto de $H_N = \{id\}$. Se $N = 0$, então $G = H_0 = S_n$ e H_0 contém, em particular, todos os ciclos de comprimento 3. Suponhamos agora que H_j contém todos os ciclos de comprimento 3. Mostraremos que H_{j+1} também os contém. Seja (ijk) um

ciclo de comprimento 3 arbitrário. Uma vez que $n \geq 5$, podemos escolher $i, j, k, l, m \in \mathbb{N}$ todos distintos. Sejam $\phi = (mji)$ e $\psi = (ilk)$. Pela hipótese de indução sabemos que $\phi, \psi \in H_j$. Assim, pelo Lema anterior,

$$\phi^{-1}\psi^{-1}\phi\psi \in H_{j+1}.$$

Mas $\phi^{-1}\psi^{-1}\phi\psi = (ijm)(kli)(mji)(ilk) = (ijk)$. Portanto, $(ijk) \in H_{j+1}$. Como este ciclo era arbitrário, concluímos o pretendido. □

Atendendo à definição de polinómio resolúvel tem-se o seguinte:

Corolário 4.1.6 *Todo o polinómio cujo grupo de Galois é isomorfo a S_n, para algum $n \geq 5$, não é resolúvel por radicais.*

Apresentamos agora vários lemas que nos irão permitir demonstrar o resultado desejado.

Lema 4.1.7 *Seja $\mathbb{F}$ um corpo de característica zero e $f(x) \in \mathbb{F}[x]$ irredutível tal que o seu grupo de Galois é solúvel. Então existe uma sequência de corpos $\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset ... \subset \mathbb{F}_N = \mathbb{E}$ tal que, para cada j, $0 \leq j \leq N-1$, $\mathbb{F}_{j+1}$ é extensão normal de $\mathbb{F}_j$ de grau primo.*

Demonstração Por hipótese, existe uma sequência de subgrupos

$$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_N = \{id\}$$

tais que cada H_{j+1} é um subgrupo normal de H_j de índice primo.

Tomem-se os corpos fixos de $\mathbb{E}$ por cada um dos H_j,

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset ... \subset \mathbb{F}_N = \mathbb{E}$$

onde $\mathbb{F}_j = \mathbb{E}^{H_j}$. Como $\mathbb{E}$ é corpo de decomposição de $f(x)$, $\mathbb{E}$ é extensão normal de $\mathbb{F}$ logo, pela Proposição 1.2.34, é também uma extensão normal de cada um dos corpos $\mathbb{F}_j$. Assim, $H_j = G(\mathbb{E} : \mathbb{F}_j)$ (já que $\mathbb{E}$ é uma extensão normal e separável de $\mathbb{F}_j$). Como H_{j+1} é um subgrupo normal de H_j, pelo Teorema 1.3.9 (Teorema da Correspondência de Galois) $\mathbb{F}_{j+1}$ é uma extensão normal de $\mathbb{F}_j$ cujo grau é

$$\begin{aligned} |\mathbb{F}_{j+1} : \mathbb{F}_j| &= [\mathbb{E} : \mathbb{F}_j] \,/\, [\mathbb{E} : \mathbb{F}_{j+1}] \\ &= |G(\mathbb{E} : \mathbb{F}_j)| \,/\, |G(\mathbb{E} : \mathbb{F}_{j+1})| \\ &= |H_j| \,/\, |H_{j+1}| \\ &= |H_j : H_{j+1}| \\ &= p, \text{ primo,} \end{aligned}$$

como se desejava demonstrar. □

Mostrar-se-á que todo o elemento de uma extensão normal de grau primo de um corpo $\mathbb{K}$, pode ser obtido a partir de $\mathbb{K}$ usando apenas operações racionais e extracções de p-ésimas raízes.

Lema 4.1.8 *Seja $\mathbb{L}$ uma extensão normal de grau primo p sobre um corpo $\mathbb{K}$ de característica zero que contém as p-ésimas raízes da unidade. Então existe uma família de $p-1$ elementos $a_1, ..., a_{p-1}$ tais que para cada i, $a_i^p \in \mathbb{K}$ e $\mathbb{L} \subset \mathbb{K}(a_1, ..., a_{p-1})$.*

Demonstração Considere-se $G(\mathbb{L} : \mathbb{K})$. Como $\mathbb{L}$ é normal sobre $\mathbb{K}$ e $\mathbb{L}$ é separável sobre $\mathbb{K}$, $|G(\mathbb{L} : \mathbb{K})| = p$, logo como p é primo, $G(\mathbb{L} : \mathbb{K})$ é cíclico. Seja ϕ um seu gerador. Pelo Teorema 1.2.26, podemos tomar $r \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(r)$. Como $\mathbb{L}$ é normal, todos os conjugados de r estão em $\mathbb{L}$. Sabemos também que os automorfismos ϕ de $G = G(\mathbb{L} : \mathbb{K})$ transformam r nos seus conjugados. Seja $r_i = \phi^i(r)$ para cada $1 \leq i \leq p$. Se $i, j \in \{1, ..., p\}$, com $i \neq j$, então $\phi^i \neq \phi^j$, pelo que $r_i \neq r_j$.

Como $[\mathbb{L} : \mathbb{K}] = p$, r tem exactamente p conjugados. Seja g o polinómio mínimo de r sobre $\mathbb{K}$, $r_1, ..., r_p$ as suas raízes e w uma p-ésima raiz primitiva da unidade. Consideremos, para $0 \leq j \leq p-1$,

$$a_j = r_1 + w^j r_2 + w^{2j} r_3 + ... + w^{(p-1)j} r_p,$$

isto é,

$$\begin{aligned}
a_0 &= r_1 + r_2 + r_3 + ... + r_p, \\
a_1 &= r_1 + w r_2 + w^2 r_3 + ... + w^{(p-1)} r_p, \\
a_2 &= r_1 + w^2 r_2 + w^4 r_3 + ... + w^{2(p-1)} r_p, \\
&\vdots \\
a_{p-1} &= r_1 + w^{p-1} r_2 + w^{2(p-1)} r_3 + ... + w^{(p-1)^2} r_p.
\end{aligned}$$

Podemos considerar estas equações como um sistema linear de p equações em p incógnitas $r_1, ..., r_p$. Note-se que $a_0 \in \mathbb{K}$ uma vez que podemos pensar em a_0 como um polinómio simétrico elementar nas incógnitas $r_1, ..., r_p$, que são as raízes de g sobre $\mathbb{K}$. Verificamos agora que, para $0 \leq j \leq p-1$, os $(a_j)^p$ são invariantes por $G(\mathbb{L} : \mathbb{K})$ e que $(a_j)^p \in \mathbb{K}$. Tem-se que, para cada

$0 \leq j \leq p-1$ e para cada $\phi \in G(\mathbb{L}:\mathbb{K})$,

$$\begin{aligned}
\phi\left[(a_j)^p\right] &= \left[\phi(a_j)\right]^p \\
&= \left[\phi(r_1) + w^j\phi(r_2) + w^{2j}\phi(r_3) + ... + w^{(p-1)j}\phi(r_p)\right]^p \\
&= \left[r_2 + w^j r_3 + w^{2j} r_4 + ... + w^{(p-1)j} r_1\right]^p \\
&= \left[w^{-j} a_j\right]^p \\
&= (a_j)^p,
\end{aligned}$$

portanto $(a_j)^p \in \mathbb{K}$.

Calculemos agora o determinante da matriz dos coeficientes do sistema de equações acima:

$$\begin{vmatrix}
1 & 1 & 1^2 & 1^3 & \cdots & 1^{p-1} \\
1 & w & w^2 & w^3 & \cdots & w^{p-1} \\
1 & w^2 & (w^2)^2 & (w^2)^3 & \cdots & (w^2)^{p-1} \\
\vdots & & & & & \\
1 & w^{p-1} & (w^{p-1})^2 & (w^{p-1})^3 & \cdots & (w^{p-1})^{p-1}
\end{vmatrix}$$

O que se obtém é o determinante de Vandermonde o qual é

$$\prod_{0 \leq i < j \leq p-1} \left(w^j - w^i\right).$$

Este determinante é não nulo uma vez que $w^j \neq w^i$, quando $0 \leq i < j \leq p-1$. Assim, como a matriz é não singular, pela regra de Cramer, os r_i's podem ser obtidos a partir dos a_j's e de w através de operações racionais. Deste modo, para cada i, $r_i \in \mathbb{K}(a_1, ..., a_{p-1})$, de onde $\mathbb{L} = \mathbb{K}(r) \subset \mathbb{K}(a_1, ..., a_{p-1})$. □

Lema 4.1.9 *Seja $\mathbb{K}$ um corpo de característica zero. Se $\mathbb{L}$ é uma extensão normal e radical de $\mathbb{K}$ então $G(\mathbb{L}:\mathbb{K})$ é um grupo solúvel.*

Demonstração Seja $\mathbb{L} = \mathbb{K}(\alpha_1, ..., \alpha_n)$, com $\alpha_1^{n_1} \in \mathbb{K}$ e $\alpha_i^{n_i} \in \mathbb{K}(\alpha_1, ..., \alpha_{i-1})$, para alguns $n_1, ..., n_n \in \mathbb{N}$. É fácil demonstrar que podemos, sem perda de generalidade, supor que todos os expoentes n_i são primos.

Seja p um primo tal que $\alpha_1^p \in \mathbb{K}$. A demonstração efectua-se agora por indução em n. Se $n = 0$, $\mathbb{L} = \mathbb{K}$ e $G(\mathbb{L}:\mathbb{K}) = \{id\}$, logo solúvel.

Suponhamos agora o resultado para extensões radicais da forma $\mathbb{K}(\beta_1, ..., \beta_j)$ tal que $\beta_i^{n_i} \in \mathbb{K}(\beta_1, ..., \beta_{i-1})$ e $j < n$. Se $\alpha_1 \in \mathbb{K}$ então $\mathbb{L} = \mathbb{K}(\alpha_2, ..., \alpha_n)$ e o

resultado é válido por hipótese de indução. Supomos agora que $\alpha_1 \notin \mathbb{K}$. Seja $f(x)$ o polinómio mínimo de α_1 sobre $\mathbb{K}$. Assim $\deg f(x) \geq 2$ e como $\mathbb{L}$ é uma extensão normal de $\mathbb{K}$, $f(x)$ decompõe-se em factores lineares em $\mathbb{L}[x]$. Como $\mathbb{K}$ é um corpo de característica zero, pelo Teorema 1.2.24, todas as raízes de $f(x)$ são distintas. Seja $\beta \neq \alpha_1$ uma raiz de $f(x)$. Como $\alpha_1^p \in \mathbb{K}$ (onde $p = n_1$, primo), α_1 é raiz de $x^p - a$, para algum $a \in \mathbb{K}$. Consequentemente, $f(x)$ divide $x^p - a$. Como β é um zero de $f(x)$,

$$\beta^p - a = 0.$$

Logo

$$\left(\frac{\alpha_1}{\beta}\right)^p = 1.$$

Como p é primo e $\beta \neq \alpha_1$, $\frac{\alpha_1}{\beta}$ tem ordem prima p no grupo $(\mathbb{L} - \{0\}, \cdot)$ e $1, \frac{\alpha_1}{\beta}, \left(\frac{\alpha_1}{\beta}\right)^2, ..., \left(\frac{\alpha_1}{\beta}\right)^{p-1}$ são as p raízes distintas do polinómio $g(x) = x^p - 1$ em $\mathbb{L}$. O corpo $\mathbb{M} = \mathbb{K}(\frac{\alpha_1}{\beta}) \subseteq \mathbb{L}$ é um corpo de decomposição de $g(x)$ sobre $\mathbb{K}$. Obtemos assim a seguinte cadeia

$$\mathbb{K} \subseteq \mathbb{M} = \mathbb{K}(\frac{\alpha_1}{\beta}) \subseteq \mathbb{M}(\alpha_1) \subseteq \mathbb{L}.$$

Uma vez que as raízes de $x^p - \alpha_1^p$ são da forma $\varepsilon\alpha_1$, onde $\varepsilon \in \mathbb{M}$ é raiz de $x^p - 1$ (ver, por exemplo, [4, Proposição 7.6.10]), tem-se que $\mathbb{M}(\alpha_1)$ é corpo de decomposição de $x^p - \alpha_1^p$ sobre $\mathbb{M}$. Mais, cada $\mathbb{M}$-automorfismo de $\mathbb{M}(\alpha_1)$ é determinado pela imagem do elemento α_1; para cada $\varphi \in G(\mathbb{M}(\alpha_1) : \mathbb{M})$

$$\varphi_i(\alpha_1) = \varepsilon_i\alpha_1,$$

onde ε_i é raiz de $x^p - 1$. Assim, $G(\mathbb{M}(\alpha_1) : \mathbb{M})$ é abeliano. Uma vez que $\mathbb{M}$ é corpo de decomposição de $x^p - 1$, existem p raízes distintas e o conjunto das raízes do polinómio constitui um grupo cíclico para o produto. Sendo α um gerador do grupo das raízes, qualquer $\mathbb{K}$-automorfismo fica determinado pela sua imagem, a qual será α^j para $j \in \{0, ..., p-1\}$. Assim $G(\mathbb{M} : \mathbb{K})$ é cíclico.

Temos que $\mathbb{L} = \mathbb{K}(\alpha_1, ..., \alpha_n) = \mathbb{M}(\alpha_1, ..., \alpha_n) = \mathbb{M}(\alpha_1)(\alpha_2, ..., \alpha_n)$ é extensão normal e radical de $\mathbb{M}(\alpha_1)$, logo por hipótese de indução, $G(\mathbb{L} : \mathbb{M}(\alpha_1))$ é solúvel.

Como $\mathbb{L}$ é uma extensão finita, normal e separável de $\mathbb{K}$, o mesmo acontece a $\mathbb{M}$, pela Proposição 1.2.34. Pelo Teorema 1.3.9 tem-se que

$$G(\mathbb{M}(\alpha_1) : \mathbb{M}) \cong \frac{G(\mathbb{L} : \mathbb{M})}{G(\mathbb{L} : \mathbb{M}(\alpha_1))}.$$

Como $G(\mathbb{M}(\alpha_1) : \mathbb{M})$ é abeliano e $G(\mathbb{L} : \mathbb{M}(\alpha_1))$ é solúvel, $G(\mathbb{L} : \mathbb{M})$ é solúvel [11, Teorema 4.11.14]. Aplicando agora o Teorema 1.3.9 à sequência de extensões

$$\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$$

tem-se

$$G(\mathbb{M} : \mathbb{K}) \cong \frac{G(\mathbb{L} : \mathbb{K})}{G(\mathbb{L} : \mathbb{M})}.$$

Como $G(\mathbb{M} : \mathbb{K})$ é abeliano e $G(\mathbb{L} : \mathbb{M})$ é solúvel, deduz-se que $G(\mathbb{L} : \mathbb{K})$ é solúvel como se pretendia, [11, Teorema 4.11.14]. □

Introduzimos agora uma nova definição necessária para o desenrolar do trabalho

Definição 4.1.10 *Seja $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$. Dizemos que uma extensão $\mathbb{N}$ de $\mathbb{L}$ é um **fecho normal** de $\mathbb{L}$ se:*

1. *$\mathbb{N}$ é uma extensão normal de $\mathbb{K}$;*
2. *Se $\mathbb{M}$ é um corpo tal que $\mathbb{L} \subset \mathbb{M} \subset \mathbb{N}$ e $\mathbb{M}$ é extensão normal de $\mathbb{K}$, então $\mathbb{M} = \mathbb{N}$.*

Estão agora reunidos os requisitos necessários para demonstrar o Teorema pretendido

Demonstração do Teorema 4.1.3 Seja $f(x)$ um polinómio sobre um corpo $\mathbb{F}$ de característica zero, $\mathbb{E}$ o seu corpo de decomposição e suponhamos que $G(\mathbb{E} : \mathbb{F})$ é solúvel. Pelo Lema 4.1.7 existe uma sequência de corpos tais que

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset ... \subset \mathbb{F}_N = \mathbb{E},$$

$|\mathbb{F}_{j+1} : \mathbb{F}_j| = p_j$ e $\mathbb{F}_{j+1}$ é extensão normal de $\mathbb{F}_j$. Para cada $j \in \{0, ..., N-1\}$ seja w_j uma p_j-ésima raiz primitiva da unidade e considere-se $\mathbb{F}_j(w_j)$ e $\mathbb{F}_{j+1}(w_j)$. Sabemos que $|\mathbb{F}_j(w_j) : \mathbb{F}_j| = \deg_{\mathbb{F}_j}(w_j) \leq p_j - 1$ e

$$\begin{aligned} |\mathbb{F}_{j+1}(w_j) : \mathbb{F}_{j+1}|\,|\mathbb{F}_{j+1} : \mathbb{F}_j| &= |\mathbb{F}_{j+1}(w_j) : \mathbb{F}_j| \\ &= |\mathbb{F}_{j+1}(w_j) : \mathbb{F}_j(w_j)|\,|\mathbb{F}_j(w_j) : \mathbb{F}_j|\,. \end{aligned}$$

Como $p = |\mathbb{F}_{j+1} : \mathbb{F}_j|$ e $|\mathbb{F}_j(w_j) : \mathbb{F}_j| \leq p_j - 1$, das igualdades anteriores conclui-se que $p \mid |\mathbb{F}_{j+1}(w_j) : \mathbb{F}_j(w_j)|$. Portanto, $|\mathbb{F}_{j+1}(w_j) : \mathbb{F}_j(w_j)| \geq p$. Mas,

$$|\mathbb{F}_{j+1}(w_j) : \mathbb{F}_{j+1}| = \deg_{\mathbb{F}_{j+1}} w_j \leq \deg_{\mathbb{F}_j} w_j = |\mathbb{F}_j(w_j) : \mathbb{F}_j|\,.$$

Logo, $|\mathbb{F}_{j+1}(w_j) : \mathbb{F}_j(w_j)| \leq p$, de onde $|\mathbb{F}_{j+1}(w_j) : \mathbb{F}_j(w_j)| = p$.

Como $\mathbb{F}_{j+1} = \mathbb{F}_j(a_j)$ para algum a_j, seja g_j o polinómio mínimo de a_j sobre $\mathbb{F}_j$. Então $\mathbb{F}_{j+1}(w_j)$ é o corpo de decomposição de $g_j(x)(x^{p_j} - 1)$ sobre $\mathbb{F}_j$ (note-se que $\mathbb{F}_{j+1}$ é extensão normal de $\mathbb{F}_j$). Logo $\mathbb{F}_j(w_j) \subset \mathbb{F}_{j+1}(w_j)$ é uma extensão normal de grau p. Pelo Lema 4.1.8, $\mathbb{F}_{j+1} \subseteq \mathbb{F}_j(w_j, a_{j1}, ..., a_{jp_j-1})$ tal que para cada i, $a_j^{p_j} \in \mathbb{F}_j$. Considere-se

$$\mathbb{E}' = \mathbb{F}(w_0, a_{0,1}, ..., a_{0,p_0-1}, ..., w_{N-1}, a_{N-1,1}, ..., a_{N-1,p_{N-1}-1})$$

extensão por radicais de $\mathbb{F}$. Como $\mathbb{E} = \mathbb{F}_N = \mathbb{F}_{N-1}(w_{N-1}, a_{N-1,1}, ..., a_{N-1,p_{N-1}-1})$, demonstra-se, atendendo à construção dos a_{ji}, que $\mathbb{E} \subseteq \mathbb{E}'$. Mas então, $f(x)$ é resolúvel por radicais.

Reciprocamente, suponhamos que $f(x)$ é resolúvel por radicais. Por definição, o corpo de decomposição de $f(x)$ sobre $\mathbb{F}$ está contido numa extensão de $\mathbb{F}$ por radicais, $\mathbb{E}$. Seja $\mathbb{M}$ uma extensão radical de $\mathbb{F}$, com $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{M}$, $G = G(\mathbb{E} : \mathbb{F})$, $\mathbb{K} = \mathbb{E}^G$ e $\mathbb{N}$ um fecho normal da extensão $\mathbb{K}$. Assim,

$$\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{M} \subseteq \mathbb{N}.$$

Como $\mathbb{M}$ é uma extensão radical de $\mathbb{K}$, por definição, $\mathbb{M} = \mathbb{K}(\alpha_1, ..., \alpha_r)$, com $\alpha_1^{n_1} \in \mathbb{K}$ e $\alpha_i^{n_i} \in \mathbb{K}(\alpha_1, ..., \alpha_{i-1})$. Seja $f_i(x)$ o polinómio mínimo de α_i sobre $\mathbb{K}$ para cada $i \in \{1, ..., r\}$. É fácil verificar que sendo $\mathbb{N}$ o fecho normal de $\mathbb{M}$ sobre $\mathbb{F}$, $\mathbb{N}$ é o corpo de decomposição do polinómio $f_1(x) \cdot ... \cdot f_n(x)$. Sejam β_{ij} os zeros de $f_i(x)$, para cada $i \in \{1, ..., r\}$. Para cada β_{ij} podemos estabelecer um isomorfismo

$$\sigma_{ij} : \mathbb{K}(\alpha_i) \longrightarrow \mathbb{K}(\beta_{ij}).$$

o qual se estende a um $\mathbb{K}$-automorfismo de $\mathbb{N}$. Como cada α_i é exprimível por radicais sobre $\mathbb{K}$, β_{ij} também o é. Logo, $\mathbb{N}$ é uma extensão radical de $\mathbb{K}$. Pelo Lema 4.1.9, $G(\mathbb{N} : \mathbb{K})$ é solúvel.

Como $\mathbb{E}$ é uma extensão normal de $\mathbb{K}$ ($\mathbb{E}$ é corpo de decomposição de um polinómio sobre $\mathbb{K}$), pelo Teorema 1.3.9,

$$G(\mathbb{E} : \mathbb{K}) \cong \frac{G(\mathbb{N} : \mathbb{K})}{G(\mathbb{N} : \mathbb{E})}.$$

Assim, $G(\mathbb{E} : \mathbb{K})$ é solúvel. Por [11, Teorema 4.11.14], uma vez que $G(\mathbb{E} : \mathbb{F}) = G(\mathbb{E} : \mathbb{K})$, tem-se o pretendido. □

4.2 Polinómios sem zeros exprimíveis por radicais

Pretendemos agora construir polinómios cujos zeros não sejam exprimíveis por radicais. Começamos por verificar que todos os zeros de polinómios de terceiro e quarto graus podem ser expressos por radicais.

Considere-se a equação

$$ax^3 + bx^2 + cx + d = 0$$

onde $a, b, c, d \in \mathbb{F}$ corpo de característica zero. Vemos agora que todas as equações do terceiro grau são resolúveis por radicais. Sem perda de generalidade podemos supor que $a = 1$. Assim,

$$x^3 + bx^2 + cx + d = 0.$$

Aplicando a seguinte mudança de variável

$$x = y + L$$

para algum $L \in \mathbb{F}$, obtém-se a equação

$$y^3 + (3L + b)\, y^2 + \left(3L^2 + 2bL + c\right) y + L^3 + bL^2 + cL + d = 0.$$

Fazendo $L = -b/3$, obtém-se uma equação do tipo

$$y^3 + By + C = 0,$$

para alguns $B, C \in \mathbb{F}$.

Se $C = 0$, a resolução é evidente. Se $C \neq 0$, $y = 0$ não é solução da equação. Fazendo a substituição $y = z + K/z$, para algum K, tem-se

$$z^6 + (3K + B)\, z^4 + Cz^3 + (3K + B)\, Kz^2 + K^3 = 0.$$

Neste caso, dois coeficientes anulam-se quando se substitui K por $-B/3$, resultando a equação

$$z^6 + Cz^3 + K^3 = 0.$$

Esta equação pode agora ser resolvida do mesmo modo que uma equação quadrática, considerando

$$\left(z^3\right)^2 + C\left(z^3\right) + K^3 = 0.$$

Demonstra-se assim que

Lema 4.2.1 *Seja $\mathbb{F}$ um corpo de característica zero. Então, todo o polinómio $p(x) = ax^3 + bx^2 + cx + d \in \mathbb{F}[x]$ é resolúvel por radicais.*

Demonstramos que um resultado análogo é válido para equações de grau 4.

Lema 4.2.2 *Seja $\mathbb{F}$ um corpo de característica zero. Então, todo o polinómio $p(x) = ax^4 + bx^3 + cx^2 + dx + e \in \mathbb{F}[x]$ é resolúvel por radicais.*

Demonstração Se $a = 0$ estamos nas condições do Lema 4.2.1.

Se $a \neq 0$, podemos, sem perda de generalidade, supor que $a = 1$. Assim,

$$x^4 + bx^3 + cx^2 + dx + e = 0.$$

Da mudança de variável

$$x = y - \frac{b}{4}$$

resulta uma equação do tipo

$$y^4 + Cy^2 + Dy + E = 0.$$

Somando a ambos os membros da equação anterior o termo $y^2t + \frac{t^2}{4}$, onde t é um elemento do corpo $\mathbb{F}$, obtemos

$$\left(y^2 + \frac{t}{2}\right)^2 - \left[y^2(t - C) - Dy + \frac{t^2}{4} - E\right] = 0.$$

De forma a que

$$y^2(t - C) - Dy + \frac{t^2}{4} - E$$

seja um quadrado perfeito, escolhemos t tal que o binómio discriminante da equação $y^2(t - C) - Dy + \frac{t^2}{4} - E = 0$ seja nulo, isto é,

$$(-D)^2 - 4(t - C)\left(\frac{t^2}{4} - E\right) = 0,$$

obtendo a equação do terceiro grau

$$-t^3 + Ct^2 + 4Et + D^2 - 4CE = 0.$$

Pelo Lema 4.2.1 esta equação é resolúvel por radicais. Seja t_0 uma das suas raízes. Então,

$$y^2 (t_0 - C) - Dy + \frac{t_0^2}{4} - E = (t_0 - C) \left(y - \frac{D}{2(t_0 - C)} \right)^2.$$

Assim,

$$\left(y^2 + \frac{t_0}{2} \right)^2 - (t_0 - C) \left(y - \frac{D}{2 (t_0 - C)} \right)^2 = 0.$$

Usando a diferença do quadrado,

$$\left[y^2 + t_0/2 - \sqrt{t_0 - C} \left(y - \frac{D}{2 (t_0 - C)} \right) \right] \left[y^2 + t_0/2 + \sqrt{t_0 - C} \left(y - \frac{D}{2 (t_0 - C)} \right) \right] = 0.$$

Igualando cada termo a zero obtemos y em função de radicais, e consequentemente x, como era pretendido. □

No lema seguinte demonstramos que se alguma raiz de um dado polinómio irredutível pode ser obtida por radicais, então todas podem.

Lema 4.2.3 *Seja $f(x) \in \mathbb{F}[x]$ irredutível e r uma raiz de $f(x)$ exprimível por radicais. Então $f(x)$ é solúvel por radicais.*

Demonstração Seja $f(x) \in \mathbb{F}[x]$ irredutível e r uma raiz de $f(x)$ exprimível por radicais. Então existem $\alpha_1, ..., \alpha_{m+1}$ tais que

1. $\alpha_1^{n_1} \in \mathbb{F}$,
2. $\alpha_i^{n_i} \in \mathbb{F}(\alpha_1, ..., \alpha_{i-1})$,
3. $r \in \mathbb{F}(\alpha_1, ..., \alpha_{m+1})$,

para alguns $n_1, ..., n_m, m \in \mathbb{Z}$. Seja $\mathbb{F}_i = \mathbb{F}(\alpha_1, ..., \alpha_{i-1})$. Assim, $\mathbb{F}_{j+1} = \mathbb{F}_j(\alpha_j)$ e $r \in \mathbb{F}(\alpha_1, ..., \alpha_m, \alpha_{m+1})$. Tome-se $\alpha_{m+2} = r$.

Seja $b_j = \alpha_j^{n_j} \in \mathbb{F}_{j-1}$ e sejam $b_j = b_{j1}, b_{j2}, ..., b_{jm_j}$ os conjugados de b_j em $\mathbb{F}$ e

$$g_j(x) = (x^{n_j} - b_{j1})(x^{n_j} - b_{j2})...(x^{n_j} - b_{jm_j}).$$

Assim definido, $g(x)$ é um polinómio cujos coeficientes são os polinómios simétricos avaliados em $b_{j1}, b_{j2}, ..., b_{jm_j}$. Assim, para cada j, $g_j(x) \in \mathbb{F}[x]$.

Considere-se

$$h(x) = \prod_{j=1}^{m+1} g_j(x) \in \mathbb{F}[x]$$

e $\mathbb{E}$ o seu corpo de decomposição sobre $\mathbb{F}$. Assim,

$$\mathbb{E} = \mathbb{F}(b_{11}, ..., b_{1m_1}, b_{21}, ..., b_{2m_2}, ..., b_{m+1,1}..., b_{m+1,m_{m+1}})$$

e $\mathbb{E}$ é uma extensão por radicais de $\mathbb{F}$. Como $\mathbb{E}$ é corpo de decomposição de um polinómio, $\mathbb{E}$ é normal. Uma vez que $r \in \mathbb{E}$, todas as raízes de $f(x)$ estão em $\mathbb{E}$. Consequentemente, $f(x)$ é resolúvel por radicais. □

Mostra-se assim que se uma raiz de um polinómio irredutível pode ser exprimível por radicais, todas podem.

Caracterizamos agora o grupo de Galois de um polinómio de grau primo sobre $\mathbb{Q}$ dependendo do número das suas raízes reais.

Lema 4.2.4 *Seja $f(x) \in \mathbb{Q}[x]$ um polinómio irredutível de grau primo p. Se $f(x)$ tem duas e só duas raízes complexas não reais, então o grupo de Galois de $f(x)$ é o grupo simétrico S_p.*

Demonstração Seja $\mathbb{L}$ ($\subseteq \mathbb{C}$) o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$ e G o grupo de Galois de $f(x)$ sobre $\mathbb{Q}$. Uma vez que $\mathbb{Q}$ tem característica zero, $p(x)$ tem exactamente p raízes distintas, logo $|G| \leq p!$.

Note-se que, por construção de corpo de decomposição, p divide $[\mathbb{L} : \mathbb{Q}]$. Pelo Teorema 1.3.9, p divide $|G|$, logo, pelo Teorema de Cauchy, G tem um elemento de ordem p, isto é, um ciclo de comprimento p.

Consideremos o $\mathbb{Q}$-automorfismo de $\mathbb{L}$ induzido pela conjugação dos números complexos. Assim, este mantém invariante os $p-2$ zeros reais de $f(x)$ e que permuta os dois zeros não reais. Então, G contém uma transposição.

Uma vez que G contém um ciclo de comprimento p e uma transposição $G = S_p$. □

Usando o Lema anterior podemos agora construir um polinómio de grau 5 resolúvel por radicais sobre $\mathbb{Q}$.

Consideremos o polinómio

$$p(x) = x^5 - 6x + 3.$$

Pelo critério de Eisenstein, Teorema 1.1.12, $p(x)$ é um polinómio irredutível em $\mathbb{Q}[x]$. Tem-se que

$$\begin{aligned} p(-2) &= -17 \\ p(-1) &= 8 \\ p(1) &= -2 \\ p(2) &= 23 \end{aligned}$$

e uma vez que $p'(x) = 5x^4 - 6$ tem dois zeros reais, resulta que $p(x)$ tem exactamente três raízes reais. Uma vez que $\mathbb{Q}$ tem característica zero, $p(x)$ não pode ter raízes múltiplas. Portanto $p(x)$ tem duas raízes complexas não reais. Pelo Lema 4.2.4, o grupo de Galois de $p(x)$ será S_5, que não é um grupo solúvel. Logo, pelo Teorema 4.1.3, o polinómio $p(x)$ não é resolúvel por radicais sobre $\mathbb{Q}$.

Multiplicando o polinómio $p(x)$ por x^k, obtemos um polinómio de grau $5+k$ o qual não é resolúvel por radicais. Mostra-se assim o Teorema de Abel.

Teorema 4.2.5 (Teorema de Abel) *Para cada $n \geq 5$, existem polinómios de grau n não resolúveis por radicais.*

Isto é, mostra-se a existência de polinómios de grau n, para cada $n \geq 5$, para os quais existe pelo menos uma raiz não exprimível por radicais. Note-se que os polinómios construídos para a demonstração do Teorema de Abel resultam do produto de um polinómio de grau 5 por uma potência adequada de x, logo não são irredutíveis.

Usando o Teorema 2.3.5 demonstra-se, para cada $n \geq 5$, a existência de polinómios sobre $\mathbb{Q}$ de grau n tal que nenhuma das suas raízes é exprimível por radicais.

Teorema 4.2.6 *Para cada $n \geq 5$, existe um polinómio sobre $\mathbb{Q}$ de grau n tal que nenhum dos seus zeros pode ser exprimível por radicais.*

Demonstração Seja $n \geq 5$. Pelo Teorema 2.3.5, existe um polinómio $p(x)$ sobre $\mathbb{Q}$ cujo grupo de Galois é S_n. Pelo Lema 4.1.5, S_n não é solúvel. Assim, pelo Teorema 4.1.3, $p(x)$ não é resolúvel por radicais. Porém, como o grupo de Galois de $p(x)$ é S_n, pela Proposição 2.1.2, $p(x)$ é irredutível. Pelo Lema 4.2.3, conclui-se que nenhuma das suas raízes pode ser exprimível por radicais. □

Capítulo 5

Problema Inverso de Galois

O problema inverso da teoria de Galois consiste em descobrir em que condições podemos encontrar uma extensão de um corpo $\mathbb{K}$ com um dado grupo de Galois. Por outras palavras, dado G um grupo finito e $\mathbb{K}$ um corpo, a questão é: será que existe uma extensão de Galois $\mathbb{L}/\mathbb{K}$, finita, tal que o grupo de Galois da extensão é isomorfo ao grupo G?

Neste capítulo estudaremos extensões de Galois do tipo $\mathbb{C}(x) \subset \mathbb{L}$, ou, mais geralmente, do tipo $\mathbb{K}(x) \subset \mathbb{L}$, onde $\mathbb{K}$ é um corpo algebricamente fechado de característica zero. Pelo Teorema do Elemento Primitivo (Teorema 1.2.26) existe $y \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{C}(x)(y)$ e y é algébrico sobre $\mathbb{C}(x)$. Assim, existe $F(x,z) \in \mathbb{C}(x)[z]$ tal que $F(x,y) = 0$. Tenta-se encontrar y que seja uma série de potências em x, $\mathbb{C}[[x]]$. Começamos por caracterizar extensões finitas de $\mathbb{K}((t)) = \Lambda$, corpo de fracções de $\mathbb{K}[[t]]$.

Na segunda secção trabalhamos com extensões de Galois de $\mathbb{K}(x)$ e a estas associamos dois invariantes, o índice de ramificação e a classe de conjugação. Fixado um grupo G finito, um subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$ e uma família $\mathbf{C}$ de classes de conjugação não triviais indexadas por P, ao terno $\Gamma = [G, P, \mathbf{C}]$ damos o nome de tipo de ramificação. A uma extensão de Galois fazemos corresponder um tipo de ramificação, já que demonstramos que os pontos de ramificação são finitos. O Teorema da Existência de Riemann (Teorema 5.2.13) será apenas enunciado, uma vez que não é conhecida alguma demonstração algébrica. Este teorema dá-nos condições necessárias e suficientes para que existam extensões de Galois de $\mathbb{C}(x)$ de determinado tipo. A secção e o capítulo é terminado com a demonstração da unicidade de extensões de Galois de $\mathbb{C}(x)$ de determinado tipo. Para tal introduzimos o conceito de tipo (fracamente) rígido.

5.1 Extensões das Séries Formais de Laurent

Seja $\mathbb{K}$ um corpo algebricamente fechado de característica zero. Nesta secção construímos Λ o corpo das séries formais de Laurent sobre $\mathbb{K}$ e demonstramos algumas das suas propriedades. Em particular, descrevemos as suas extensões finitas. Começamos por definir o conjunto de certas sequências em $\mathbb{K}$:

Definição 5.1.1 *Seja $\mathbb{K}$ um corpo. Definimos Λ como sendo o conjunto das sequências $(a_i)_{i\in\mathbb{Z}}$, com $a_i \in \mathbb{K}$ tal que existe um inteiro $n \in \mathbb{Z}$ tal que $a_i = 0$, para todo $i < n$.*

Em Λ, define-se uma adição e uma multiplicação da seguinte forma:

$$(a_i) + (b_i) = (a_i + b_i)$$

e

$$(a_i) \,.\, (b_j) = (c_n) = \left(\sum_{i+j=n} a_i b_j \right).$$

Lema 5.1.2 *Seja $\mathbb{K}$ um corpo. O conjunto Λ definido na definição 5.1.1, algebrizado com as operações definidas antes, é um corpo.*

Demonstração O conjunto Λ é um anel comutativo, cujo elemento neutro da adição é a sequência formada apenas por zeros e cujo elemento neutro da multiplicação é a sequência

$$(a_i) = \begin{cases} 1 & se \quad i = 0 \\ 0 & se \quad i \neq 0 \end{cases}$$

.

Seja $(a_i)_{i\in\mathbb{Z}} \in \Lambda$ um elemento não nulo. Então existe um inteiro $N \in \mathbb{Z}$ tal que $a_i = 0$ para $i < N$ e $a_N \neq 0$. Seja $b_j = 0$ para $j < -N$ e $b_{-N} = a_N^{-1}$. Então, a equação

$$\sum_{i+j=n} a_i b_j = 0, n = 1, 2, ...$$

pode ser resolvida em b_j indutivamente fazendo,, $j = -N+1, -N+2, ...$ A sequência (b_i) será o elemento inverso de (a_i). As restantes propriedades são facilmente demonstráveis, deduzindo-se que Λ é de facto um corpo. □

Podemos considerar $\mathbb{K}$ um subcorpo de Λ através do seguinte mergulho:

$$\begin{array}{ccc} \mathbb{K} & \to & \Lambda \\ a & \longmapsto & (a_i) := \begin{cases} a_0 = a \\ a_i = 0, \text{ se } i \neq 0 \end{cases} \end{array}.$$

Seja $t := (t_i)$ a sequência tal que

$$t := (t_i) = \begin{cases} t_1 = 1 \\ t_i = 0, \ i \neq 1 \end{cases}$$

e $\mathbb{K}[t]$ o subanel de Λ gerado por $\mathbb{K}$ e t. $\mathbb{K}[t]$ é o **anel de polinómios sobre** $\mathbb{K}$ **na variável** t cujos elementos são da forma

$$(a_i) = \sum_{i=0}^{M} a_i t^i,$$

com $a_i = 0$ se $i < 0$ ou $i > M$.

Dado $(a_i)_{i\in\mathbb{Z}} \in \Lambda$ tal que $a_i = 0$ se $i < n$ para algum $n \in \mathbb{Z}$, podemo-lo escrever da seguinte forma

$$(a_i) = \sum_{i=n}^{\infty} a_i t^i.$$

Assim, chamamos a Λ o **corpo das séries formais de Laurent sobre** $\mathbb{K}$ e notamos $\Lambda = \mathbb{K}((t))$.

Ao subanel de Λ

$$\mathbb{K}[[t]] := \left\{ \sum_{i=0}^{\infty} a_i t^i \in \Lambda \right\}$$

dá-se o nome de **anel das séries de potências formais sobre** $\mathbb{K}$.

O lema seguinte relaciona-nos os vários anéis introduzidos até ao momento:

Lema 5.1.3 *Seja $\mathbb{K}$ um corpo. Tem-se que $\mathbb{K}(t) \subseteq \mathbb{K}((t))$, $\mathbb{K}(t)$ é o corpo das fracções de $\mathbb{K}[t]$ e $\Lambda = \mathbb{K}((t))$ é o corpo das fracções de $\mathbb{K}[[t]]$.*

Proposição 5.1.4 *$\mathbb{K}[[t]]$ é um domínio de factorização única e $y^n - t$ é irredutível em $\mathbb{K}((t))[y]$ qualquer que seja $n \in \mathbb{N}$.*

Demonstração Note-se que em $\mathbb{K}[[t]]$ todo o elemento da forma $\sum_{i=0}^{\infty} a_i t^i$ com $a_0 \neq 0$ é invertível e que t é primo. É então fácil concluir que $\mathbb{K}[[t]]$ é um domínio de factorização única. Como t é primo e $\mathbb{K}[[t]]$ é DFU, pelo critério de Eisenstein ([4, exercício 3.8.3]) $y^n - t$ é irredutível em $\mathbb{K}((t))[y]$ qualquer que seja $n \in \mathbb{N}$. □

A aplicação

$$\begin{array}{rccc} \varphi: & \mathbb{K}[[t]] & \longrightarrow & \mathbb{K} \\ & \sum_{i=0}^{\infty} a_i t^i & \longmapsto & a_0 \end{array}$$

é um homomorfismo de anéis. Dado $F(y) \in \mathbb{K}[[t]][y]$ um polinómio com coeficientes em $\mathbb{K}[[t]]$ na incógnita y, podemos construir $F_0(y) \in \mathbb{K}[y]$ da seguinte forma; se

$$F(y) = \sum_{i=0}^{M} \left(\sum_{j_i=0}^{\infty} a_{i,j} t^{j_i} \right) y^i,$$

$F_0(y) = \sum_{i=0}^{M} \varphi \left(\sum_{j_i=0}^{\infty} a_{i,j} t^{j_i} \right) y^i = \sum_{i=0}^{M} a_{i,0} y^i$, isto é, estendemos φ a um homomorfismo de $\mathbb{K}[[t]][y]$ em $\mathbb{K}[y]$.

A proposição seguinte permite-nos relacionar factorização em $\mathbb{K}[y]$ com factorização em $\mathbb{K}[[t]][y]$.

Proposição 5.1.5 (Lema de Hensel) *Seja F um polinómio mónico na variável y com coeficientes em $\mathbb{K}[[t]]$. Suponhamos que o polinómio associado a $F(y)$, $F_0(y) \in \mathbb{K}[y]$ se factoriza*

$$F_0 = gh,$$

para $g, h \in \mathbb{K}[y]$ polinómios mónicos tais que $m.d.c(g, h) = 1$. Então,

$$F = GH,$$

com G, H polinómios mónicos na variável y e com coeficientes em $\mathbb{K}[[t]]$ tais que $G_0 = g, H_0 = h$.

Demonstração Seja F tal como nas hipóteses do enunciado do Lema. Podemos escrever

$$F = \sum_{i=0}^{\infty} F_i t^i$$

com $F_i \in \mathbb{K}[y]$. Seja $M := \deg(F) = \deg(F_0)$. Então, $\deg(F_i) < M$ para todo $i > 0$. Seja $r = \deg(g)$ e $s = \deg(h)$. Pretendemos encontrar

$$G = \sum_{i=0}^{\infty} G_i t^i \text{ e } H = \sum_{i=0}^{\infty} H_i t^i$$

com $G_0 = g$, $H_0 = h$ e G_i, $H_i \in \mathbb{K}[y]$ de graus inferiores que r e s, respectivamente.

A condição $F = GH$ é equivalente ao sistema de equações

$$F_n = \sum_{i+j=n} G_i H_j,$$

para cada $n = 0, 1, ...$ Estas equações serão resolvidas por indução. Por hipótese, para $n = 0$, $F_0 = gh = G_0 H_0$. Suponhamos que para dado $n > 0$ se tem para qualquer $m \in \{1, ..., n-1\}$,

$$F_m = \sum_{i+j=m} G_i H_j.$$

Então da n-ésima equação

$$F_n = \sum_{i+j=n} G_i H_j$$

deduz-se que

$$F_n - \sum_{i=1}^{n-1} G_i H_{n-i} = G_0 H_n + H_0 G_n \tag{1}$$

Seja $U_n = F_n - \sum_{i=1}^{n-1} G_i H_{n-i}$. Assim definido, $U_n \in \mathbb{K}[y]$ e tem grau inferior a m. Como, por hipóteses, $(G_0, H_0) = 1$, o ideal gerado por eles é $\mathbb{K}[y]$. Logo, existem polinómios $P, Q \in \mathbb{K}[y]$ tais que

$$G_0 P + H_0 Q = U_n.$$

Pelo algoritmo da divisão, podemos escrever

$$P = H_0 S + R$$

para alguns polinómios $R, S \in \mathbb{K}[y]$, tais que $\deg(R) < \deg(H_0) = s$. Sejam $H_n = R$ e $G_n = Q + G_0 S$. Então, de (1) tem-se

$$\begin{aligned} G_0 R + H_0 (Q + G_0 S) &= G_0 R + H_0 Q + H_0 G_0 S \\ &= G_0 (H_0 S + R) + H_0 Q \\ &= G_0 P + H_0 Q \\ &= U_n \end{aligned}$$

com $\deg(H_n) = \deg(R) < s$. Uma vez que $\deg(G_0) = r$, $\deg(H_n) < s$, $m = rs$ e

$$H_0 G_n = U_n - G_0 H_n$$

deduz-se que

$$\deg(H_0 G_n) < m.$$

Logo, $\deg(G_n) < r$. □

Note-se que $\mathbb{K}[[y]]$ é um anel local completo (é de facto a completação m-ádica com $m = \langle y \rangle$ em $\mathbb{K}[y]$, com $\mathbb{K}$ algebricamente fechado de característica zero cujo ideal maximal é $\langle y \rangle$). A Proposição 5.1.5, exactamente com o mesmo enunciado, é válida para anéis locais completos (em vez de $\mathbb{K}[[t]]$ e em vez do homomorfismo φ usamos $A[y] \longrightarrow (A/m)[y]$ onde m é o ideal maximal do anel local, [2, Exercício 9]).

Deduzimos agora algumas consequências do Lema de Hensel (Proposição 5.1.5) que serão necessárias para o desenvolvimento do trabalho.

Corolário 5.1.6 *Seja $\mathbb{K}$ um corpo algebricamente fechado de característica zero e F um polinómio com coeficientes em $\mathbb{K}[[t]]$ na variável y de grau superior a 1. Se o coeficiente de F_0, de grau n, em y^{n-1} é zero e $F_0(y) \neq y^n$, então F factoriza-se em $F = GH$, com G, H polinómios mónicos na variável y com coeficientes em $\mathbb{K}[[t]]$.*

Demonstração Como $\mathbb{K}$ é um corpo algebricamente fechado, o polinómio $F_0 \in \mathbb{K}[y]$ decompõem-se num produto de polinómios mónicos lineares. Suponhamos que estes factores lineares não são todos iguais. Então, $F_0 = gh$, onde g, h são polinómios não constantes e $(g, h) = 1$ em $\mathbb{K}[y]$. Neste caso, o resultado segue do lema anterior.

Por outro lado, se os factores em que F_0 se decompõe forem todos iguais, podíamos escrever

$$\begin{aligned} F_0 &= (y-a)^n,\ a \in \mathbb{K} \\ &= y^n - nay^{n-1} + \ldots \end{aligned}$$

Como, por hipótese, o coeficiente do termo y^{n-1} é zero, teríamos que $a = 0$, dado que $\mathbb{K}$ é um corpo de característica zero. Deste modo teríamos $F_0 = y^n$, o que contraria a hipótese inicial. Logo, $F = GH$, para alguns $G, H \in \mathbb{K}[[t]][y]$ mónicos. □

Corolário 5.1.7 *Seja $\mathbb{K}$ um corpo algebricamente fechado de característica zero e $\overline{g} \in \mathbb{K}[[t]]$ da forma $\sum_{i=0}^{\infty} a_i t^i$ com $a_0 \neq 0$. Então, para qualquer $n \in \mathbb{N}$, existe $f \in \mathbb{K}[[t]]$ tal que $f^n = g$.*

Demonstração Seja $g \in \mathbb{K}[[t]]$ nas condições do enunciado do Lema e $a_0 \neq 0$. Considere-se $F(y) = y^n - g \in \mathbb{K}[[t]][y]$. Assim, tem-se que $F_0(y) = y^n - a_0$.

Como $\mathbb{K}$ é algebricamente fechado podemos escrever $F_0(y)$ como produto de polinómios lineares mónicos. Note-se que $F_0(y)$ tem n raízes distintas. Seja a_1 uma raiz simples de $F_0(y)$. Então existe $\overline{g} \in \mathbb{K}[y]$ tal que $F_0(y) = (y-a_1)\overline{g}$ e $(y-a_1, \overline{g}) = 1$. Pelo Lema de Hensel, Proposição 5.1.5, existem $H, G \in \mathbb{K}[[t]][y]$ mónicos tais que $H_0 = y - a_1$, $G_0 = \overline{g}$ e $F = HG$. Logo, $H = y - \sum_{i=0}^{\infty} b_i t^i$ onde $b_0 = a_1$, isto é, $F(y)$ tem raiz em $\mathbb{K}[[t]]$ como se desejava demonstrar. □

Introduzimos agora um novo conjunto; dado e um número natural seja $\mathbb{Z}_{1/e}$ o conjunto de todos os números racionais da forma $\frac{i}{e}$, com $i \in \mathbb{Z}$, isto é,

$$\mathbb{Z}_{1/e} = \{i/e : i \in \mathbb{Z}\}.$$

Proposição 5.1.8 *O grupo aditivo $\mathbb{Z}_{1/e}$ é isomorfo a $\mathbb{Z}$ e $\left[\mathbb{Z}_{1/e} : \mathbb{Z}\right] = e$.*

Demonstração A aplicação

$$\begin{aligned} \alpha : \mathbb{Z} &\to \mathbb{Z}_{1/e} \\ i &\mapsto i/e \end{aligned}$$

representa um isomorfismo entre $\mathbb{Z}_{1/e}$ e $\mathbb{Z}$. □

Seja Λ_e o conjunto das sequências $(a_j)_{j\in\mathbb{Z}_{1/e}}$ com $a_j \in \mathbb{K}$, tais que $a_j = 0$ para quase todos os $j < 0$. Defina-se a adição e a multiplicação de forma análoga à definida para Λ. Então:

Lema 5.1.9 *Λ_e é um corpo e a aplicação*

$$\begin{array}{rccc} \alpha: & \Lambda_e & \to & \Lambda \\ & (a_j)_{j\in\mathbb{Z}_{1/e}} & \mapsto & (b_i) \end{array}$$

onde $b_i = a_{i/e}$, é um isomorfismo.

Tomando $\tau := \begin{cases} a_{1/e} = 1 \\ a_j = 0, \quad \text{caso contrário} \end{cases}$, tem-se que $\alpha(\tau) = t$.

O corpo Λ pode ser visto como um subcorpo de Λ_e identificando cada elemento $(a_j)_{j\in\mathbb{Z}} \in \Lambda$ com $(\tilde{a}_j)_{j\in\mathbb{Z}_{1/e}}$ onde $\tilde{a}_j = 0$ se $j \notin \mathbb{Z}$, $\tilde{a}_j = a_j$ se $j \in \mathbb{Z}$. Verifica-se então que $\tau^e = t$. Note-se também que, se $e \mid e'$, então Λ_e é subcorpo de $\Lambda_{e'}$.

Dado $(a_j) \in \Lambda_e$, este pode ser escrito da forma

$$(a_j) = \sum_{j\in\mathbb{Z}_{1/e}} a_j t^j = \sum_{i\in\mathbb{Z}} a_{\frac{i}{e}} \tau^i = \sum_{i\in\mathbb{Z}} b_i \tau^i,$$

identificamos assim Λ_e com $\mathbb{K}\left(\left(t^{1/e}\right)\right) = \mathbb{K}((\tau))$.

Definição 5.1.10 *Um elemento $\zeta \in \mathbb{K}$ tal que $\zeta^n = 1$ diz-se uma **n-ésima raiz da unidade**. Assim, o conjunto das n raízes da unidade coincide com as raízes do polinómio $x^n - 1$. Estas raízes formam um grupo cíclico. Às raízes geradoras deste grupo chamamos **raiz primitiva da unidade**.*

Introduzimos agora condições suficientes para o corpo Λ_e ser uma extensão de Galois de Λ.

Lema 5.1.11 *Suponhamos que $\mathbb{K}$ contém ζ_e uma e-ésima raiz primitiva da unidade. Então Λ_e é Galois sobre Λ de grau e. O grupo de Galois associado à extensão é cíclico, gerado pelo elemento*

$$\begin{array}{rccc} \omega: & \Lambda_e & \to & \Lambda_e \\ & \sum\limits_{i\in\mathbb{Z}} b_i \tau^i & \mapsto & \sum\limits_{i\in\mathbb{Z}} \left(b_i \zeta_e^i\right) \tau^i. \end{array}$$

Tem-se ainda que $\Lambda_e = \Lambda(\tau)$ com $\tau^e = t$.

Demonstração Note-se que pela observação anterior ao enunciado do Lema, cada elemento de Λ_e pode ser escrito na forma $\sum_{i\in\mathbb{Z}} b_i\tau^i$.

Assim definido, $\omega:\ \Lambda_e \rightarrow \Lambda_e$ é um automorfismo de corpos.
Seja $x = \sum_{i\in\mathbb{Z}} b_i\tau^i \in \Lambda_e$ qualquer tal que

$$\omega\left(\sum_{i\in\mathbb{Z}} b_i\tau^i\right) = \sum_{i\in\mathbb{Z}} b_i\tau^i.$$

Assim,

$$\sum_{i\in\mathbb{Z}} b_i\zeta_e^i\tau^i = \sum_{i\in\mathbb{Z}} b_i\tau^i.$$

Logo, para cada $i \in \mathbb{Z}$, $b_i\zeta_e^i = b_i$. Assim, $b_i = 0$ ou $\zeta_e^i = 1$. Se $b_i \neq 0$, como ζ_e é uma e-ésima raiz primitiva da unidade, $e \mid i$, isto é, $i = je$. Ora

$$\tau^e = t$$

logo

$$\tau^i = \tau^{je} = t^j\ .$$

Dado que

$$x = \sum_{i\in\mathbb{Z}} b_i\tau^i = \sum_{b_i\neq 0 \wedge e|i} b_i\tau^i = \sum b_{je}t^j \in \Lambda$$

conclui-se que $x \in \Lambda$ e $(\Lambda_e)^G = \Lambda$ onde $G = \langle\omega\rangle$.
Dado $x = \sum_{i\in\mathbb{Z}} b_i\tau^i \in \Lambda_e$ tem-se que

$$\omega^e\left(\sum_{i\in\mathbb{Z}} b_i\tau^i\right) = \sum b_i\zeta_e^{ie}\tau^i = \sum b_i\tau^i = x.$$

Logo $o(\omega) < e$.
Seja $n \in \mathbb{N}$ tal que $\omega^n = id$. Assim,

$$\omega^n(\tau) = \tau$$

logo

$$\zeta_e^n\tau = \tau$$

concluindo que

$$\zeta_e^n = 1$$

e consequentemente que

$$e \mid n.$$

Logo $o(\omega) = e$ e $G = \langle \omega \rangle$ é um grupo finito de ordem e.

Pelo Teorema de Artin, Teorema 1.3.10, conclui-se que Λ_e é de Galois sobre Λ e o grupo de Galois da extensão é $\langle \omega \rangle$. Mais, tem-se que

$$[\Lambda_e : \Lambda] = |G(\Lambda_e : \Lambda)| = e.$$

□

O Teorema seguinte descreve-nos as extensões finitas de corpos das séries formais de Laurent sobre corpos $\mathbb{K}$ algebricamente fechados de característica zero.

Teorema 5.1.12 *Seja $\mathbb{K}$ um corpo algebricamente fechado de característica zero. Seja Δ uma extensão de corpos de $\Lambda = \mathbb{K}((t))$ de grau finito e. Então $\Delta = \Lambda(\delta)$ com $\delta^e = t$.*

Com vista a demonstrar o Teorema 5.1.12, começamos por demonstrar um resultado acerca da existência de raízes para alguns polinómios com coeficientes em $\mathbb{K}[[t]]$. Demonstra-se que todo o polinómio sobre Λ tem uma raiz em algum Λ_e. Mostramos depois que os dois resultados, Lema 5.1.13 e Teorema 5.1.12 são equivalentes, obtendo assim uma demonstração do resultado pretendido.

Lema 5.1.13 *Seja $\mathbb{K}$ um corpo algebricamente fechado de característica zero. Seja F um polinómio mónico não constante com coeficientes em $\mathbb{K}[[t]]$ na variável y. Então F tem uma raiz em Λ_e, para algum e.*

Demonstração A demonstração é feita por redução ao absurdo. Suponhamos que existem polinómios não constantes com coeficientes em $\mathbb{K}[[t]]$ na variável y sem raízes em Λ_e, qualquer que seja e. Seja F um polinómio de grau mínimo entre os polinómios sem raízes em qualquer Λ_e. Então $n = \deg(F) \geq 2$,

$$F(y) = y^n + \lambda_{n-1} y^{n-1} + \ldots + \lambda_0$$

com $\lambda_\nu \in \mathbb{K}[[t]]$. Então o polinómio

$$\begin{aligned} \widetilde{F}(y) &= F(y - \tfrac{\lambda_{n-1}}{n}) \\ &= \left(y - \tfrac{\lambda_{n-1}}{n}\right)^n + \lambda_{n-1}\left(y - \tfrac{\lambda_{n-1}}{n}\right)^{n-1} + \ldots + \lambda_0 \\ &\vdots \\ &= (y^n - \lambda_{n-1} y^{n-1} + \ldots) + \lambda_{n-1}(y^{n-1} - \ldots) \end{aligned}$$

tem o coeficiente do termo y^{n-1} nulo. Portanto podemos, sem perda de generalidade escolher um polinómio com coeficiente em y^{n-1} nulo. Suponhamos que $F_0(y) \neq y^n$. Então, pelo Corolário 5.1.6, $F(y)$ decompõe-se, contrariando a minimalidade de $F(y)$. Portanto $F_0(y) = y^n$, concluindo-se que todos os λ_ν têm os termos constantes nulos.

Sabemos que, para algum $\nu = 0, 1, ..., n-2$, $\lambda_\nu \neq 0$, caso contrário, $F(y) = y^n$ admitiria a raiz nula. Consideremos apenas tais ν. Seja m_ν a menor potência de t que ocorre com coeficiente não nulo em cada λ_ν:

$$\lambda_\nu = a_\nu t^{m_\nu} + \text{ termos de maior potência,}$$

onde $a_\nu \in \mathbb{K}$ é não nulo. Então $m_\nu > 0$. Seja u o mínimo dos valores $\frac{m_\nu}{n-\nu}$, isto é,

$$u = \min\left\{\frac{m_\nu}{n-\nu} : \nu = 0, 1, ..., n-2 \text{ com } \lambda_\nu = 0\right\}.$$

Então u é um número racional positivo. Tomemos $u = \frac{d}{e}$, com $d, e \in \mathbb{N}$.

Considere-se o mergulho de $\Lambda = \mathbb{K}((t))$ em Λ_e e o polinómio

$$F^*(y) = \tau^{-dn} F(\tau^d y) = y^n + \sum_{\nu=0}^{n-2} \lambda_\nu \tau^{d(\nu-n)} y^\nu \in \Lambda_e[y].$$

O coeficiente em y^ν deste polinómio, caso seja diferente de zero, é uma série de Laurent em τ da forma

$$\begin{aligned} \lambda_\nu \tau^{d(\nu-n)} &= a t^{m_\nu} \tau^{d(\nu-n)} + (\text{termos de maior potência})\ \tau^{d(\nu-n)} \\ &= a\tau^{E_\nu} + (\text{termos de maior potência})\ \tau^{d(\nu-n)} \end{aligned}$$

onde

$$E_\nu = e(n-\nu)\left(\frac{m_\nu}{n-\nu} - u\right) \geq 0,$$

e $E_\nu = 0$ para pelo menos um ν. Deste modo, cada coeficiente de F^* é uma série de potências em τ, e para, no mínimo um ν esta série de potências tem termos constantes não nulos. Portanto, F^* satisfaz as condições do Corolário 5.1.6 (substituindo t por τ), sendo que $F^* = GH$, isto é, F^* decompõe-se sobre $\mathbb{K}[[\tau]]$. Assim, pela minimalidade de n, H, que tem grau estritamente menor que n, tem uma raiz em algum $\Lambda_e\left(\tau^{1/e'}\right)$. Portanto também F^* e, consequentemente, F, têm uma raiz em $\Lambda_e\left(\tau^{1/e'}\right) = \Lambda_{ee'}$. □

Demonstração (do Teorema 5.1.12) Seja Δ uma extensão de corpos de $\Lambda = \mathbb{K}((\tau))$ de grau finito e. Como $\mathbb{K}$ é um corpo de característica zero, existe θ tal que $\Delta = \Lambda(\theta)$. Deste modo, existe um polinómio irredutível $F \in \Lambda[y]$ que admite θ como raiz. Pelo Lema 1.2.22 podemos supor que $\theta \in \Delta$é tal que $F(t) \in \mathbb{K}[[t]]$ é mónico em y. Assim, pelo Lema 5.1.13, F tem uma raiz $\rho \in \Lambda_{e'}$, para algum e'. Uma vez que existe um monomrfismo de $\Delta = \Lambda(\theta)$, para $\Lambda(\rho) \subseteq \Lambda_{e'}$, podemos, sem perda de generalidade, supor que $\Delta \subseteq \Lambda_{e'}$. Uma vez que $G(\Lambda_{e'} : \Lambda)$ é cíclico, para cada divisor e de e' existe um único corpo Λ' com $\Lambda \subset \Lambda' \subset \Lambda_{e'}$ de grau e sobre Λ. Pelo Lema 5.1.11, $\Delta = \Lambda_e = \Lambda\left(t^{1/e}\right)$. Fica assim demonstrado o Teorema. □

5.2 Extensões de $\mathbb{K}(x)$

Tal como foi afirmado no início do capítulo, tomamos $\mathbb{K}$ um corpo algebricamente fechado de característica zero.

Dada $\mathbb{K}(x) \subset \mathbb{L}$ uma extensão de Galois, introduzimos nesta secção dois invariantes que lhe estão associados; os pontos de ramificação e as classes de conjugação associadas a um ponto $p \in \mathbb{P}^1_{\mathbb{K}} = \mathbb{K} \cup \{\infty\}$.

Começamos por fixar um sistema $(\zeta_e)_{e\in\mathbb{N}}$ de e-ésimas raízes primitivas da unidade tais que se $e = e'e''$ então $\zeta_e^{e''} = \zeta_{e'}$.

Seja $\Lambda = \mathbb{K}((t))$ e consideremos Δ uma extensão de Galois de Λ. Suponhamos que $[\Delta : \Lambda] = e$. Pelo Teorema 5.1.12, $\Delta = \Lambda(\delta)$ onde $\delta^e = t$. Assim, $G(\Delta : \Lambda)$ é um grupo cíclico cuja ordem é e. Note-se novamente que por $x^e - t$ ser irredutível (por 5.1.4),os elementos de $G(\Delta : \Lambda)$ são determinados pelas imagens dos elementos da base da extensão, $1, \delta, \delta^2, ..., \delta^{e-1}$. Assim, todo o elemento de $G(\Delta : \Lambda)$ é determinado pela imagem de δ. Mas, se $\alpha \in G(\Delta : \Lambda)$, $\alpha(\delta)$ satisfaz a equação $x^e - t = 0$. As raízes de $x^e - t$ são $\{z\delta : z^e - 1 = 0\}$. Tome-se $\omega \in G(\Delta : \Lambda)$ tal que $\omega(\delta) = \zeta_e\delta$. Assim definido, ω gera $G(\Delta : \Lambda)$. Chamaremos a ω o **gerador especial** de $G(\Delta : \Lambda)$. Seja $\delta' \in \Delta$ tal que $(\delta')^e = t$ para algum inteiro $e' \geq 1$. Note-se que $x^{e'} - t$ é um polinómio irredutível em $\mathbb{K}((t))[x]$. Assim, $e' = [\Lambda(\delta') : \Lambda]$ e $e' \mid [\Delta : \Lambda] = e$. Portanto $e/e' \in \mathbb{Z}$ e $\delta^{e/e'}$ é solução de $x^{e'} - t = 0$. Assim, $\delta' \in \left\{\overline{z}\delta^{e/e'} : \overline{z}^e - 1 = 0\right\}$. Tem-se que

$$\omega(\delta') = \omega(\overline{z}\delta^{e/e'})$$

$$\begin{aligned} &= \overline{z}\omega(\delta^{e/e'}) \\ &= \overline{z}(\zeta_\eta)^{e/e'}\delta^{e/e} \\ &= (\zeta_\eta)^{e/e'}\overline{z}\delta^{e/e} \\ &= (\zeta_\eta)^{e/e}\,\delta' \end{aligned}$$

Mas, dada a hipótese do sistema de raízes,

$$(\zeta_e)^{e/e'} = \zeta_{e/(e/e')} = \zeta_{e'}.$$

Portanto,

$$\omega(\delta') = \zeta_{e'}\delta'.$$

Em particular, se $\Lambda \subset \Delta' \subset \Delta$ então $\omega\,|_{\Delta'}$ é o gerador especial de $G(\Delta' : \Lambda)$.

Seja $p \in \mathbb{P}^1_{\mathbb{K}}$. Para cada $p \in \mathbb{P}^1$ define-se

$$\begin{array}{rccl} \vartheta_p: & \mathbb{K}(x) & \longrightarrow & \mathbb{K}(t) \\ & \kappa & \longmapsto & \kappa \in \mathbb{K} \\ & x & \longmapsto & \begin{cases} t+p & \text{se} \quad p \neq \infty \\ 1/t & \text{se} \quad p = \infty \end{cases} \end{array}$$

um isomorfismo-$\mathbb{K}$ de corpos.

Seja $\mathbb{K}(x) \subset \mathbb{L}$ uma extensão de Galois e γ um elemento primitivo associado a esta extensão, $F(y) \in \mathbb{K}(x)[y]$ o polinómio mínimo de γ sobre $\mathbb{K}(x)$ e $\vartheta_p(F) \in \mathbb{K}(t)[y]$ o polinómio obtido a partir da extensão de ϑ_p a $\mathbb{K}(x)[y]$; isto é

$$\begin{array}{rccc} \vartheta_p : \mathbb{K}(x)[y] & \longrightarrow & \mathbb{K}(t)[y] \\ \sum p_i y^i & \longmapsto & \sum \vartheta_p(p_i) y^i \end{array}$$

Seja h um factor irredutível qualquer de $\vartheta_p(F)$ em $\mathbb{K}((t))[y]$, $\langle h \rangle$ o ideal gerado por h em $\mathbb{K}((t))[y]$ e $\Delta = \mathbb{K}((t))[y]/\langle h \rangle$. Como h é irredutível e $h \in \mathbb{K}((t))[y]$, anel de polinómios com coeficientes num corpo, $\langle h \rangle$ é maximal. Logo Δ é corpo. Mais, Δ é extensão finita de $\mathbb{K}((t)) = \Lambda$ e $[\Delta : \Lambda] = \deg(h)$.

Seja γ' raiz de h em Δ. Tem-se que $\Delta = \Lambda[\gamma']$. Como γ' é raiz de $h \in \Lambda[y]$, é também raiz de $\vartheta_p(F) \in \mathbb{K}(t)[y]$. Portanto γ' é algébrico sobre $\mathbb{K}(t)$ e $\mathbb{K}(t)[\gamma'] = \mathbb{K}(t)(\gamma')$ é corpo.

Podemos agora comparar as seguintes extensões

$$\begin{array}{ccccc} & & \textit{Galois} & & \\ \mathbb{K}(x) & \hookrightarrow & \mathbb{L} = \mathbb{K}(x)[\gamma] & & \\ \downarrow\approx & & \downarrow & & \\ \mathbb{K}(t) & \hookrightarrow & \mathbb{L}_\vartheta := \mathbb{K}(t)[\gamma'] & \hookrightarrow & \Delta = \mathbb{K}((t))[\gamma'] \end{array}$$

Consideremos o isomorfismo anterior $\vartheta_p : \mathbb{K}(x) \longrightarrow \mathbb{K}(t)$ e $F(y) \in \mathbb{K}((x))[y]$ um polinómio irredutível. Como $\vartheta_p : \mathbb{K}(x) \longrightarrow \mathbb{K}(t)$ é um isomorfismo, $\vartheta_p(F)$ é irredutível. Como γ é raiz de $F(y)$ e γ' é raiz de $\vartheta_p(F)$ tem-se que $\mathbb{L} = \mathbb{K}(x)[\gamma] \approx \mathbb{K}(t)[\gamma'] = \mathbb{L}_\vartheta$. Note-se também que $\mathbb{L}$ é corpo de decomposição de F e, dada a forma como $\mathbb{L}_\vartheta$ foi construído, $\mathbb{L}_\vartheta$ é corpo de decomposição de $\vartheta_p(F)$.

Sabemos que $[\Delta : \Lambda] = \deg(h)$. Seja $e = \deg(h)$. Pelo Teorema 5.1.12, conclui-se que $\Delta = \Lambda(\gamma') \simeq \Lambda_e$ sobre Λ (isto é, existe um $\Lambda-$ isomorfismo de Δ em Λ_e). Pelo Lema 5.1.11 conclui-se que Δ é extensão de Galois de Λ.

Assim pelo que foi dito antes, $|G(\Delta : \Lambda)| = o(\omega)$, onde ω é o gerador especial de $G(\Delta : \Lambda)$. Logo,

$$e = [\Delta : \Lambda] = |G(\Delta : \Lambda)| = o(\omega).$$

Mais,

$$\begin{array}{ccc} G(\Delta : \Lambda) & \longrightarrow & G(\mathbb{L}_\vartheta : \mathbb{K}(t)) \\ \alpha & \longmapsto & \alpha\,|_{\mathbb{L}_\vartheta} \end{array}$$

é um homomorfismo de grupos injectivo. Assim, $o(\omega) = o(\omega\,|_{\mathbb{L}_\vartheta})$. Portanto,

$$[\Delta : \Lambda] = |G(\Delta : \Lambda)| = o(\omega\,|_{\mathbb{L}_\vartheta}).$$

Antes de enunciar o próximo resultado relembramos o conceito de classe de conjugação num grupo.

Definição 5.2.1 *Dois elementos a e a' de um grupo G dizem-se* ***conjugados*** *se $a' = bab^{-1}$, para algum $b \in G$.*

Definição 5.2.2 *A* ***classe de conjugação*** *de um elemento x num grupo G é o conjunto de todos os conjugados de x em G:*

$$C_x = \left\{x' \in G : gxg^{-1} = x',\ \textit{para algum } g \in G\right\}.$$

Lema 5.2.3 *Seja $\mathbb{K}(x) \subset \mathbb{L}$, nas condições anteriores, podemos estender $\vartheta_p : \mathbb{K}(x) \longrightarrow \mathbb{K}(t)$ ao isomorfismo $\vartheta : \mathbb{L} \longrightarrow \mathbb{L}_\vartheta$ onde $\mathbb{L}_\vartheta$ é um subcorpo de uma extensão Δ de Galois de Λ. Mais $G(\Delta : \Lambda)$ deixa $\mathbb{L}_\vartheta$ invariante.*

Seja $g_\vartheta = \vartheta^{-1} \circ \omega \circ \vartheta \in G = G(\mathbb{L} : \mathbb{K}(x))$ onde ω é o gerador especial de $G(\Delta : \Lambda)$ construído anteriormente. Se $\widetilde{\Delta}$ for outra extensão de Galois de Λ com subcorpo $\mathbb{L}_\vartheta$ e $\widetilde{\vartheta} : \mathbb{L} \longrightarrow \mathbb{L}_{\widetilde{\vartheta}}$ um isomorfismo que estende ϑ_p, então $g_{\widetilde{\vartheta}}$ e g_ϑ estão na mesma classe de conjugação de G.

Demonstração Tome-se $\Delta = \Lambda[y]/\langle h\rangle$ como antes e $\mathbb{L}_\vartheta = \mathbb{K}(t)[\gamma']$. A primeira afirmação foi demonstrada antes. Resta-nos demostrar que $G(\Delta : \Lambda)$ deixa $\mathbb{L}_\vartheta$ invariante assim como a terceira afirmação.

Uma vez que $\mathbb{L}_\vartheta$ é corpo de decomposição de $\vartheta_p(F)$, $\mathbb{L}_\vartheta$ é gerado sobre $\mathbb{K}(t)$ pelas raízes de $\vartheta_p(F)$. Como $G(\Delta : \Lambda)$ permuta estas raízes, tem-se que $\mathbb{L}_\vartheta$ é invariante por $G(\Delta : \Lambda)$.

Sejam Δ e $\widetilde{\Delta}$ extensões de Galois de Λ. Podemos supor que existe Δ_0 extensão finita de Galois tal que Δ, $\widetilde{\Delta} \subseteq \Delta_0$. Temos que uma extensão $\Lambda \subseteq \Delta$ é Galois se e só se Δ é uma extensão finita, normal e separável de Λ. Seja Δ corpo de decomposição de $f(x)$ e $\widetilde{\Delta}$ corpo de decomposição de $g(x)$, e consideremos Δ_1 o corpo de decomposição de $f(x)g(x)$. Como uma extensão é finita e normal se e só se for o corpo de decomposição de algum polinómio e uma vez que toda a extensão de um corpo de característica zero é separável, resulta que $\Delta_1 = \Delta_0$ é uma extensão finita, normal e separável de Δ, isto é, Δ_0 é uma extensão de Galois de Λ. Note-se que todas as extensões de Galois de Λ são da forma Λ_e.

Seja $\mathbb{L}_{\widetilde{\vartheta}}$ o subcorpo de $\widetilde{\Delta}$ construído de forma análoga ao subcorpo $\mathbb{L}_\vartheta$ de Δ e $\widetilde{\vartheta}$ a extensão de ϑ_p ao isomorfismo de $\mathbb{L}$ em $\mathbb{L}_{\widetilde{\vartheta}}$. Assim, $\mathbb{L}_\vartheta$ e $\mathbb{L}_{\widetilde{\vartheta}}$ são gerados sobre $\mathbb{K}(t)$ pelas raízes de $\vartheta_p F$ em Δ_0. Logo $\mathbb{L}_\vartheta = \mathbb{L}_{\widetilde{\vartheta}}$. Seja $h = \vartheta^{-1}\widetilde{\vartheta} \in G = G(\mathbb{L} : \mathbb{K}(x))$. Como, $G(\Delta_0 : \Lambda) = \langle\omega_0\rangle$ e $G(\Delta : \Lambda) = \langle\omega_0 \mid_\Delta\rangle$, então,

$$g_{\widetilde{\vartheta}} = \widetilde{\vartheta}^{-1}\omega_0\widetilde{\vartheta} = h^{-1}\vartheta^{-1}\omega_0\vartheta h = h^{-1}g_\vartheta h,$$

isto é, $g_{\widetilde{\vartheta}}$ e g_ϑ pertencem à mesma classe de conjugação de G. □

Definição 5.2.4 *Dada $\mathbb{K}(x) \subset \mathbb{L}$ uma extensão de Galois, a* ***classe de conjugação de g_ϑ*** *em G nota-se por $\mathbf{C}_p$ e designa-se por* ***classe de G associada a p.***

Note-se que C_p depende unicamente de p e de $\mathbb{L}$.

Definição 5.2.5 *À ordem (comum) dos elementos de C_p dá-se o nome de* ***índice de ramificação*** *de $\mathbb{L}$ em p e nota-se por $e = e_{\mathbb{L},p}$.*

Proposição 5.2.6 *Nas condições anteriores, todos os factores irredutíveis de $\vartheta_p F$ em $\Lambda[y]$ têm o mesmo grau, o qual é igual ao índice de ramificação de $\mathbb{L}$ em p.*

Demonstração Seja ω o gerador especial de $G(\Delta : \Lambda)$. Como $\Lambda \subseteq \Delta$ é uma extensão de Galois,

$$[\Delta : \Lambda] = |G(\Delta : \Lambda)| = o(\omega).$$

Uma vez que a restrição induz um monomorfismo

$$\begin{array}{ccc} G(\Delta : \Lambda) & \hookrightarrow & G(\mathbb{L}_\vartheta : \mathbb{K}(t)) \\ \alpha & \mapsto & \alpha\,|_{\mathbb{L}_\vartheta} \end{array},$$

e

$$o(\omega) = o(\omega\,|_{\mathbb{L}_\vartheta}) = o(g_\vartheta)$$

Portanto,

$$e_{\mathbb{L},p} = [\Delta : \Lambda] = \deg(h).$$

Se h' for um outro factor irredutível de $\vartheta_p F$ em $\mathbb{K}((t))[y]$, $\Delta' = \mathbb{K}((t))[y]/\langle h' \rangle$ é outra extensão de Galois. Pela segunda parte do Lema 5.2.3 sabemos que se $\mathbb{L}_{\widetilde{\vartheta}}$ for um subcorpo intermédio da extensão e $\widetilde{\vartheta} : \mathbb{L} \longmapsto \mathbb{L}_{\widetilde{\vartheta}}$ um isomorfismo que estende ϑ_p, então $g_{\widetilde{\vartheta}}$ e g_ϑ estão na mesma classe, logo,

$$\deg(h') = [\Delta' : \Lambda] = o(g_{\widetilde{\vartheta}}) = o(g_\vartheta) = e_{L,p} = \deg(h).$$

□

Estabelecemos agora condições suficientes para o índice de ramificação de uma extensão $\mathbb{L}$ de Galois de $\mathbb{K}(x)$ num ponto p, $e_{\mathbb{L},p}$, ser 1. Note-se que isto é o mesmo que se ter que $\vartheta_p F$ se decompõe em factores lineares em $\mathbb{K}((t))[y]$.

Proposição 5.2.7 *Nas condições anteriores, podemos escolher um elemento primitivo γ de $\mathbb{L}$ sobre $\mathbb{K}(x)$ tal que o polinómio mínimo de γ sobre $\mathbb{K}(x)$ $F(y) = F(x, y) \in \mathbb{K}[x, y]$ é mónico em y. Assim, o discriminante $D(x)$ de $F(y)$ sobre $\mathbb{K}(x)$ é um elemento de $\mathbb{K}[x]$. Se $p \in \mathbb{K}$ e $D(p) \neq 0$ então $e_{\mathbb{L},p} = 1$.*

Demonstração Seja γ tal que $\mathbb{L} = \mathbb{K}(x)(\gamma)$ e $F(y) \in \mathbb{K}(x)[y]$ irredutível tal que $F(\gamma) = 0$. Existe $d(x) \in \mathbb{K}[x]$ tal que $d(x)F(y) \in \mathbb{K}[x][y]$. Usando a demonstração do Lema 1.2.22 podemos, sem perda de generalidade, supor que $F(y) \in \mathbb{K}[x, y]$ e que é mónico em y. Considere-se agora o seu discriminante, para tal, e atendendo à forma como a noção de discriminante foi introduzida, pensamos em $F(y) \in \mathbb{K}(x)[y]$. Sejam $p_i(x)$ as suas raízes. Pela Proposição 1.2.42,

$$D(x) = \prod_{i<j} (p_i(x) - p_j(x))^2 \in \mathbb{K}[x].$$

Como $F(y)$ é irredutível em $\mathbb{K}(x)[y]$ e $\mathbb{K}$ é um corpo de característca zero, $F(y)$ é separável logo, por 1.2.36, $D(x) \neq 0$.

Considere-se $p \in \mathbb{K}$ e o polinómio em y, $F(p, y) \in \mathbb{K}[y]$. As suas raízes serão $p_1(p), ..., p_n(p)$ e o seu discriminante $D(p)$. Se $p \in \mathbb{K}$ for tal que $D(p) \neq 0$, então $F(p, y) \in \mathbb{K}[y]$ é separável. Tem-se que $(\vartheta_p F)(y) = F(t + p, y)$. Assim $\vartheta_p F$ é um polinómio mónico em y com coeficientes em $\mathbb{K}[t]$. Mais, $(\vartheta_p F)_0(y) = F(p, y)$.

Se $F(p, y)$ é separável, pelo Lema de Hensel, Lema 5.1.5, $\vartheta_p F$ factoriza-se em produtos de factores lineares em $\Lambda[y]$. Logo $e_{\mathbb{L},p} = 1 =$ grau dos factores irredutíveis de $\vartheta_p F$. □

Definição 5.2.8 *Seja $\mathbb{K}(x) \subset \mathbb{L}$ uma extensão de Galois e $p \in \mathbb{P}^1_{\mathbb{K}}$. Diz-se que p é um **ponto de ramificação** da extensão $\mathbb{K}(x) \subset \mathbb{L}$ se $e_{\mathbb{L},p} > 1$, isto é, se a classe C_p de $G(\mathbb{L} : \mathbb{K}(x))$ é não trivial.*

A Proposição 5.2.7 dá-nos condições suficientes para um ponto não ser ponto de ramificação. Mais, podemos concluir que o conjunto dos pontos de ramificação é finito.

Seja $\mathbb{K}(x) \subset \mathbb{L}$, nas condições anteriores, podemos estender $\vartheta_p : \mathbb{K}(x) \longrightarrow \mathbb{K}(t)$ ao isomorfismo $\vartheta : \mathbb{L} \longrightarrow \mathbb{L}_\vartheta$ onde $\mathbb{L}_\vartheta$ é um subcorpo de uma extensão Δ de Galois de Λ. Mais $G(\Delta : \Lambda)$ deixa $\mathbb{L}_\vartheta$ invariante. Seja $g_\vartheta = \vartheta^{-1} \circ \omega \circ \vartheta \in G = G(\mathbb{L} : \mathbb{K}(x))$ onde ω é o gerador especial de $G(\Delta : \Lambda)$ construído anteriormente. Se $\widetilde{\Delta}$ for outra extensão de Galois de Λ com subcorpo $\mathbb{L}_\vartheta$ e $\widetilde{\vartheta} : \mathbb{L} \longrightarrow \mathbb{L}_{\widetilde{\vartheta}}$ um isomorfismo que estende ϑ_p, então $g_{\widetilde{\vartheta}}$ e g_ϑ estão na mesma classe de conjugação de G, pelo Lema 5.2.3.

Proposição 5.2.9 *Seja $\mathbb{K}(x) \subset \mathbb{L}$ uma extensão de Galois e $\mathbb{K}(x) \subset \mathbb{L}'$ outra extensão de Galois com $\mathbb{L}' \subset \mathbb{L}$. Então a aplicação restrição de $G = G(\mathbb{L} : \mathbb{K}(x))$ em $G' = G(\mathbb{L}' : \mathbb{K}(x))$ envia as classes de conjugação C_p de G nas classes de C'_p de G' associadas a p.*

Demonstração Consideremos o isomorfismo $\vartheta : \mathbb{L} \to \mathbb{L}_\vartheta$ definido no Lema 5.2.3 e $g_\vartheta = \vartheta^{-1} \circ \omega \circ \vartheta \in G = G(\mathbb{L} : \mathbb{K}(x))$ onde ω é o gerador especial de $G(\Delta : \Lambda)$. Seja $\vartheta' = \vartheta \mid_{\mathbb{L}'}$. Assim, ϑ' é um isomorfismo de $\mathbb{L}$ em $\vartheta'(\mathbb{L}') \subset \Delta$. Uma vez que

$$g_{\vartheta'} = (\vartheta')^{-1} \omega \vartheta' = \vartheta^{-1} \omega \vartheta \mid_{\mathbb{L}'}$$

tem-se o resultado. □

Exemplo Seja $\mathbb{K}$ um corpo de característica zero, $f(x) \in \mathbb{K}(x), n \in \mathbb{N}, n \geq 2$, $g(y) = y^n - f \in \mathbb{K}(x)[y]$ e f_0 uma raiz de g em alguma extensão de $\mathbb{K}(x)$. Considere-se $\mathbb{L} = \mathbb{K}(x)(f_0)$. Como $\mathbb{K}$ é algebricamente fechado, a menos de n-ésimas potências, podemos supor que

$$f(x) = \prod_j (x - p_j)^{m_j}$$

com $p_j \in \mathbb{K}$ distintos dois a dois e $1 \leq m_j \leq n-1$.

Portanto, $g(y) = y^n - \prod_j (x - p_j)^{m_j}$. Consideremos o isomorfismo definido anteriormente,

$$\begin{array}{rccl} \vartheta_p : & \mathbb{K}(x) & \longrightarrow & \mathbb{K}(t) \\ & \kappa & \longmapsto & \kappa \in \mathbb{K} \\ & x & \longmapsto & \begin{cases} t+p & \text{se} \quad p \neq \infty \\ 1/t & \text{se} \quad p = \infty \end{cases} \end{array}.$$

Seja $p \in \mathbb{K}$. Então,

$$\begin{aligned} \vartheta_{p_i}(y^n - f(x)) &= y^n - \prod_j (t + p_i - p_j)^{m_j} \\ &= y^n - t^{m_i} \prod_{j \neq i} (t + p_i - p_j)^{m_j} \end{aligned}$$

Mas $g(t) = \prod_{j \neq i} (t + p_i - p_j)^{m_j} \in \mathbb{K}[[t]]$ e, pelo Corolário 5.1.7, para algum $h \in \mathbb{K}[[t]]$, $g(t) = h^n$. Portanto,

$$\vartheta_{p_i}(y^n - f(x)) = y^n - t^{m_j} h^n$$

Notemos $e_i = e_{\mathbb{L},p_i}$. Deste modo,

$$\Lambda_{e_i} = \Lambda\left((t^{m_i} h^n)^{1/n}\right) = \Lambda\left(t^{m_i/n} h\right) = \Lambda\left(t^{m_i/n}\right),$$

uma vez que $h \in \mathbb{K}[[t]]$. Pela demonstração do Lema 5.1.11 tem-se que

$$e_i = [\Lambda_{e_i} : \Lambda] = |G(\Lambda_{e_i} : \Lambda)|$$

onde $\Lambda_{e_i} = \Lambda(t^{m_i/n})$.

Uma vez que $\left[\Lambda(t^{1/n}) : \Lambda\right] = n$ e como

$$\Lambda \subseteq \Lambda(t^{m_i/n}) \subseteq \Lambda(t^{1/n}),$$

$e_i \mid n$ e $G(\Lambda(t^{m_i/n}) : \Lambda) \leq G(\Lambda(t^{1/n}) : \Lambda)$. Seja ω o gerador de $G(\Lambda(t^{1/n}) : \Lambda)$. Assim, ω^{m_i} é o gerador de $G(\Lambda(t^{m_i/n}) : \Lambda)$ e

$$e_i = o(G(\Lambda(t^{m_i/n}) : \Lambda)) = \frac{n}{m.d.c.(n, m_i)}.$$

Se $p \in \mathbb{K}$ é tal que $p \neq p_i$ então $D(p) \neq 0$, e pela Proposição 5.2.7, $e_{\mathbb{L},p} = 1$. Como, por definição, p é um ponto de ramificação se $e_{\mathbb{L},p} > 1$, tem-se que apenas os $p_i's$ são pontos de ramificação de $\mathbb{L}$.

No caso em que $p = \infty$, tomemos o polinómio $f(x)$ na forma $f(x) = a_m x^m + ... + a_0$ com $a_m \neq 0$. Então

$$\begin{aligned} \vartheta_\infty\left(y^n - f\left(x\right)\right) &= y^n - (a_m(1/t)^m + ... + a_0) \\ &= y^n - t^{-m}(a_m + ... + a_0 t^m). \end{aligned}$$

Assim, fazendo $e_\infty = e_{\mathbb{L},\infty}$,

$$\Lambda_{e_\infty} = \Lambda\left(f\left(1/t\right)^{1/n}\right) = \Lambda\left(t^{-m/n}\left(a_m + ... + a_0 t^m\right)^{1/n}\right) = \Lambda\left(t^{-m/n}\right) = \Lambda\left(t^{m/n}\right).$$

Por argumento análogo ao anterior,

$$e_\infty = \frac{n}{m.d.c(n, m)}$$

onde $m = \deg(f)$. Tem-se que $e_\infty > 1$ se e só se n não divide $\deg(f)$.

Sabemos que o número de pontos de ramificação de uma extensão $\mathbb{L}$ de Galois de $\mathbb{K}(x)$ é finito.

Pretendemos agora estudar como é que os pontos de ramificação e as classes de conjugação de uma extensão de Galois $\mathbb{K}(x) \subset \mathbb{L}$ variam quando passamos para uma determinada extensão de Galois de $\mathbb{K}(x)$.

Lema 5.2.10 (Argumento do ciclo da ramificação) *Sejam $\mathbb{K}(x) \subset \mathbb{L}$ e $\mathbb{K}(x) \subset \mathbb{L}'$ extensões de Galois de grau n. Para cada $p \in P^1_{\mathbb{K}}$, seja C_p (respectivamente, C'_p) a classe de $G = G(\mathbb{L} : \mathbb{K}(x))$ (respectivamente, $G' =$*

$G(\mathbb{L}' : \mathbb{K}(x))$) associada a p. Seja $\alpha \in Aut(\mathbb{K})$ e $m \in \mathbb{N}$ tal que $\alpha^{-1}(\zeta_n) = \zeta_n^m$ (onde $(\zeta_e)_{e\in\mathbb{N}}$ é um sistema compatível de e-ésimas raízes primitivas da unidade em $\mathbb{K}$). Suponhamos que α se estende a um isomorfismo $\lambda : \mathbb{L} \to \mathbb{L}'$ tal que $\lambda(x) = x$. Seja λ^* o isomorfismo de grupos de G em G' induzido por λ ($g \in G \longrightarrow \lambda g \lambda^{-1}$). Então

$$C'_{\alpha(p)} = \lambda^* (C_p)^m .$$

Note-se que no caso em que $\mathbb{L} = \mathbb{L}'$, α pode ser estendido a um isomorfismo λ de $\mathbb{L}$ em $\mathbb{L}'$ tal que $\lambda(x) = x$, temos que $C'_{\alpha(p)} = \lambda C_p^m \lambda^{-1}$, isto é, o Lema 5.2.10, diz-nos como variam as classes de conjugação quando consideramos as imagens dos pontos por um automorfismo de $\mathbb{K}$.

Demonstração [do Lema 5.2.10] Seja $p \in P^1_{\mathbb{K}}$ e $e = e_{\mathbb{L},p}$. Como, por definição, e é a ordem de elementos de G e $|G| = n$, $e \mid n$. Se $a \in \mathbb{N}$ for tal que $n = ae$, dada a forma do sistema $(\zeta_n)_{n\in\mathbb{N}}$ (sistema compatível de raízes primitivas da unidade em $\mathbb{K}$), temos que $\zeta_n^a = \zeta_e$, logo

$$\alpha^{-1}(\zeta_e) = \alpha^{-1}(\zeta_n^a) = \left(\alpha^{-1}(\zeta_e)\right)^a = (\zeta_n^m)^a = (\zeta_n^a)^m = \zeta_e^m.$$

Considere-se

$$\begin{array}{rccc} \widetilde{\alpha}: & \Lambda_e = \mathbb{K}((\tau)) & \longrightarrow & \Lambda_e = \mathbb{K}((\tau)) \\ & \sum b_i \tau^i & \longmapsto & \sum \alpha(b_i)\tau^i \end{array} .$$

É fácil verificar que $\widetilde{\alpha}$ é um automorfismo que estende $\alpha \in aut(\mathbb{K})$. Considere-se a identificação de $\mathbb{K}((t))$ com um subcorpo de Λ_e, com $t = \tau^e$. Tal como no Lema 5.1.11, seja ω o gerador de $G(\Lambda_e : \Delta)$ tal que $\omega(\tau) = \zeta_e \tau$. Assim, tem-se que

$$\widetilde{\alpha}^{-1}\omega\widetilde{\alpha}(\tau) = \widetilde{\alpha}^{-1}\omega(\tau) = \alpha^{-1}(\zeta_e\tau) = \alpha^{-1}\zeta_e\tau = \zeta_e^m\tau = \omega^m(\tau).$$

Portanto,

$$\widetilde{\alpha}^{-1}\omega\widetilde{\alpha} = \omega^m.$$

Seja ϑ o isomorfismo de $\mathbb{L}$ num subcorpo de Λ_e que estende ϑ_p (existe pelo Lema 5.2.3). Assim,

$$\vartheta' := \widetilde{\alpha} \circ \vartheta \circ \lambda^{-1}$$

é um isomorfismo de $\mathbb{L}'$ num subcorpo de Λ_e. Tem-se também que

$$\vartheta'(x) = \widetilde{\alpha}(\vartheta(x)) = \widetilde{\alpha}(t + p) = t + \alpha(p), \text{ se } p \neq \infty$$

e

$$\vartheta'(x) = \widetilde{\alpha}(\vartheta(x)) = \widetilde{\alpha}(\frac{1}{t}) = \frac{1}{t}, \text{ se } p = \infty.$$

Uma vez que λ e $\widetilde{\alpha}$ induzem o automorfismo α em $\mathbb{K}$, ϑ' é a identidade em $\mathbb{K}$ e podemos concluir que ϑ' é um isomorfismo que estende $\vartheta_{\alpha(p)}$ de $\mathbb{L}'$ a um subcorpo de Λ_e.

$$\begin{aligned} g_{\vartheta'} &= (\vartheta')^{-1} \circ \omega \circ \vartheta' \\ &= (\widetilde{\alpha}\vartheta\lambda^{-1})^{-1}\omega(\widetilde{\alpha}\vartheta\lambda^{-1}) \\ &= \lambda\vartheta^{-1}\widetilde{\alpha}^{-1}\omega\widetilde{\alpha}\vartheta\lambda^{-1} \\ &= \lambda\vartheta^{-1}\omega^m\vartheta\lambda^{-1} \\ &= \lambda g_\vartheta^m\lambda^{-1} \\ &= \lambda^*(g_\vartheta)^m \end{aligned}$$

conclui-se o resultado pretendido. □

Associada a $\mathbb{K}(x) \subset \mathbb{L}$ extensão de Galois temos o grupo dos automorfismos de $\mathbb{L}$ que fixam $\mathbb{K}(x)$, $G = G(\mathbb{L} : \mathbb{K}(x))$, o conjunto finito $P \subseteq \mathbb{P}^1_{\mathbb{K}}$ de pontos de ramificação e para cada $p \in \mathbb{P}^1_{\mathbb{K}}$, a classe de conjugação C_p de G.

Definição 5.2.11 *Considere-se os triplos $(G, P, \mathbf{C})$ onde G é um grupo finito, P um subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$ e $\mathbf{C} = (C_p)_{p\in P}$ uma família de classes de conjugação não triviais de G, indexadas por P. Diz-se que dois triplos $(G, P, \mathbf{C})$ e $(G', P', \mathbf{C}')$ são* ***equivalentes*** *se $P = P'$ e se existe um isomorfismo φ de G em G' tal que $\varphi(C_p) = C'_p$, para todo o $p \in P$.*

A relação "ser equivalente a" definida no conjunto dos triplos define uma relação de equivalência.

Definição 5.2.12 *Dado um triplo $(G, P, \mathbf{C})$ onde G é um grupo finito, P um subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$ e $\mathbf{C} = (C_p)_{p\in P}$ uma família de classes de conjugação não triviais de G, indexadas por P denotamos por $\Gamma = [G, P, \mathbf{C}]$ a classe de equivalência de $(G, P, \mathbf{C})$. A Γ damos o nome de* ***tipo de ramificação****.*

Pelo Lema 5.2.10 concluimos que o tipo de ramificação é invariante por $\mathbb{K}(x)$-isomorfismos de $\mathbb{L}$, onde $\mathbb{L}$ é uma extensão de Galois de $\mathbb{K}(x)$.

Seja $G = (\mathbb{L} : \mathbb{C}(x))$. A existência da extensão de Galois de $\mathbb{C}(x)$ do tipo $\Gamma = [G, P, \mathbf{C}]$, onde P é um subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$ e $\mathbf{C} = (C_p)_{p\in P}$ uma

família de classes de conjugação não triviais de G, indexadas por P, é-nos garantida no próximo teorema desde que certas condições sejam satisfeitas. A sua demonstração será omitida, mas pode ser encontrada em [13].Não é conhecida demonstração algébrica do resultado que será apresentado.

Teorema 5.2.13 (Teorema da Existência de Riemann) *Seja $\Gamma = [G, P, \mathbf{C}]$ um tipo de ramificação, $r = |P|$ e enumeremos os elementos de P, $p_1, ..., p_r$. Então existe uma extensão de Galois de $\mathbb{C}(x)$ do tipo Γ se e só:*

1. *se existem geradores $g_1, ...g_r$ de G com $g_1 \cdot ... \cdot g_r = 1$;*
2. *$g_i \in C_{p_i}$ para $i = 1, ..., r$.*

Note-se que se $\mathbb{C}(x) \subset \mathbb{L}$ for uma extensão de Galois com apenas um ponto de ramificação, então $\mathbb{L}$ é uma extensão do tipo $[(G, P, \mathbf{C})]$ onde $P = \{p\}$, $G = G(\mathbb{L} : \mathbb{C}(x))$, e $\mathbf{C} = \{C_p\}$. Pelo Teorema da Existência de Riemann, conclui-se que existe um gerador g de G tal que $g = Id$ e $g \in C_p$. Então $G = \{Id\}$ e consequentemente $\mathbb{L} = \mathbb{C}(x)$. Conclui-se assim que não existem extensões de Galois próprias de $\mathbb{C}(x)$ com menos de 2 pontos de ramifcação.

Suponhamos agora que a extensão de Galois de $\mathbb{C}(x) \subset \mathbb{L}$ tem exactamente dois pontos de ramificação. Assim, $\mathbb{C}(x) \subset \mathbb{L}$ é do tipo $[(G, P, \mathbf{C})]$ onde $P = \{p_1, p_2\}$, $G = G(\mathbb{L} : \mathbb{C}(x))$, e $\mathbf{C} = \{C_{p_1}, C_{p_2}\}$. Pelo Teorema da Existência de Riemann, existem g_1, g_2 geradores de G tais que

1. $g_1 g_2 = Id$;
2. $g_1 \in C_{p_1}$, $g_2 \in C_{p_2}$.

Conclui-se então que $g_1^{-1} = g_2$ e que G é cíclico.

Observação 5.2.14 *Todo o grupo finito é grupo de Galois de alguma extensão de $\mathbb{C}(x)$.*

Uma vez que pode existir mais do que uma extensão de Galois de $\mathbb{C}(x)$ com determinado tipo de ramificação Γ sem que estas sejam necessariamente isomorfas, impomos agora uma nova condição, exigindo que os geradores de G, grupo de Galois da extensão cuja existência nos é dada pelo Teorema da Existência de Riemann, sejam de certa forma únicos.

Definição 5.2.15 *Seja $(C_1, ..., C_r)$ um r-uplo de classes de conjugação num grupo G. Dizemos que o uplo de classes é* ***rígido*** *(respectivamente,* ***fracamente rígido****) em G se:*

1. *existem geradores $g_1, ..., g_r \in G$ com $g_1 \cdot ... \cdot g_r = 1$ e $g_i \in C_i$, para $i = 1, ..., r$.*

2. *Se $g'_1, ..., g'_r$ é outro conjunto de geradores de G com as mesmas propriedades (dos geradores de 1.), então existe um único elemento $g \in G$ (respectivamente, um automorfismo γ de G) tal que $gg_ig^{-1} = g'_i$ (respectivamente, $\gamma(g_i) = g'_i$), para $i = 1, ..., r$.*

Note-se que no caso de extensões de Galois do tipo Γ onde as classes formam um conjunto fracamente rígido, o automorfismo γ é único já que é definido pelas imagens de conjuntos de geradores.

Definição 5.2.16 *Um tipo $\Gamma = \left[G, P, (C_p)_{p \in P}\right]$ diz-se rígido (respectivamente, fracamente rígido) se os elementos de P podem ser enumerados por $p_1, ..., p_r$, com $r = |P|$ tais que as classes $C_i = C_{p_i}, i = 1, ..., r$ formem um r-uplo rígido (respectivamente, fracamente rígido) em G.*

Teorema 5.2.17 *Para cada $\Gamma = [G, P, \mathbf{C}]$ tipo fracamente rígido, existe uma única extensão de Galois de $\mathbb{C}(x)$ do tipo Γ, a menos de isomorfismo.*

Demonstração A existência é consequência do Teorema da Existência de Riemann.

Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ duas extensões de Galois fracamente rígidas do mesmo tipo Γ. Podemos, sem perda de generalidade, supor que $\mathbb{L}_1$ e $\mathbb{L}_2$ estão contidas em $\mathbb{L}$, extensão de Galois de $\mathbb{C}(x)$. Sejam $G = G(\mathbb{L} : \mathbb{C}(x))$, $G_1 = G(\mathbb{L}_1 : \mathbb{C}(x))$ e $G_2 = G(\mathbb{L}_2 : \mathbb{C}(x))$. Podemos agora definir para cada $j \in \{1, 2\}$, a aplicação

$$\begin{array}{rccc} \rho_j : & G & \to & G_j \\ & g & \longmapsto & g|_{\mathbb{L}_j} \end{array}$$

é um homomorfismo de grupos. Note-se que a aplicação está bem definida já que $\mathbb{L}$, sendo extensão de Galois, é corpo de decomposição de algum polinómio sobre $\mathbb{C}(x)$ e as suas raízes são transformadas por qualquer elemento de G ainda em raízes do mesmo polinómio.

Dado $p \in \mathbb{P}^1_{\mathbb{C}}$ sejam C_p e $C_p^{(j)}$ as classes de conjugação associadas a G e a G_j, respectivamente, então, pela Proposição 5.2.9,

$$\rho_j(C_p) = C_p^{(j)}.$$

Sejam $p_1, ..., p_r$ os pontos de ramificação de $\mathbb{L}$. Pelo Teorema da Existência de Riemann existem geradores $g_1, ..., g_r$ de G com $g_1 \cdot ... \cdot g_r = 1$ e $g_i \in C_{p_i}$, para cada $i = 1, ..., r$. Então, para cada $j \in \{1, 2\}$, $\rho_i(g_1), ..., \rho_i(g_r)$ são geradores de G_j e satisfazem propriedades análogas.

Como $\mathbb{L}_1$ e $\mathbb{L}_2$ são extensões do mesmo tipo, existe um isomorfismo $\epsilon : G_2 \to G_1$ tal que $\epsilon\left(C_p^{(2)}\right) = C_p^{(1)}, \forall p \in P$. Assim, $\epsilon(\rho_2(g_1)), ..., \epsilon(\rho_2(g_r))$ satisfazem as mesmas propriedades que $\rho_1(g_1), ..., \rho_1(g_r)$.

Uma vez que o tipo é fracamente rígido, existe um automorfismo δ de G_1 tal que $\delta(\epsilon(\rho_2(g_i))) = \rho_1(g_i)$, para todo $i = 1, ..., r$. Considere-se

$$\gamma := \delta\epsilon : G_2 \to G_1.$$

Assim, γ é um isomorfismo tal que $\gamma(\rho_2(g_i)) = \rho_1(g_i)$, qualquer que seja $i = 1, ..., r$. Assim, $\rho_1 = \gamma \circ \rho_2$ (basta que as imagens dos geradores sejam as mesmas).

Como γ é um isomorfismo, facilmente se verifica que $\ker \rho_1 = \ker \rho_2$. Uma vez que $G(\mathbb{L} : \mathbb{L}_1) = \{g \in G(\mathbb{L} : \mathbb{C}(x)) : g|_{\mathbb{L}_1} = Id\} = \ker \rho_1$, resulta que $\mathbb{L}^{\ker \rho_1} = \mathbb{L}_1$, pois a extensão $\mathbb{L} \supseteq \mathbb{L}_1$ é Galois. Analogamente, $\mathbb{L}^{\ker \rho_2} = \mathbb{L}_2$. Como $\ker \rho_1 = \ker \rho_2$, resulta que $\mathbb{L}_1 = \mathbb{L}_2$. □

Índice

Bibliografia

[1] Michael Artin, *Algebra*, Englewood Cliffs, Prentice-Hall, 1991.

[2] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, University of Oxford, Addison-Wesley, 1969.

[3] Owen J. Brison, *Teoria de Galois*, Textos de Matemática (3^aedição), Volume 6, Departamento de Matemática, Faculdade de Ciências da Universidade de Lisboa, Lisboa, 1999.

[4] Rui Loja Fernandes e Manuel Ricou, *Introdução à Álgebra*, Ensino da Ciência e da Tecnologia, Instituto Superior Técnico, IST Press, 2004.

[5] John B. Fraleigh, *A First Course in Abstract Algebra* (5^aedição), Addison-Wesley, Reading, Massachusetts, 1967.

[6] Frederick M.Goodman, *Algebra, Abstract and Concrete*, Prentice Hall, New Jersey, 1998.

[7] Charles Hadlock, *Field Theory and its Classical Problems*, The Carus Mathematical Monographs, Volume 16, The Mathematical Associaion of America, 1978.

[8] Serge Lang, *Algebra* (3^aedição), Addison-Wesley, Reading, Massachusetts, 1993.

[9] Gunter Malle e B. Heinrich Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin, 1999.

[10] John Maxfield, *Abstract Algebra and Solutions by Radicals*, Dover Publications, Inc., New York, 1992.

[11] António Monteiro e Isabel Matos, *Algebra, Um primeiro curso*, 2ªedição, Escolar Editora, Lisboa, 2001.

[12] Joseph J. Rotman, *Advanced Modern Algebra*, Prentice Hall, 2002.

[13] Helmut Volklein, *Groups as Galois groups: an introduction*, Cambridge University Press, Cambridge, 1996.

[14] Seth Warner, *Modern Algebra*, Dover Publications, Inc., New York, 1990.