Universidade Federal de Minas Gerais

Instituto de Ciências Exatas

Departamento de Matemática

Dualidade de Grupos, Cohomologia Galoisiana e Correspondências de Kummer

Vinícius Lara Lima

Belo Horizonte, dezembro de 2015

Vinícius Lara Lima

Dualidade de Grupos, Cohomologia Galoisiana e Correspondências de Kummer

Dissertação apresentada ao corpo docente de Pós-Graduação em Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como parte dos requisitos para a obtenção do título de Mestre em Matemática.

Orientador: Renato Vidal da Silva Martins

Coorientador: André Gimenez Bueno

Belo Horizonte

2015

Agradeço à minha família, professores, secretárias da pós
e colegas da UFMG.

RESUMO

O assunto a ser tratado neste trabalho está relacionado à Teoria de Galois. Iremos estudar as consequências do teorema fundamental de Galois, e dissertar sobre o Teorema de Artin-Schreier, que mostra o fato de uma extensão de corpo E sobre K de característica p, com grau da extensão igual à sua característica, pode ser escrita como uma extensão simples gerada pela raiz de um polinômio do tipo $x^p - x - a$.

Estudaremos Cohomologia de Galois, em particular, mostraremos, como consequência do Teorema 90 de Hilbert, que dada uma extensão galoisiana E sobre o corpo K, a ação do grupo de galois $G(E/K)$ sobre o grupo multiplicativo K^* ou sobre o grupo aditivo K^+, implicará, em ambos os casos, na verificação de que o primeiro grupo de Cohomologia é trivial, isto é, $H^1(G,K^*) = 1$ e $H^1(G,K^+) = 0$ respectivamente.

Abordaremos o estudo das chamadas Extensões de Kummer e mostraremos a bijeção entre as extensões abelianas de um corpo K de característica p e os subgrupos de K^* que contém o grupo $K^{*m} := \{a \in K^* |\ a = b^m,\ \text{para algum}\ b \in K^*\}$. Como hipótese, exigimos que mdc$(m,p) = 1$ e que a m-ésima raiz primitiva da unidade esteja em K. De forma análoga, mostraremos a bijeção entre extensões abelianas de expoente p e subgrupos aditivos de K^+ que contém o grupo $\wp(K^+) := \{a \in K^+ |\ a = b^p - b,\ \text{para algum}\ b \in K^+\}$, como consequência do Teorema de Artin-Schreier.

Na Teoria de Kummer, utilizaremos os dois primeiros grupos de Cohomologia Galoisiana. Outra ferramenta a ser usada é a dualidade de grupos abelianos.

O tema deste projeto pode ser considerado como o começo da Teoria de Corpos de Classes, que pode ser encontrada com detalhes no livro *Class Field Theory* [9], onde as extensões abelianas são analisadas a partir de subgrupos aditivos de K^+ ou multiplicativos de K^*.

Palavras-chave: Dualidade de grupos, Teoria de Galois, Extensão Artin-Schreier, Teorema 90 de Hilbert, Cohomologia Galoisiana, Teoria de Kummer.

ABSTRACT

The subject to be treated in this work is related to Galois theory. We will study the consequences of the fundamental theorem of Galois, and speak about the theorem of Artin-Schreier, which shows whether a field extension E over K of characteristic p, with a length of degree equal to its characteristic, can be written as a simple extension generated by the roots of a polynomial of the type $x^p - x - a$.

Cohomology study of Galois in particular show, as a consequence of Theorem 90 of Hilbert, that given a galois extension E on the field K, the action of galois group $G(E/K)$ over the group multiplicative K^* or the additive group K^+, implies in both cases, the finding that the first cohomology group is trivial, that is, $H^1(G,K^*) = 1$ and $H^1(G,K^+) = 0$ respectively.

We will cover the study of called Kummer extensions and show the bijection between the Abelian extensions of a field K of characteristic p and subgroups of K^* containing the group $K^{*m} := \{a \in K^* |\ a = b^m,$ for some $b \in K^*\}$. As a hypothesis, we require mdc$(m,p) = 1$ and the m-th primitive root of the unit is in K. Similarly, we will show bijection between Abelian extensions of exponent p and additive subgroups of K^+ containing $\wp(K^+) := \{a \in K^+ |\ a = b^p - b,$ for some $b \in K^+\}$, as a consequence of Theorem Artin-Schreier.

In the Kummer Theory, we will use the first two cohomology groups of Galois. Another tool to be used is the duality of Abelian groups.

The theme of this project can be considered as the beginning of Class Field Theory, which can be found in detail in the book *Class Field Theory* [9], where the Abelian extensions are analyzed from additive subgroups of K^+ or multiplicative subgroups of K^*.

Keywords: Duality groups, Galois theory, Artin-Schreier extension, Theorem 90 Hilbert, Galois Cohomology, Kummer theory.

Sumário

INTRODUÇÃO

Este trabalho foi motivado pelo interesse nas consequências da Teoria de Galois e pela curiosidade em verificar as interseções entre Cohomologia de Grupos e a teoria de corpos.

Os resultados principais deste trabalho estão no capítulo 4 e que trazem a classificação de certas extensões abelianas sobre corpos que contém o conjunto das m-ésimas raízes da unidade. Para uma melhor compreensão do texto desse capítulo, inserimos, além de preliminares básicas, que podem ser ignoradas pelo leitor mais experiente, a seção 1.2 que trata de Dualidade de Grupos, as seções 2.6 e 2.8 onde encontra-se o teorema fundamental da teoria de Galois, o teorema 90 de Hilbert e o teorema de Artin-Schreier. Também essencial é o texto exibido no capítulo 3 de Cohomologia Galoisiana sem o qual não conseguiríamos entender a seção 4.2.2.

A teoria de Kummer tem aplicações principalmente na teoria dos números, desenvolvida pelo alemão Ernest Eduard Kummer (1810-1893) e suas consequências serão comentadas ao final desta dissertação.

Com intenção de trazer clareza ao texto, o autor teve o cuidado de detalhar demonstrações e de inserir comentários, observações e exemplos que trazem originalidade a este trabalho e, de fato, o distingue do texto encontrado em qualquer das referências.

Capítulo 1

Grupos

Neste Capítulo apresentaremos resultados da Teoria de Grupos e em seguida resultados da Teoria de Corpos. Tais resultados são essenciais para entender os principais teoremas dos capítulos seguintes.

1.1 Ação de Grupos

Vamos relembrar alguns conceitos básicos.

Uma *permutação* de um conjunto Ω é uma bijeção de Ω em Ω.

Chamamos de *grupo simétrico* de Ω o conjunto formado por todas as suas permutações. Verifica-se a estrutura de grupo tomando a composição como operação. Denotamos o grupo de permutações de Ω por $\mathrm{Sym}(\Omega)$.

Se $\Omega = \{1,...,n\}$, representaremos o conjunto de todas as permutações de Ω por S_n.

Se $g \in \mathrm{Sym}(\Omega)$ e $\alpha \in \Omega$ denotaremos por $g\alpha$ a imagem de α via a permutação g. Sendo assim, a composição gh, das permutações g e h, significa aplicar primeiro a permutação h e depois a permutação g.

Chamamos *ação à esquerda* de G em Ω uma aplicação de $G \times \Omega$ em Ω, tal que $(g, \alpha) \mapsto$

$g\alpha$, que satisfaz as seguintes condições:

a) $1\alpha = \alpha$, para todo $\alpha \in \Omega$, onde 1 é o elemento neutro da operação em G.

b) $g(h\alpha) = (gh)\alpha$ para todo $\alpha \in \Omega$ e para todos g, $h \in G$.

Dizemos que G *age* em Ω, caso exista uma ação de G em Ω.

Exemplo 1.1.1. *Considere a aplicação Sym(Ω)$\times$ $\Omega \to \Omega$, com $(g, \alpha) \mapsto g\alpha$. É fácil de verificar que esta aplicação define uma ação de Sym(Ω) em Ω.*

De maneira análoga a que definimos ação à esquerda, podemos definir *ação à direita*. Entretando usaremos regularmente a ação à esquerda, a não ser que seja dito o contrário.

A partir de uma ação de G em Ω e um elemento $\alpha \in \Omega$ podemos definir o conjunto $G\alpha = \{g\alpha \mid g \in G\}$ que é chamado *órbita* de α em Ω e o conjunto $G_\alpha = \{g \in G \mid g\alpha = \alpha\}$ chamado *estabilizador* de α ou *grupo de isotropia* de α.

Os elementos de uma mesma órbita são equivalentes, isto é, a órbita de um elemento α é uma classe de equivalência com a seguinte relação: $x \sim y$ então $\exists\ g \in G$ tal que $x = gy$. Observe que, se $x = h\alpha$ e $y = g\alpha$, para g e h em G então $x = ny$ com $n = h \circ g^{-1} \in G$. Assim, as diferentes órbitas formam uma partição disjunta para o conjunto Ω.

Podemos observar também que o estabilizador G_α, como definimos, é um subgrupo de G. Podemos generalizar essa definição da seguinte maneira: dado um subconjunto S de Ω, chamamos de *estabilizador pontual* de S ao conjunto $G_S = \bigcap\limits_{\alpha \in S} G_\alpha = \{g \in G \mid g\alpha = \alpha \text{ para todo } \alpha \in S\}$.

Vamos apresentar agora o principal resultado que envolve ações de grupos. Uma demonstração para esse resultado pode ser verificada em [5].

Teorema 1.1.2. *Seja G um grupo agindo em Ω. Então se verificam:*

i) Dados α, $\beta \in \Omega$ e $g \in G$ tais que $\beta = g\alpha$, então $G_\beta = g^{-1}G_\alpha g$.

ii) Para qualquer $\alpha \in \Omega$ temos $|G\alpha| = |G : G_\alpha|$. Em particular, se G for finito, temos $|G| = |G\alpha|\,|G_\alpha|$.

Seja G um grupo agindo em Ω, dizemos que G é *transitivo*, ou que a ação de G em Ω é *transitiva*, se existir uma única órbita.

Temos diretamente da definição que G é transitivo se somente se, dados quaisquer α, $\beta \in \Omega$, existe $g \in G$ tal que $\alpha = g\beta$ ou se somente se $G\alpha = \Omega$, para qualquer $\alpha \in \Omega$. Além disso, se G for finito e transitivo o item ii) do teorema 1.1.2 implica que $|\Omega| = |G : G_\alpha|$ para qualquer $\alpha \in \Omega$.

Dizemos que G *age trivialmente em* Ω se dado $\alpha \in \Omega$, temos $g\alpha = \alpha \; \forall \; g \in G$.

Dado um grupo G fixemos um subgrupo H e denotamos por Γ_H o conjunto de todas as classes laterais a direita. Então podemos fazer agir G, à direita, no conjunto Γ_H definindo a aplicação $\rho_H : \Gamma_H \times G \to \Gamma_H$ por $(Ha,g) \mapsto Hag$. Esta é de fato uma ação de G em Γ_H e é chamada *multiplicação à direita.*

Por outro lado, seja $K = N_G(H)$, então desde que $H \leq K \leq G$, K também age em Γ_H por multiplicação à direita. Embora esta ação possa dar-nos alguma informação temos interesse em definir uma outra ação de K em Γ_H. Sendo assim, definamos a aplicação $\lambda_H : \Gamma_H \times K \to \Gamma_H$ por $(Ha,x) \mapsto x^{-1}(Ha) = Hx^{-1}a$. Dita aplicação é uma ação e é chamada *multiplicação à esquerda.*

Observação 1.1.3. *O fato de existir uma ação de G em Ω é equivalente ao fato de existir um homomorfismo $\psi : G \to Sym(\Omega)$. De fato, dada uma ação de G em Ω, $(g, \alpha) \mapsto g\alpha$, podemos definir $\psi : G \to Sym(\Omega)$ por $g \mapsto \psi(g)$, onde $\psi(g)$ é uma permutação que leva cada elemento $\alpha \in \Omega$ em $g\alpha$. Como $(g,\alpha) \mapsto g\alpha$ é uma ação segue que ψ é um homomorfismo.*
Reciprocamente, dado um homomorfismo $\psi : G \to Sym(\Omega)$ podemos definir a aplicação $(g, \alpha) \mapsto \psi(g)\alpha$. Assim as propriedades de ação são verificadas, pois ψ é um homomorfismo.

Desta forma, podemos ver as ações de G e K em Γ_H, como homomorfismos $\rho_H : G \to$

$\mathrm{Sym}(\Gamma_H)$ e $\lambda_H : K \to \mathrm{Sym}(\Gamma_H)$.

1.2 Dualidade de Grupos

Seja G um grupo, dizemos que G tem expoente m, $m \in \mathbb{N}$ se $\forall\ \phi \in G, \phi^m = 1$.

Seja G um grupo, e tomando um m tal que G tenha expoente m, podemos definir o *Grupo Dual* de G, denotado por $G^\wedge$, como o grupo formado pelos homomorfismos de G em $\mathbb{Z}_m$, isto é $G^\wedge = \mathrm{Hom}(G,\mathbb{Z}_m)$. Esse é um grupo com a operação adição, ou seja, dados quaisquer γ e δ em $G^\wedge$ e $g \in G$, vale que $(\gamma + \delta)(g) = \gamma(g) + \delta(g)$.

Dados dois grupos abelianos A e B, ambos de expoente m, seja $f : A \to B$ um homomorfismo de grupos, então f induz um homomorfismo $f^\wedge : B^\wedge \to A^\wedge$, da seguinte maneira:

$$f^\wedge(\sigma) = \sigma \circ f.$$

Se σ, $\tau \in B^\wedge$, $f^\wedge(\sigma + \tau) = (\sigma + \tau) \circ f = \sigma \circ f + \tau \circ f = f^\wedge(\sigma) + f^\wedge(\tau)$, o que mostra que $f^\wedge$ de fato é um homorfismo. Podemos assim observar algumas propriedades:

- $\mathrm{Id}^\wedge = \mathrm{Id}$; e,
- $(f \circ g)^\wedge = g^\wedge \circ f^\wedge$

Vamos mostrar a segunda propriedade acima:

$(f \circ g)^\wedge(\sigma) = \sigma \circ (f \circ g) = (\sigma \circ f) \circ g = (f^\wedge(\sigma)) \circ g$.

Vale observar que $f^\wedge(\sigma)$ é uma aplicação de A em $\mathbb{Z}_m$ e, portanto, $f^\wedge(\sigma) \circ g : B \to \mathbb{Z}_m \ \in B^\wedge$.

Por outro lado, $(g^\wedge \circ f^\wedge)(\sigma) = g^\wedge(f^\wedge(\sigma)) = (f^\wedge(\sigma)) \circ g$.

Teorema 1.2.1. *Se A é um grupo abeliano, finito e de expoente m tal que $A = B \times C$,* *então* $A^\wedge$ *é isomorfo a* $B^\wedge \times C^\wedge$. *Portanto, se* A *é um grupo abeliano, finito e de expoente* m, *temos* $A \cong A^\wedge$.

Demonstração. De fato, seja a aplicação

$$\begin{array}{rccccc} \varphi: & B^\wedge \times C^\wedge & \to & (B \times C)^\wedge & & \\ & (f^\wedge, g^\wedge) & \mapsto & \psi: & B \times C & \to & \mathbb{Z}_m \\ & & & & (x,y) & \mapsto & f^\wedge(x) + g^\wedge(y). \end{array}$$

A aplicação φ é homomorfismo:

$(f_1^\wedge, g_1^\wedge) + (f_2^\wedge, g_2^\wedge) = (f_1^\wedge + f_2^\wedge, g_1^\wedge + g_2^\wedge)$

e $\phi(f_1^\wedge + f_2^\wedge, g_1^\wedge + g_2^\wedge) = \psi$, tal que $\psi(x,y) = (f_1^\wedge + f_2^\wedge)(x) + (g_1^\wedge + g_2^\wedge)(y) = f_1^\wedge(x) + g_1^\wedge(x) + f_2^\wedge(x) + g_2^\wedge(y) = \psi_1 + \psi_2$, onde $\psi_1 = \varphi(f_1^\wedge, g_1^\wedge)$ e $\psi_2 = \varphi(f_2^\wedge, g_2^\wedge))$.

Seja agora

$$\begin{array}{rccc} \xi: & (B \times C)^\wedge & \to & B^\wedge \times C^\wedge \\ & \psi & \mapsto & (\psi_1, \psi_2) \end{array}$$

tal que $\psi_1(x) = \psi(x,0)$ e $\psi_2(y) = \psi(0,y)$, para $(x,y) \in B \times C$. Observe que $\psi(x,y) = \psi((x,0) + (0,y)) = \psi(x,0) + \psi(0,y) = \psi_1(x) + \psi_2(y)$.

ξ é homomorfismo, pois

$\xi(\psi + \sigma) = ((\psi + \sigma)_1, (\psi + \sigma)_2)$

$(\psi + \sigma)_1(x) = (\psi + \sigma)(x,0) = \psi(x,0) + \sigma(x,0) = \psi_1(x) + \sigma_1(x)$ e

$(\psi + \sigma)_2(y) = (\psi + \sigma)(0,y) = \psi(0,y) + \sigma(0,y) = \psi_2(y) + \sigma_2(y)$.

Como $(\psi_1+\sigma_1,\psi_2+\sigma_2) = (\psi_1,\psi_2)+(\sigma_1,\sigma_2) = \xi(\psi)+\xi(\sigma)$, temos $\xi(\psi+\sigma) = \xi(\psi)+\xi(\sigma)$.

Para concluir que $B^\wedge \times C^\wedge \cong (B \times C)^\wedge$, basta observar que $\varphi = \xi^{-1}$.

De fato, $\varphi \circ \xi(\psi) = \varphi(\xi(\psi)) = \varphi(\psi_1,\psi_2) = \theta$ onde $\theta(x,y) = \psi_1(x) + \psi_2(y) = \psi(x,y)$ isso implica que $\varphi \circ \xi = \mathrm{Id}$.

Por outro lado, $\xi \circ \varphi : B^\wedge \times C^\wedge \to B^\wedge \times C^\wedge$ e vale $\xi \circ \varphi(f^\wedge, g^\wedge) = \xi(\psi) = (\psi_1,\psi_2)$ onde $\psi_1(x) = \psi(x,0) = f^\wedge(x) + g^\wedge(0) = f^\wedge(x)$ e $\psi_2(x) = \psi(0,y) = f^\wedge(0) + g^\wedge(y) = g^\wedge(y)$ isto é, $(\psi_1, \psi_2) = (f^\wedge, g^\wedge)$ e assim $\xi \circ \varphi = \mathrm{Id}$.
Logo φ é isomorfismo.

Vamos mostrar agora que $A \cong A^\wedge$.

De fato, A é finito e abeliano e portanto A é isomorfo ao produto de grupos cíclicos (ver [10], página 226). Então, basta fazer a demonstração para o caso em que A é cíclico.

Veja que $\forall\ a \in A$ temos $m.a = 0$, pois A tem expoente m e $\forall\ a \in A\ n.A = 0$ onde n é a ordem de A. Ou seja, $m = k.n$, $k \in \{1, 2, 3, ...\}$, isto é $n \mid m$.

Agora $\mathbb{Z}_m$ contém um único subgrupo de ordem n, que é cíclico (ver [10], página 70). Seja B esse subgrupo, então $B \cong \mathbb{Z}_n$. Observe que, $\forall\ \psi \in A^\wedge$, $\psi(a)$ tem expoente n, onde a é um elemento qualquer de A, pois ψ é homomorfismo e A tem ordem n. Temos assim, que $\psi(A) \subseteq B \subseteq \mathbb{Z}_m$.

Seja y tal que $\mathbb{Z}_n = \langle y \rangle$ e $\psi_1 : A \to \mathbb{Z}_n$ com $\psi_1(x) = y$ um isomorfismo.

Tome $\lambda \in \{0,1,...,n-1\}$ e considere os homomorfismos $\lambda\psi_1$, isto é $\lambda\psi_1(x) = \psi_1(\lambda x)$.

O conjunto $\{0,\psi_1,2\psi_1, ..., (n-1)\psi_1\}$ é um subconjunto cíclico de $A^\wedge$.

Já que, para $\psi \in A^\wedge$, $\psi : A \to \mathbb{Z}_m$ e A é cíclico gerado por x, ψ é unicamente determinado por $\psi(x)$, ou seja, é determinado pelo elemento onde ψ leva x. O que implica que ψ é um dos $\lambda\psi_1$, ou seja, $A^\wedge = \{0,\psi_1, 2\psi_1, ..., (n-1)\psi_1\}$ que é cíclico de ordem n, gerado por ψ_1.

Concluímos portanto que $A^\wedge \cong A$.

■

Sejam A, A' dois grupos abelianos. Uma *aplicação bilinear* de $A \times A'$ em um grupo C é uma aplicação:

$$A \times A' \to C$$

$$(x,x') \mapsto \langle x, x' \rangle$$

tal que, para cada $x \in A$, a função $x' \mapsto \langle x, x' \rangle$ é um homomorfismo e $x \mapsto \langle x, x' \rangle$ também é um homomorfismo.

Tal aplicação bilinear é também chamada de **emparelhamento**.

Um elemento $x \in A$ é chamado de **ortogonal** (com respeito a $\langle\ ,\ \rangle$) a um subconjunto S' de A' se $\langle x, x' \rangle = 0\ \forall\ x' \in S'$, onde 0 é o elemento neutro da operação em C. O conjunto S de elementos ortogonais à S' formam obviamente um subgrupo de A. Similarmente formamos subconjuntos de A' ortogonais à subconjuntos de A.

Chamamos de **núcleo à esquerda** ao subconjunto de A formado por todos os elementos ortogonais à A'. De forma similar definimos **núcleo à direita**.

Seja $A \times A' \to C$ um emparelhamento e sejam B e B' os núcleos à esquerda e à direita. Um elemento $x' \in A'$ induz um homomorfismo $\psi_{x'}$ de A em C dado por $x \mapsto \langle x, x' \rangle$. Nesse homomorfismo, $\psi_{x'}(B) = 0$.

Além disso, $\psi_{x'} = \psi_{y'}$ se somente se $x' \equiv y' \pmod{B'}$. De fato, $\psi_{x'} = \psi_{y'} \Leftrightarrow \langle x, x' \rangle = \langle x, y' \rangle\ \forall\ x \in A \Leftrightarrow \langle x, x' - y' \rangle = 0\ \forall\ x \in A \Leftrightarrow x' - y' \in B'$.

Portanto,

$$\begin{array}{rccc} \psi' : & A'/B' & \to & \mathrm{Hom}(A/B, C) \\ & x' & \mapsto & \psi_{x'} \end{array}$$

é um homomorfismo injetivo.

O mesmo vale para

$$\begin{array}{rccc} \psi : & A/B & \to & \mathrm{Hom}(A'/B', C) \\ & x & \mapsto & \psi_{x} \end{array}.$$

Logo, se $C \cong \mathbb{Z}_m$, $m\psi_{x'} = \psi_{mx'} = 0$, isto é, A/B tem expoente m. Similarmente mostramos que A'/B' tem expoente m.

Teorema 1.2.2 (Teorema de Dualidade)**.** *Seja $A \times A' \to C$ um emparelhamento de dois grupos abelianos em um grupo cíclico de ordem m. Sejam ainda B e B' os núcleos à esquerda e à direita respectivamente. Assuma que A'/B' é finito. Então A/B é finito, e A'/B' é isomorfo ao grupo dual de A/B.*

Demonstração. Como vimos acima, $\psi' : A/B \to \mathrm{Hom}(A'/B',C)$ é homomorfismo injetivo. Vimos também que A'/B' tem expoente m. Pelo Teorema 1.2.1, $A'/B' \cong (A'/B')^{\wedge}$ e portanto

$$|A/B| \leq |(A'/B')^{\wedge}| = |\mathrm{Hom}(A'/B', C)| = |A'/B'|.$$

Por outro lado, como A/B é finito, também tem expoente m e $\psi : A'/B' \to \mathrm{Hom}(A/B, C)$ é homomorfismo injetivo, temos

$$|A'/B'| \leq |(A/B)^{\wedge}| = |\mathrm{Hom}(A/B, C)| = |A/B|.$$

Logo $|A'/B'| = |A/B|$ e mais ainda, ψ e ψ' são bijeções.

Assim, $A'/B' \cong (A/B)^{\wedge}$.

■

Corolário 1.2.3. *Seja A um grupo abeliano finito, B um subgrupo, $A^{\wedge}$ o grupo dual de A e $B^{\perp}$ o conjunto de elementos de $A^{\wedge}$ tais que, restritos a B são identicamente nulos (isto é $B^{\perp} = \{\varphi \in A^{\wedge} \mid \varphi(B) = 0\}$). Então existe um isomorfismo de $A^{\wedge}/B^{\perp}$ em $B^{\wedge}$.*

Demonstração. Basta tomar o emparelhamento $A^{\wedge} \times B \to \mathbb{Z}_m$, tal que $(\psi,\, b) \mapsto \psi(b)$, com m expoente de A e de $A^{\wedge}$, então $B^{\perp}$ é o núcleo à esquerda e $\{0\}$ é o núcleo à direita. Daí é só aplicar o Teorema acima para concluirmos que $A^{\wedge}/B^{\perp}$ é isomorfo a $(B/\{0\})^{\wedge} = B^{\wedge}$. ■

Capítulo 2

Corpos

2.1 Extensão de Corpos

Um corpo E é chamado de *extensão* de um corpo K sempre que $E \supseteq K$, isto é, se K for um subcorpo de E.

Observe que podemos enxergar E como um espaço vetorial sobre K e assim, se E tem dimensão finita - como espaço vetorial -, dizemos que E é uma extensão finita de K, se E tem dimensão infinita, dizemos que E é uma extensão infinita sobre K.

Denotamos por $[E : K]$ o *grau* da extensão E sobre K, que corresponde à dimensão do espaço vetorial E sobre K. O grau de uma extensão pode ser finito ou infinito.

Uma extensão E sobre K pode ser algébrica ou transcendente. Dizemos que E é uma *extensão algébrica* se $\forall\ \alpha \in E$, $f(\alpha) = 0$ para algum $f(x) \in K[x]$ (anel de polinômios), não nulo, nesse caso α é algébrico sobre K. Se, para algum $\alpha \in E$, $\nexists\ f(x) \in K[x]$, não nulo, tal que $f(\alpha) = 0$ então α é transcendente e a extensão E é *transcendente* .

Usamos também a notação $K(\alpha_1, \alpha_2, ..., \alpha_n)$, com $\alpha_i \in E$, $i \in \{1, \cdots, n\}$, K subcorpo de E, para denotar o menor corpo que contém o corpo K e os elementos $\alpha_1, \alpha_2, ..., \alpha_n$. Então $K(\alpha_1, \alpha_2, ..., \alpha_n)$ é uma extensão de K, uma extensão construída dessa forma é chamada de *Extensão Finitamente Gerada* e os elementos $\alpha_1, \alpha_2, ..., \alpha_n$ são chamados de *geradores*.

Dizemos também que uma extensão E sobre K é *simples* se $\exists\ \alpha \in E$ tal que $E = K(\alpha)$.

Exemplo 2.1.1. *Temos que $\mathbb{R} \subset \mathbb{C}$, $\mathbb{C}$ é extensão de $\mathbb{R}$. Como $\mathbb{C} = \mathbb{R}[i]$ e i é algébrico sobre $\mathbb{R}$, pois $f(x) = x^2 + 1 \ \in \ \mathbb{R}[x]$ e $f(i) = 0$, então $\mathbb{C}$ é uma extensão algébrica e simples.*

O corpo $\mathbb{C}$ tem grau 2 sobre $\mathbb{R}$, logo $[\mathbb{C} : \mathbb{R}] = 2$. Isso segue do fato de $\{1,i\}$ ser uma base para $\mathbb{C}$ sobre $\mathbb{R}$. De fato, todo numero complexo é da forma $a + bi$, ou seja, $\{1,i\}$ gera $\mathbb{C}$. Além disso, $a + bi = 0$, então $a = b = 0$, que mostra que $\{1,i\}$ é L.I..

Observação 2.1.2. *Observe que $\forall\ a + bi \in \mathbb{C}$, $f(x) \ = \ x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$ é um polinômio tal que $f(a + bi) = 0$.*

Exemplo 2.1.3. *$\mathbb{R}$ é extensão transcendente sobre $\mathbb{Q}$, pois $\pi \in \mathbb{R}$ é transcendente (ver [13]).*

Sendo α transcendente sobre um corpo K, a extensão $K(\alpha)$ será infinita. De fato, a base de $K(\alpha)$ deve conter α e todas as suas potências, logo $K(\alpha)$ é extensão infinita sobre K. Veremos, ainda neste capítulo, teorema que destaca o fato de $K(\alpha)$ ser isomorfo a $K(x)$ (corpo quociente do anel de polinômios), toda vez que α é transcendente.

Proposição 2.1.4. *Seja E uma extensão $finita$ sobre um corpo K, então E é uma extensão algébrica sobre K.*

Para provar a proposição acima, basta verificar que dado um elemento $\alpha \ \in \ E$, os elementos $1, \alpha, \alpha^2, \cdots, \alpha^n$, não podem ser linearmente independentes para todo número natural n, caso contrário, E não seria extensão finita. Desta forma, facilmente construímos um polinômio $f(x) \ \in \ K[x]$ tal que $f(\alpha) = 0$, ou seja, α é algébrico.

Definição 2.1.5. *O* polinômio minimal *de um elemento algébrico α, $\alpha \in E$, onde E é uma extensão sobre o corpo K, é o polinômio mônico irredutível $f(x) \in K[x]$ de menor grau tal que $f(\alpha) = 0$.*

Devemos ressaltar que o polinômio minimal é único (ver [10] página 377).

Teorema 2.1.6. *Sejam E,F e K três corpos tais que $K \subset F \subset E$, F extensão finita sobre K e E extensão finita sobre F, então*

$$[E : K] = [E : F][F : K].$$

A demonstração do teorema acima pode ser verificada em [1] na página 224.

Demonstraremos mais adiante que o grau de uma extensão algébrica finita sobre um corpo K é igual ao grau do polinômio minimal dos elementos algébricos adjuntados (polinômio mônico de menor grau que possui esses elementos como raízes).

Um *homomorfismo de corpos* é um homomorfismo de anéis. Como o núcleo de um homomorfismo de anéis é um ideal, e ideal de um corpo ou é nulo ou é todo o corpo, um homomorfismo de corpos ou é injetivo ou é identicamente nulo.

Teorema 2.1.7. *Seja $\varphi : K[x] \to E$, onde E é extensão sobre o corpo K, e tal que $\varphi(f(x)) = f(\alpha)$, com $\alpha \in E$, então φ é um homomorfismo e, além disso, vale que:*

i) $\mathrm{Im}\ \varphi = K[\alpha]$, *onde* $K[\alpha] := \{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha^1 + a_0 \mid a_i \in K\ \forall\ i = 1, \cdots, n,\ \text{com}\ n \in \mathbb{N}\}$ *anel.*

ii) *Se α é transcendente sobre K, então* $\ker \varphi = \{0\}$.

iii) *Se α é algébrico sobre K e $f(x)$ é o polinômio minimal de α, então* $\ker \varphi = K[x] \cdot f(x)$ *é um ideal maximal de $K[x]$.*

iv) $K[x]/\ker \varphi$ *(anel quociente)* $\cong K[\alpha]$.

Assim, o corpo quociente $K(\alpha) \cong K[\alpha]$ para α algébrico e, para α transcendente, $K[x] \cong K[\alpha]$, isto é, $K(x) \cong K(\alpha)$. O teorema acima pode ser demonstrado a partir do 1° teorema de homomorfismo de anéis.

Como consequência do Teorema 2.1.7 podemos verificar o seguinte corolário:

Corolário 2.1.8. *Sejam* α *e* $\beta \in L \supset K$ *dois elementos algébricos sobre* K *com o mesmo polinômio minimal. Então* $K(\alpha)$ *e* $K(\beta)$ *são isomorfos.*

Proposição 2.1.9. *Seja* n *o grau do polinômio minimal de* $\alpha \in E \supset K$*, com* E *extensão de corpos sobre* K*, então tomando* $f(x) \in K[x]$*,* $f(\alpha)$ *é expresso de modo único na forma*

$$f(\alpha) = a_0 + a_1\alpha^1 + \ldots + a_{n-1}\alpha^{n-1}$$

com $a_i \in K \ \forall \ i \in \{0,1,2,...,n-1\}$.

A partir da proposição acima, observemos que $\forall \ f \in K(\alpha)$, $f \ = a_0 + a_1\alpha^1 + \ldots + a_{n-1}\alpha^{n-1}$ desde que n seja o grau do polinômio minimal de α, assim $n = [K(\alpha) : K]$, pois podemos considerar o conjunto $\{1,\alpha^1, \ldots ,\alpha^{n-1}\}$ linearmente independente como base de $K(\alpha)$, onde 1 é a unidade de K.

Exemplo 2.1.10. *Sejam* $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ *e* $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$*. Os polinômios* $f(x) = x^2 - 2$ *e* $g(x) = x^4 - 2$ *são os polinômios minimais de* $\sqrt{2}$ *e* $\sqrt[4]{2}$ *respectivamente e temos que:*

- $\forall \ k_1 \in \mathbb{Q}(\sqrt{2})$, $k_1 = a_0 + a_1\sqrt{2}$ *com* $a_i \in \mathbb{Q}$, $i \in \{0,1\}$.
- $\forall \ k_2 \in \mathbb{Q}(\sqrt[4]{2})$, $k_2 = b_0 + b_1\sqrt[4]{2} + b_2(\sqrt[4]{2})^2 + b_3(\sqrt[4]{2})^3$ *com* $b_j \in \mathbb{Q}$, $j \in \{0,1,2,3\}$.

Isto é $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$*. Note que* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ *e* $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$*. Então* $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$.

Exemplo 2.1.11. *O elemento* $\alpha = \sqrt[3]{2}$ *é algébrico sobre* $\mathbb{Q}$*.*

$\mathbb{Q}[\sqrt[3]{2}]$ *é corpo e* $f(x) = x^3 - 2$ *é o polinômio minimal de* $\sqrt[3]{2}$*. Mas*

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

também tem $f(x)$ *como polinômio minimal,* $\mathbb{Q}[\beta]$ *é corpo. Temos então* $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, $[\mathbb{Q}[\beta] : \mathbb{Q}] = 3$ *e* $\mathbb{Q}[\alpha] \cong \mathbb{Q}[\beta]$.

Exemplo 2.1.12. *Seja p primo e $\alpha_j = \sqrt[2^j]{p} \in \mathbb{R}$. Então $f(x) = x^{2^j} - p \in \mathbb{Q}[x]$ é o polinômio minimal de α_j, $\forall\ j \in \mathbb{N}$.*

Como α_j é algébrico, $\mathbb{Q}[\alpha_j]$ é corpo, $[\mathbb{Q}[\alpha_j] : \mathbb{Q}] = 2^j$, $\mathbb{Q} \subset \mathbb{Q}[\alpha_j] \subset \mathbb{R}$ e ainda

$$\mathbb{Q} \subset \mathbb{Q}[\alpha_1] \subset \mathbb{Q}[\alpha_2] \subset \mathbb{Q}[\alpha_3] \subset \ldots \subset \mathbb{R}.$$

Verificamos que $\mathbb{R}$ é uma extensão infinita sobre $\mathbb{Q}$.

Definição 2.1.13. *Dado um corpo K, se $\forall\ f(x) \in K[x]$ de grau ≥ 1 possui raiz em K, então dizemos que K é* algebricamente fechado*.*

Vamos lembrar aqui da definição de característica de um corpo.

Definição 2.1.14. *A* característica *de um corpo K é o menor número inteiro positivo p tal que $p.a = 0\ \forall a \in K$. Se tal número não existe, dizemos que K tem característica zero.*

Observe que a característica de um corpo K ou é zero ou é um número p primo. De fato, suponha que a característica seja n composto. Então $n = s.t$, com s e t inteiros positivos menores que n, e $n.1 = 0$. Isso implica que $s.t.1 = (s.1).(t.1) = 0$, e portanto $s.1 = 0$ ou $t.1 = 0$, ou seja, $s.a = 0$ ou $t.a = 0\ \forall a \in K$. Contrariando o fato de n ser característica.

Proposição 2.1.15. *Seja K um corpo de característica zero. Então as afirmações seguintes são equivalentes:*

i) *K é um corpo algebricamente fechado.*

ii) *Todo polinômio $f(x) \in K[x]$ se decompõe num produto de fatores lineares.*

iii) *Se $f(x) \in K[x]$ é irredutível, então $f(x)$ tem grau 1.*

iv) *Não existem extensões algébricas próprias de K.*

Essa proprosição pode ser facilmente verificada.

Para todo $f(x) \in K[x]$, $f(x) = c(x-\alpha_1)^{m_1} \cdot \ldots \cdot (x-\alpha_r)^{m_r}$ tal que r, $m_i \in \mathbb{N}$, $\alpha_i \neq \alpha_j$ $\forall\ i \neq j$, com $i, j \in \{1, \ldots ,r\}$ e $c \in K$. Chamamos de m_i a *multiplicidade da raiz* α_i e, se $m_i = 1$, α_i é chamada de *raiz simples* de $f(x)$.

No Capítulo 2.3 veremos mais detalhes e resultados que envolvem polinômios que se decompõe em fatores lineares bem como os corpos onde esses polinômios se decompõe.

Proposição 2.1.16. *Seja K um corpo de característica zero. Se $f(x) \in K[x]$ é um polinômio irredutível sobre K, então $f(x)$ possui apenas raízes simples.*

Nas proposições 2.1.15 e 2.1.16, a hipótese de K ser corpo de característica zero é essencial, verifique o exemplo abaixo.

Exemplo 2.1.17. *Seja $K = \mathbb{F}_p(y)$ corpo de frações de $\mathbb{F}_p[y]$, onde $\mathbb{F}_p$ denota o corpo formado pelo quociente $\mathbb{Z}/p\mathbb{Z}$. Temos que K tem característica p e seja $\beta = \sqrt[p]{\alpha}$ tal que $\alpha \in K$, mas $\beta \notin K$ (tome por exemplo $\alpha = y$). O polinômio $f(x) = x^p - \alpha \in K[x]$, é minimal de β. Agora considere a extensão $L = K(\beta)$ e tome o polinômio $l(x) = x^p - \beta^p = x^p - \alpha \in L[x]$. Observe que apesar de $f(x)$ ser irredutível em $K[x]$, β é raiz de multiplicidade p em $L[x]$.*

Definição 2.1.18. *Seja E uma extensão do corpo K. Dizemos que E é um* corpo de fatoração *ou* corpo de decomposição *de um polinômio $f(x) \in K[x]$ sobre K se E é o menor corpo que contém todas as raízes de $f(x)$.*

Exemplo 2.1.19. *O corpo $\mathbb{C}$ é algebricamente fechado e $\mathbb{C} = \mathbb{R}[i]$ é corpo de decomposição de $x^2 + 1 \in \mathbb{R}[x]$.*

Exemplo 2.1.20. *Se $f(x) \in \mathbb{Q}[x]$, $f(x) = x^3 - 2$, então $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$ e $\bar{\beta}$ são as raízes de $f(x)$.*

Observe que $\mathbb{Q}[\beta] \ni \bar{\beta}$, mas $\sqrt[3]{2} \notin \mathbb{Q}[\bar{\beta}]$, então $\mathbb{Q}[\sqrt[3]{2}, \beta]$ é corpo de decomposição de $f(x) = x^3 - 2$ sobre $\mathbb{Q}$.

De forma mais geral, podemos mostrar que se $f(x) = x^n - 2 \in \mathbb{Q}[x]$, $\alpha = \sqrt[n]{2}$, $u = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, $\beta = \alpha u$, *então* $\mathbb{Q}[\alpha,u] = \mathbb{Q}[\alpha,\beta]$ *é corpo de decomposição de* $f(x) = x^n - 2$ *sobre* $\mathbb{Q}$.

Como sabemos, $\mathbb{R}[x]/\langle x^2+1\rangle$ é corpo que contém as raízes de $f(x) = x^2+1 \in \mathbb{R}[x]$ e contém $\mathbb{R}$, isto é, extensão de $\mathbb{R}$. Apresentamos agora uma importante generalização de tal fato.

O Teorema abaixo é também conhecido como o Teorema Fundamental da Teoria de Corpos.

Teorema 2.1.21 (Kronecker)**.** *Seja* K *um corpo e* $f(x)$ *um polinômio não constante de* $K[x]$*. Então existe uma extensão* E *do corpo* K *que contém uma raiz de* $f(x)$*.*

Omitiremos aqui a demonstração do Teorema acima, mas é possível vê-la de forma bem clara em [10] na página 377. Entretanto, vale ressaltar que a extensão E procurada é exatamente $K[x]/\langle f_i(x)\rangle$, com $f_i(x)$ um fator irredutível de $f(x)$. Sempre podemos tomar $f_i(x)$ pois $K[x]$ é domínio de fatoração única. Então a raiz de $f(x)$ em E é raiz de $f_i(x)$.

Teorema 2.1.22. *Seja* K *um corpo e* $f(x)$ *um polinômio não constante de* $K[x]$*. Então existe um corpo de decomposição* E *de* $f(x)$ *sobre* K*.*

A demonstração é como no teorema acima.

Abaixo seguem Teorema e Corolário cujas demonstrações são encontradas na referência [1] na página 231.

Teorema 2.1.23. *Seja* K *um corpo. Existe uma extensão algebricamente fechada de* K*.*

Corolário 2.1.24. *Dado um corpo* K*, existe uma extensão algébrica* L *sobre* K *que é algebricamente fechada.*

Definição 2.1.25. *A extensão algébrica E de um corpo K que contém as raízes de todos os polinômios com coeficientes em K é chamada de* fecho algébrico *de K.*

Definição 2.1.26. Extensão Normal *de um corpo K é uma extensão algébrica E tal que todo polinômio irredutível em $K[x]$ que possui uma raiz em E pode ser decomposto em $E[x]$ em termos lineares, ou, equivalentemente, para todo elemento de E, todas raízes de seu polinômio minimal estarão em E.*

Exemplo 2.1.27. *Tome $\mathbb{C}$, extensão de corpo que contém $\mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$. Tomamos 1, a unidade em $\mathbb{R}$, e $\{1,i\}$ a base de $\mathbb{C}$, $i \in \mathbb{C}$ e $i \notin \mathbb{R}$. Seja $f(x)$ irredutível em $\mathbb{R}[x]$ com raiz em $\mathbb{C}$, e seja $a + bi$, $a,b \in \mathbb{R}$, essa raiz. Agora, seja $g(x)$ o polinômio minimal de $a + bi$ sobre $\mathbb{R}$, então $g(x)$ tem grau 2, caso contrário, $[\mathbb{C} : \mathbb{R}] \neq 2$ e $f(x)$ é múltiplo de $g(x)$. Como $f(x)$ é irredutível, $f(x) = g(x) \cdot \lambda$ com $\lambda \in \mathbb{R}$. Concluímos que, assim como $g(x)$ tem as raízes em $\mathbb{C}$ (se $a+bi$ é raiz de $g(x)$, $a - bi \in \mathbb{C}$ é a outra raiz), $f(x)$ também o tem. Logo $f(x)$ pode ser decomposto em termos lineares em $\mathbb{C}[x]$.*

Exemplo 2.1.28. $\mathbb{Q}[\sqrt[3]{3}]$ *é extensão de $\mathbb{Q}$, $\sqrt[3]{3}$ é algébrico sobre $\mathbb{Q}$ e $f(x) = x^3 - 3$ é o seu polinômio minimal. Mas $\mathbb{Q}[\sqrt[3]{3}]$ não possui as raízes complexas de $f(x) \in \mathbb{Q}[x]$. Assim, $f(x)$ não pode ser decomposto em fatores lineares em $\mathbb{Q}[\sqrt[3]{3}][x]$.*

Observe que numa extensão normal E de K, se algum polinômio $f(x) \in K[x]$ irredutível tem alguma raiz em E, então todas as suas raízes estão em E.

2.2 Corpos Finitos

Quando falamos sobre a característica de um corpo, dizemos que este corpo possui uma cópia de $\mathbb{Q}$ (característica zero) ou uma cópia de $\mathbb{F}_p$ para algum p primo (característica p).

Para verificar a afirmação acima tome um corpo F e o homomorfismo $\phi : \mathbb{Z} \to F$ que leva 1 de Z em 1_F (unidade no corpo F). Temos que $n \in \mathbb{Z}$ positivo é levado em $1_F + 1_F + ... + 1_F$, com n parcelas. Quando o núcleo de ϕ é zero, $\forall\ n \in \mathbb{Z}$, $n \neq 0$, a imagem $n.1_F$ é diferente de zero, e portanto podemos tomar o homomorfimo injetivo $\mathbb{Q} \hookrightarrow F$, tal que $m/n \mapsto (m.1_F).(n.1_F)^{-1}$, onde m/n é irredutível. Logo F tem uma cópia de $\mathbb{Q}$.

Por outro lado, se o núcleo de ϕ for diferente de zero, como núcleo de homomorfismo é um ideal e o domínio deste homomorfismo é $\mathbb{Z}$, o núcleo será um ideal principal. É fácil verificar também que esse ideal é primo, portanto gerado por p, um número primo, isto é, é do tipo $p\mathbb{Z}$. Desta forma, pelo primeiro teorema de homomorfismo de anéis, $\mathbb{Z}/p\mathbb{Z} \simeq \text{Im } \phi$ e portanto F tem uma cópia de $\mathbb{F}_p$.

Assim, um *Corpo Finito* F, digamos com q elementos (atenção para a diferença entre corpos finitos e extensões finitas), só pode ter uma cópia de $\mathbb{F}_p$. Além disso, $q = p^n$ onde n é a dimensão de F sobre $\mathbb{F}_p$, visto como espaço vetorial. De fato, tome $\{1, e_1, e_2, ..., e_{n-1}\}$ a base de F sobre $\mathbb{F}_p$ onde 1 é o gerador de $\mathbb{F}_p$. Então, dado $q \in F$, $q = \lambda_1.1 + \lambda_2.e_1 + ... + \lambda_n.e_{n-1}$, onde cada λ_i é um elemento de $\mathbb{F}_p$. Mas temos apenas p elementos distindos em $\mathbb{F}_p$, o que significa que temos p^n elementos distintos em F.

Observe que um Corpo de Característica p não é sempre finito, como exemplo tome o corpo quociente $\mathbb{F}_p(x) = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{F}_p[x], g(x) \neq 0\}$.

Considere um corpo finito F com q elementos, $q = p^n$, e ϕ o *Homomorfismo de Frobenius*, $\phi : F \to F$ dado por $\phi(x) = x^p$ para todo $x \in F$. O núcleo desse homorfismo é 0, pois F é um corpo. Como F é finito, temos que ϕ é um automorfismo. Então:

Teorema 2.2.1. *O grupo de automorfismos de F é cíclico de ordem n, gerado por ϕ.*

Recomenda-se ao leitor verificar a demonstração deste teorema em [1] (p. 246). Observe que todo automorfismo ϕ de um corpo finito tem como característica manter fixos os elementos do corpo $\mathbb{F}_p$ que ele contém, dizendo de outra forma, $\phi \in \text{Aut}_{\mathbb{F}_p}(F)$ (tal conjunto é definido no próximo capítulo).

Exemplo 2.2.2. *Considere o polinômio $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Observe que $f(x)$ é irredutível sobre $\mathbb{F}_2$, já que possui grau 3 e não possui raízes em $\mathbb{F}_2$. Podemos então tomar a extensão finita E de $\mathbb{F}_2$ como no Teorema 2.1.21, isto é, $E = \mathbb{F}_2[x]/\langle f(x)\rangle$.*

O corpo E assim formado possui $2^3 = 8$ elementos. De fato, podemos ver E como o corpo $\{a\theta^2 + b\theta + c \mid a, b, c \in \mathbb{F}_2\}$, onde θ é raiz de $f(x)$. Como $f(\theta) = \theta^3 + \theta + 1 = 0$, temos que $\theta^3 = \theta + 1$ (aqui vale lembrar que $-1 = 1$ em $\mathbb{F}_2$) e portanto, não é difícil de verificar que θ^2 e $\theta^4 = \theta^2 + \theta$ também são raízes de $f(x)$. Agora considere G o conjunto de automorfismos de E, temos que os elementos de G são três, a saber: ϕ_1 tal que $\phi_1(\theta) = \theta^2$; ϕ_2 tal que $\phi_2(\theta) = \theta^4$ e ϕ_3 tal que $\phi_3(\theta) = \theta$, já que os automorfismos levam raiz de $f(x)$ em raiz de $f(x)$.

Veja como calculamos a imagem de ϕ_1:

$$\begin{aligned}
\phi_1(0) &= 0^2 = 0 \\
\phi_1(1) &= 1^2 = 1 \\
\phi_1(\theta) &= \theta^2 \\
\phi_1(\theta^2) &= (\theta^2)^2 = \theta^4 = \theta^3\theta = (\theta+1)\theta = \theta^2 + \theta \\
\phi_1(\theta+1) &= (\theta+1)^2 = \theta^2 + 2\theta 1 + 1^2 = \theta^2 + 1 \\
\phi_1(\theta^2+1) &= \theta^4 + 2\theta^2 1 + 1^2 = \theta^2 + \theta + 1 \\
\phi_1(\theta^2+\theta) &= (\theta^2+\theta)^2 = (\theta^2)^2 + 2\theta^2\theta + \theta^2 = \theta^4 + \theta^2 = \theta^2 + \theta + \theta^2 = 2\theta^2 + \theta = \theta \\
\phi_1(\theta^2+\theta+1) &= (\theta^2+\theta+1)^2 = (\theta^2+\theta)^2 + 2(\theta^2+\theta)1 + 1^2 = \theta + 1
\end{aligned}$$

Na tabela abaixo temos as imagens de todos os automorfismos de E:

Elementos de E	*Imagem por ϕ_1*	*Imagem por ϕ_2*	*Imagem por $\phi_3 = \mathrm{Id}$*
0	0	0	0
1	1	1	1
θ	θ^2	$\theta^2+\theta$	θ
θ^2	$\theta^2+\theta$	θ	θ^2
$\theta+1$	θ^2+1	$\theta^2+\theta+1$	$\theta+1$
θ^2+1	$\theta^2+\theta+1$	$\theta+1$	θ^2+1
$\theta^2+\theta$	θ	θ^2	$\theta^2+\theta$
$\theta^2+\theta+1$	$\theta+1$	θ^2+1	$\theta^2+\theta+1$

Como esperado, $\phi_i \in G$, $i \in \{1,2,3\}$, mantém fixos os elementos de $\mathbb{F}_2$.

Perceba ainda que $\phi_2 = \phi_1 \circ \phi_1$ e $\phi_3 = \phi_1 \circ \phi_1 \circ \phi_1 = \mathrm{Id}$ isto é, G é um grupo cíclico, gerado por ϕ_1, de ordem 3, mesmo grau da extensão $E/\mathbb{F}_2$.

O automorfismo ϕ_1 é o Automorfismo de Frobenius.

2.3 Extensões Separáveis

Um polinômio irredutível $f(x) \in K[x]$ é *separável* sobre K se suas raízes em um fecho algébrico de K são distintas.

Uma extensão algébrica E sobre o corpo K é dita *separável* se para todo elemento de E seu polinômio minimal for separável sobre K.

Teorema 2.3.1. *Sejam K e L corpos tais que L é algebricamente fechado e seja $\alpha \in L$ um elemento algébrico sobre K. Se ψ é um homomorfismo de corpos de K em L, então o número de homomorfismos de corpos $\sigma : K(\alpha) \to L$, tal que $\sigma|_K = \psi$, é igual ao número de raízes distintas do polinômio minimal de α, $f(x) \in K[x]$.*

A demonstração do teorema acima pode ser vista no livro [1] página 233.

Seja E uma extensão algébrica sobre K e S o conjunto de todos os homomorfismos de corpos do tipo $\sigma : K(\alpha) \to L$, com $\alpha \in E$ e tal que $\sigma|_K = \psi$, onde $\psi : K \to L$ é um homomorfismo. Então chamamos de *grau de separabilidade de E sobre K* a cardinalidade de S que é denotado por $[E : K]_s$.

Os resultados apresentados abaixo podem ser verificados no livro [1] a partir da página 239.

Teorema 2.3.2. *Se $K \subset F \subset E$, onde E é uma extensão finita sobre K, então $[E : K]_s$ é finita e vale*

$$[E : K]_s = [E : F]_s \cdot [F : K]_s.$$

Além disso, $[E : K]_s \leq [E : K]$, onde $[E : K]$ é o grau da extensão.

Teorema 2.3.3. *Seja E uma extensão algébrica finita de K. E é extensão separável sobre K se somente se $[E : K]_s = [E : K]$. O elemento α é separável sobre K se somente se $K(\alpha)$ é separável sobre K.*

Teorema 2.3.4. *Seja E uma extensão algébrica de K e sejam $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementos que geram essa extensão. Se α_i é separável sobre K para todo $i \in \{1, 2, \ldots, n\}$ então E é separável sobre K.*

Teorema 2.3.5. *Seja E uma extensão finita de K. Existe um elemento $\alpha \in E$ tal que $E = K(\alpha)$ se, e somente se, existe um número finito de corpos intermediários entre K e E. Se E é extensão separável, tal elemento α existe.*

O elemento α como acima é chamado *elemento primitivo.*

As definições e os resultados apresentados a seguir nos ajudarão no entendimento de um dos principais teoremas desta seção.

Definição 2.3.6. *Seja $f(x) \in K[x]$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. O polinômio $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 2 a_2 x + a_1 \in K[x]$ é chamado de* derivada de $f(x)$.

Para $f(x), g(x) \in K[x]$ valem as seguintes propriedades:

1. $(f(x) + g(x))' = f'(x) + g'(x)$
2. $(af(x))' = af'(x)$ para todo $a \in K$.
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Esta definição nos auxilia na verificação da existência de zeros múltiplos de um polinômio $f(x) \in K[x]$.

Teorema 2.3.7. *Um polinômio $f(x)$ sobre K tem raiz múltipla em alguma extensão E se somente se $f(x)$ e $f'(x)$ tem fator comum, dadas as respectivas decomposições.*

O resultado acima é uma importante ferramenta quando necessitamos verificar a irredutibilidade de um polinômio com coeficientes em corpos de característica 0 e nos ajuda a compreender a prova de outro importante resultado, apresentado a seguir.

Teorema 2.3.8. *Seja $f(x)$ um polinômio irredutível sobre K. Se K tem característica zero, então $f(x)$ não tem raízes múltiplas. Se K tem característica $p \neq 0$, então $f(x)$ tem raiz múltipla se somente se $f(x) = g(x^p)$ para algum $g(x) \in K[x]$.*

Ver [2] página 233.

Definição 2.3.9. *Um corpo K é chamado de* corpo perfeito *se todo polinômio irredutível $f(x) \in K[x]$ é separável.*

Podemos afirmar que K é corpo perfeito se tem característica zero ou se tem característica p e $K^p = \{a^p | a \in K\} = K$.

De fato, $f(x) \in K[x]$ irredutível com a característica de K igual a zero, pelo teorema acima, $f(x)$ não possui múltiplos zeros, isto é, é separável. Agora, se K tem característica p, suponha $f(x) \in K[x]$ não separável. Então $f(x)$ terá raízes múltiplas e poderá ser escrito como $g(x^p)$ para algum $g(x) \in K[x]$ e cada termo de $g(x^p)$ pode ser escrito como $a_k x^{pl_k}$, com $a_k \in K$ e $k \in \{1,2,\ldots,n\}$. Como $K^p = K$, temos que $a_k x^{pl_k} = b_k^p x^{pl_k}$, com $b_k \in K$, logo $a_k x^{pl_k} = (b_k x^{l_k})^p$. Assim $f(x)$ é decomposto em polinômios do tipo $(h(x))^p$, e portanto não será irredutível. Absurdo.

Dessa maneira podemos mostrar que todo corpo finito K é perfeito, basta tomar $\phi : K \to K$ tal que $\phi(x) = x^p$, com p primo, a característica de K, e mostrar que ϕ é um isomorfismo.

Corolário 2.3.10. *Se K é corpo de característica zero, então toda extensão finita E sobre K é separável.*

Ver [1] página 248.

Observação 2.3.11. *Os homomorfismos de corpos que compõem o cojunto S, definido no início desta seção, cuja cardinalidade define o grau de separabilidade, irá coincidir* *com o grupo de automorfismos da extensão que fixam o corpo base, toda vez que a extensão for normal e separável. Em geral, dada uma extensão E de um corpo K, os isomorfismos que fixam os elementos de K que vão da extensão E até uma subextensão de um fecho algébrico de K podem ser vistos como os elementos de S (tal resultado pode ser visto em [8], teorema 20, seção 5 do Capítulo I). Como vimos, quando uma extensão é separável e finita, o grau de separabilidade é o mesmo grau da extensão, veremos nas seções seguintes que esse valor também será igual à ordem do grupo de automorfismos dessa extensão que fixam o corpo base.*

2.4 Raízes da Unidade

Seja K um corpo. Se $\zeta \in K$ é tal que $\zeta^n = 1$, para algum $n \geq 1$ natural, então chamamos ζ de *raiz da unidade.*

Se K tem característica p, então a equação $x^{p^m} = 1$ tem somente uma raiz, 1, logo não existe p^m-ésima raiz da unidade além de 1.

Seja $n \in \mathbb{N}$, $n > 1$ e não divisível pela característica de K, então o polinômio $x^n - 1$ é separável pois a derivada $nx^{n-1} \neq 0$ e sua única raiz é zero, isto é, não tem raiz comum com $x^n - 1$. Portanto em uma extensão de decomposição de $x^n - 1$ sobre K, encontramos n raízes da unidade distintas.

O conjunto das n raízes da unidade formam um grupo cíclico cujo gerador é chamado de raiz n-ésima primitiva da unidade, denotado por ζ_n.

2.5 Extensões Inseparáveis

Os resultados desta seção podem ser verificados no livro [1] página 247 em diante.

Dizemos que uma extensão de corpos é *inseparável* se não for separável.

Proposição 2.5.1. *Seja α algébrico sobre K, $\alpha \in L$, onde L é fecho algébrico de K.*

Seja ainda $f(x)$ o polinômio minimal de α sobre K. Se K tem característica zero, então todas as raízes de $f(x)$ tem multiplicidade 1 (f é separável em L). Se K tem característica $p > 0$, então existe um inteiro $\mu \geq 0$ tal que toda raiz de $f(x)$ tem multiplicidade p^μ. Além disso

$$[K(\alpha) : K] = p^\mu [K(\alpha) : K]_s$$

e α^{p^μ} é separável sobre K.

Corolário 2.5.2. *Para qualquer extensão finita E de K, o grau de separabilidade $[E : K]_s$ divide o grau da extensão $[E : K]$. O quociente é 1 se a característica de K é zero, e uma potência de p se a característica de K for $p > 0$.*

Definição 2.5.3. *Chamamos de* grau de inseparabilidade *o quociente $[E : K]/[E : K]_s$ e o denotamos por $[E : K]_i$.*

Corolário 2.5.4. *Uma extensão finita é separável se somente se $[E : K]_i = 1$.*

Corolário 2.5.5. *Se $E \supset F \supset K$ são duas extensões finitas, então $[E : K]_i = [E : F]_i [F : K]_i$.*

Definição 2.5.6. *Um elemento α algébrico sobre K, corpo de característica $p > 0$, é* puramente inseparável sobre *K se existe um inteiro $n \geq 0$ tal que α^{p^n} é um elemento de K.*

Tomando a extensão algébrica E sobre K pode-se verificar também as seguintes afirmações equivalentes: (K corpo de característica $p > 0$)

i) $[E : K]_s = 1$

ii) Todo elemento α de E é puramente inseparável sobre K.

iii) Para todo elemento $\alpha \in E$, o polinômio minimal de α sobre K é do tipo $f(x) = x^{p^n} - a$ para algum $n \geq 0$ e $a \in K$.

iv) Existe um conjunto de geradores $\{\alpha_i\}_{i\in I}$ de E sobre K tal que cada α_i é puramente inseparável sobre K.

Definição 2.5.7. *A extensão E sobre K que satisfaz alguma das propriedades acima é chamada de* extensão puramente inseparável.

2.6 O Teorema de Galois

Definição 2.6.1. *Uma extensão E de um corpo K é chamada* Extensão Galoisiana *ou* Extensão de Galois *se for normal e separável.*

Uma extensão de corpo finita sobre um corpo K que é galoisiana, portanto separável, pode ser formada pela adjunção de um elemento algébrico α (elemento primitivo) ao corpo K e, como também é normal, podemos tomar o polinômio minimal de α, cujo grau é o mesmo da extensão, para que essa extensão seja seu corpo de decomposição. De maneira recíproca, se uma extensão finita é corpo de decomposição de algum polinômio com coeficientes no seu corpo base então é normal e separável. (ver Teorema 3.11, página 262, do livro [12])

Exemplo 2.6.2. $\mathbb{Q}(\sqrt[3]{2})$ *é subextensão de* $\mathbb{Q}(\sqrt[3]{2},\omega)$ *sobre* $\mathbb{Q}$*, onde* ω *é uma raiz complexa de* $f(x) = x^3 - 2$*. A extensão* $\mathbb{Q}(\sqrt[3]{2},\omega)$ *de* $\mathbb{Q}$ *é galoisiana, mas* $\mathbb{Q}(\sqrt[3]{2})$ *não é galoisiana.*

Definição 2.6.3. *Seja E uma extensão de K. Chamamos de $\mathrm{Aut}_K E$ o conjunto de todos automorfismos de E que fixam K, isto é, se $\varphi \in \mathrm{Aut}_K E$ então $\varphi|_K = \mathrm{Id}$. Também dizemos que φ é um K-*automorfismo *de E.*

Dados φ_1, φ_2, $\varphi_3 \in \mathrm{Aut}_K E$, $(\varphi_1 \circ \varphi_2) \circ \varphi_3 = \varphi_1 \circ (\varphi_2 \circ \varphi_3)$, $\mathrm{Id} \in \mathrm{Aut_K E}$ e $\varphi \circ \mathrm{Id} = \mathrm{Id} \circ \varphi = \varphi \ \forall \ \varphi \in \mathrm{Aut}_K E$, e, por fim, $\forall \ \varphi \in \mathrm{Aut}_K E$, $\exists \ \varphi^{-1}$ tal que $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \mathrm{Id}$ pois φ é isomorfismo. Portanto, $\mathrm{Aut}_K E$ forma um grupo com a operação composição.

Denotamos por

$$\begin{aligned} G(E/K) &= \{\varphi : E \to E \mid \varphi \text{ é um } K\text{-automorfismo}\} \\ &= \{\varphi | \varphi \in \mathrm{Aut}_K E\} \end{aligned}$$

este grupo é chamado de *Grupo de Galois* de E sobre K.

Teorema 2.6.4. *Seja E uma extensão finita de K. Então as seguintes condições são equivalentes:*

i) *E é extensão galoisiana sobre K;*

ii) $\forall\ \alpha \in E \setminus K\ \exists\ \varphi \in\ \mathrm{Aut}_K E$ *tal que* $\varphi(\alpha) \neq \alpha$*;*

iii) $[E : K] = |G(E/K)|$.

Exemplo 2.6.5. $\mathbb{Q}(\sqrt{2})$ *é uma extensão galoisiana, pois é também o corpo de decomposição de $f(x) = x^2 - 2$, que é minimal sobre $\mathbb{Q}$. Como $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $\mathbb{Q}(\sqrt{2})$ é extensão normal (ver exemplo (2.1.10) na página 20).*

Agora, seja $\alpha \in \mathbb{Q}(\sqrt{2})$, então $\alpha = a + b\sqrt{2}$, com a, $b \in \mathbb{Q}$. A base desta extensão é $\{1, \sqrt{2}\}$, e sendo φ um $\mathbb{Q}$-automorfismo, $2 = \varphi(2)$, mas

$$\varphi(2) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = (\varphi(\sqrt{2}))^2.$$

Logo $\varphi(\sqrt{2}) = \pm\sqrt{2}$.

E essas são as possibilidades de automorfismos de $\mathbb{Q}(\sqrt{2})$. Se $\varphi(\sqrt{2}) = \sqrt{2}$ e $\varphi|_{\mathbb{Q}} = \mathrm{Id}$ então $\varphi = \mathrm{Id}$. Portanto $|G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$.

Exemplo 2.6.6. *Considerando* $\mathbb{Q}(\sqrt{3},\sqrt{5})$ *extensão de* $\mathbb{Q}$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{3},\sqrt{5}) \arrow[dl, dash, "2"'] \arrow[dd, dash, "4"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Verificamos facilmente que $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 4$ *e que* $\mathbb{Q}(\sqrt{3},\sqrt{2})$ *é o corpo de decomposição de* $f(x) = (x^2 - 3)(x^2 - 5)$ *em* $\mathbb{Q}[x]$.

Um isomorfismo leva base em base e $\{1,\sqrt{3},\sqrt{5},\sqrt{3}\sqrt{5}\}$ *é base de* $\mathbb{Q}(\sqrt{3},\sqrt{5})$ *sobre* $\mathbb{Q}$, *visto como espaço vetorial.*

Assim, se φ *é um* $\mathbb{Q}$*-automorfismo de* $\mathbb{Q}(\sqrt{3},\sqrt{5})$, $\varphi(\sqrt{3}\sqrt{5}) = \varphi(\sqrt{3})\varphi(\sqrt{5})$. *Basta então definirmos* $\varphi(\sqrt{3})$ *e* $\varphi(\sqrt{5})$. *Mas,*

$$(\varphi(\sqrt{3}))^2 = \varphi((\sqrt{3})^2) = \varphi(3) = 3 \quad \Rightarrow \quad \varphi(\sqrt{3}) = \pm\sqrt{3}$$
$$(\varphi(\sqrt{5}))^2 = \varphi((\sqrt{5})^2) = \varphi(5) = 5 \quad \Rightarrow \quad \varphi(\sqrt{5}) = \pm\sqrt{5}$$

Temos então os seguinte $\mathbb{Q}$*-automorfismos:*

$$\begin{aligned}
\varphi_1(\sqrt{3}) &= \sqrt{3},\ \varphi_1(\sqrt{5}) = \sqrt{5} \ \Rightarrow \ \varphi_1 = \mathrm{Id}.\\
\varphi_2(\sqrt{3}) &= -\sqrt{3},\ \varphi_2(\sqrt{5}) = \sqrt{5}\\
\varphi_3(\sqrt{3}) &= \sqrt{3},\ \varphi_3(\sqrt{5}) = -\sqrt{5}\\
\varphi_4(\sqrt{3}) &= -\sqrt{3},\ \varphi_4(\sqrt{5}) = -\sqrt{5}
\end{aligned}$$

Logo, $|G(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q})| = 4$.

Definição 2.6.7. *Seja* E *uma extensão do corpo* K *e seja* $G(E/K)$ *o grupo de galois.*

Se H é um subgrupo de $G(E/K)$, o conjunto denotado por

$$E_H = \{x \in E \mid \varphi(x) = x, \forall\ \varphi \in H\}$$

é um corpo chamado de corpo fixo *de H.*

Lema 2.6.8 (Artin)**.** *Se $G(E/K)$ é o grupo finito dos K-automorfismos de E, então*

$$|G(E/K)| \leq [E : K]$$

Teorema 2.6.9 (Teorema Fundamental da Teoria de Galois)**.** *Seja L extensão finita e galoisiana de K. Existe uma correspondência biunívoca entre os subcorpos de L que contém K e os subgrupos de $G(L/K)$. Essa correspondência é dada pela função ψ tal que $\psi(H) \mapsto L_H$, $H \subset G(L/K)$ subgrupo, e a inversa $\psi^{-1}(E) \mapsto \mathrm{Aut}_E L$, $K \subset E \subset L$, E subcorpo de L.*

Nesta correspondência, se $H = \mathrm{Aut}_E L$ então $[L : E] = |H|$. Além disso, E é extensão galoisiana sobre K se e só se H for subgrupo normal de $G(L/K)$, neste caso $\mathrm{Aut}_K E \cong G(L/K)/H$.

Exemplo 2.6.10. *Seja $\mathbb{Q}(i,\sqrt{2})$, extensão galoisiana de $\mathbb{Q}$. Temos que $\{1,i,\sqrt{2},i\sqrt{2}\}$ é a base do espaço vetorial $\mathbb{Q}(i,\sqrt{2})$ sobre $\mathbb{Q}$ e $\phi(i\sqrt{2}) = \phi(i)\phi(\sqrt{2})$, $\forall$ automorfismo ϕ de $\mathbb{Q}(i,\sqrt{2})$. Assim determinamos os automorfismos:*

$$\begin{aligned}
\phi_1,\ \textit{tal que}\ \phi_1(i) &= i\ \textit{e}\ \phi_1(\sqrt{2}) = -\sqrt{2} \\
\phi_2,\ \textit{tal que}\ \phi_2(i) &= -i\ \textit{e}\ \phi_2(\sqrt{2}) = \sqrt{2} \\
\phi_3,\ \textit{tal que}\ \phi_3(i) &= -i\ \textit{e}\ \phi_3(\sqrt{2}) = -\sqrt{2}
\end{aligned}$$

como elementos de $G(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})$ além da identidade. Neste caso sabemos também que $\{\mathrm{Id},\phi_1\}$, $\{\mathrm{Id},\phi_2\}$, $\{\mathrm{Id},\phi_3\}$ são os subgrupos próprios de $G(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})$, e $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$ são os subcorpos próprios de $\mathbb{Q}(i,\sqrt{2})$ que contém $\mathbb{Q}$.

Observe ainda que $\{\mathrm{Id}, \phi_1\} = \mathrm{Aut}_{\mathbb{Q}(\mathrm{i})}\mathbb{Q}(\mathrm{i}, \sqrt{2})$, *assim*

$$[\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}(i)] = |\mathrm{Aut}_{\mathbb{Q}(i)}\mathbb{Q}(i,\sqrt{2})|.$$

E, $\mathbb{Q}(i)$ *é extensão galoisiana, pois é a extensão de decomposição de* $f(x) = x^2+1$ *sobre* $\mathbb{Q}$. *O subgrupo* $\{\mathrm{Id}, \phi_1\}$ *de* $G(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})$ *é normal. De fato,*

$$\begin{array}{rcl} \phi_2^{-1} \circ \mathrm{Id} \circ \phi_2 & = & \mathrm{Id}, \\ \phi_2^{-1} \circ \phi_1 \circ \phi_2 & : & \phi_2^{-1}(\phi_1(\phi_2(i))) = \phi_2^{-1}(\phi_1(-i)) = \phi_2^{-1}(-i) = i = \phi_1(i) \\ & : & \phi_2^{-1}(\phi_1(\phi_2(\sqrt{2}))) = \phi_2^{-1}(\phi_1(\sqrt{2})) = \phi_2^{-1}(-\sqrt{2}) = -\sqrt{2} = \phi_1(\sqrt{2}) \\ & \Rightarrow & \phi_2^{-1} \circ \phi_1 \circ \phi_2 = \phi_1 \in \ \{\mathrm{Id}, \phi_1\} \end{array}$$

Analogamente verificamos que $\phi_3^{-1} \circ \mathrm{Id} \circ \phi_3 = \mathrm{Id}$ *e* $\phi_3^{-1} \circ \phi_1 \circ \phi_3 = \phi_1$.

Portanto, $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(i) \cong G(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})/\mathrm{Aut}_{\mathbb{Q}(i)}\mathbb{Q}(i,\sqrt{2})$, *fato que pode ser facilmente verificado, pois ambos os grupos possuem ordem* 2.

Teorema 2.6.11 (Artin)**.** *Seja* E *um corpo e seja* G *o grupo de automorfismos de* E*, com ordem de* G *igual a* n. *Seja* $K = E_G$ *(corpo fixo de* G*). Então* E *é uma extensão galoisiana de* K, $G = G(E/K)$ *e* $[E : K] = n$.

Corolário 2.6.12. *Seja* E *uma extensão galoisiana finita de* K *e seja* $G(E/K)$ *o grupo de galois correspondente. Então todo subgrupo de* $G(E/K)$ *é grupo de galois de* E *sobre alguma extensão de* K *contida em* E.

De fato, o corolário pode ser facilmente verificado com a aplicação do Teorema Tundamental da Teoria de Galois e o teorema acima. A demonstração pode ser encontrada em [1] página 264.

Definição 2.6.13. *Sejam duas extensões* E *e* F *sobre um corpo* K. *Então definimos como* extensão composta *e denotamos por* EF *o menor corpo que contém* E *e* F. *Se* $F = K(\alpha_1, \ldots, \alpha_n)$ *e* E *é outra extensão sobre* K, *então podemos usar a notação* $EF = E(\alpha_1, \ldots, \alpha_n)$.

Teorema 2.6.14. *Seja E uma extensão galoisiana de K e seja F outra extensão algébrica de K. Suponha que E e F sejam subcorpos de outra extensão algébrica de K. Então EF é extensão galoisiana sobre F, e E é extensão galoisiana sobre $E \cap F$. Agora, tome a aplicação*

$$\varphi : G(EF/F) \to G(E/K)$$

tal que $\varphi(\sigma) = \sigma_{|_E}$, então φ é um isomorfismo de $G(EF/F)$ em $G(E/E \cap F) \subset G(E/K)$.

A demonstração do teorema acima está na primeira seção do capítulo sexto de [1].

Corolário 2.6.15. *Seja E uma extensão galoisiana finita de K e F uma outra extensão qualquer de K, então $[EF : F]$ divide $[E : K]$.*

É só verificar que a ordem de $G(EF/F)$ divide a ordem de $G(E/K)$ pelo Teorema de Lagrange, pois $G(EF/F)$ é isomorfo a um subgrupo de $G(E/K)$, pelo Teorema (2.6.14).

Importante observar que se excluirmos a hipótese de E ser galoisiana sobre K, não teríamos o mesmo resultado. Basta verificar o seguinte exemplo.

Exemplo 2.6.16. *Tome $\zeta = \dfrac{-1+\sqrt{-3}}{2}$, $\alpha = \sqrt[3]{2}$ e $\beta = \zeta \cdot \alpha$. Agora sejam as extensões $E = \mathbb{Q}(\beta)$, $F = \mathbb{Q}(\alpha)$, $E \neq F$, e*

$$EF = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha,\zeta) = \mathbb{Q}(\alpha,\sqrt{-3}).$$

Temos que $E \cap F$ é subcorpo de F, logo tem grau 3 ou 1 sobre $\mathbb{Q}$, pois F tem grau 3 sobre $\mathbb{Q}$. Assim, $E \cap F$ deve ter grau 1 sobre $\mathbb{Q}$ (isto é $E \cap F = \mathbb{Q}$), já que $F \not\subset E$. Como $EF = \mathbb{Q}(\alpha,\sqrt{-3})$, EF/F tem grau 2, logo $E/E \cap F = E/\mathbb{Q}$ tem grau 2. Absurdo. O absurdo aconteceu pois tentamos usar o Teorema (2.6.14) com E não galoisiana.

Teorema 2.6.17. *Sejam E_1 e E_2 extensões galoisianas de K. Então E_1E_2 é extensão galoisiana sobre K, a aplicação $\varphi : G(E_1E_2/K) \to G(E_1/K) \times G(E_2/K)$ tal que $\varphi(\sigma) = (\sigma_{|_{E_1}}, \sigma_{|_{E_2}})$ é injetiva. Se $E_1 \cap E_2 = K$, então φ é isomorfismo.*

Observe que obtemos uma decomposição para $G(E_1E_2/K)$ caso $E_1 \cap E_2 = K$.

Corolário 2.6.18. *Seja E uma extensão galoisiana finita sobre K, e suponha $G(E/K) \simeq G_1 \times G_2 \times ... \times G_n$. Seja ainda K_i o corpo fixo de $G_1 \times G_2 \times ... \times \{1\} \times ... \times G_n$, onde o grupo $\{1\}$ ocupa a i-ésima posição no produto direto. Então K_i é extensão galoisiana sobre K e $K_{i+1} \cap (K_1...K_i) = K$. Além disso, $E = K_1...K_n$.*

O corolário acima nos diz que caso a extensão galoisiana seja finita e exista a decomposição do seu grupo de galois, podemos decompor também a extensão, de maneira que cada extensão obtida nesta decomposição terá seu grupo de galois correspondendo com algum na decomposição do grupo de galois da extensão inicial. Observe que se o grupo de Galois dessa extensão for abeliano, certamente haverá uma decomposição para ele. Usaremos esse fato quando mostrarmos os teoremas de correspondência na teoria de Kummer.

2.7 Norma e Traço

Seja E uma extensão finita de K tal que $[E:K]_s = r$. Vimos que $[E:K]_i = p^\mu$ se a característica de K é $p > 0$ e $[E:K]_i = 1$ se a característica de K é zero.

Se α é um elemento de E e $\sigma_1, \ldots, \sigma_r$ os homomorfismos distintos de E sobre L, fecho algébrico de K, definimos a *norma* de E sobre K como

$$\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_K^E(\alpha) = \prod_{v=1}^{r} \sigma_v(\alpha)^{[E:K]_i} = \left(\prod_{v=1}^{r} \sigma_v(\alpha)\right)^{[E:K]_i}.$$

Também definimos *traço* como:

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_K^E(\alpha) = [E:K]_i \sum_{v=1}^{r} \sigma_v(\alpha).$$

O traço é igual a zero se $[E:K]_i > 1$, em outras palavras, se E/K não é separável. (Basta observar que $[E:K]_i = p^\mu$ para algum μ natural.)

Se E é separável sobre K, temos

$$\mathrm{N}_K^E(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

onde o produto é dado usando os distintos homomorfismos de E em L sobre K.

Se E/K é separável, então

$$\mathrm{Tr}_K^E(\alpha) = \sum_{\sigma} \sigma(\alpha).$$

Teorema 2.7.1.

- *Seja E/K uma extensão finita. Então a norma N_K^E é um homomorfismo multiplicativo de E^* em K^* e o traço é um homomorfismo aditivo de E em K.*
- *Se $E \supset F \supset K$ é uma cadeia de corpos, então*

$$\mathrm{N}_K^E = \mathrm{N}_F^E \circ \mathrm{N}_K^F \quad e \quad \mathrm{Tr}_K^E = \mathrm{Tr}_F^E \circ \mathrm{Tr}_K^F,$$

  isto é, possuem a propriedade transitiva.
- *Se $E = K(\alpha)$ e $f(x)$ for o polinômio minimal de α sobre K, então*

$$\mathrm{N}_K^{K(\alpha)}(\alpha) = (-1)^n a_0 \quad e \quad \mathrm{Tr}_K^{K(\alpha)}(\alpha) = -a_{n-1},$$

  onde n é o grau de $f(x)$, a_0 e a_{n-1} são, respectivamente, termo independente de $f(x)$ e o coeficiente de x^{n-1} em $f(x)$.

Exemplo 2.7.2. *Tome $\mathrm{N} : \mathbb{C}^* \to \mathbb{R}^*$, a norma de $\mathbb{C}$ sobre $\mathbb{R}$. Temos que $\mathbb{C}$ tem característica 0, portanto separável, e $\mathrm{N}(a+bi) = \sigma_1(a+bi).\sigma_2(a+bi)$ (temos dois automorfismos distintos, um que leva i em i e outro que leva i em $-i$). Logo $\mathrm{N}(a+bi) = a^2+b^2$. É fácil verificar que N de fato é um homomorfismo.*

Vemos também que o traço $\mathrm{Tr} : \mathbb{C}^+ \to \mathbb{R}^+$, onde $\mathbb{C}^+$ e $\mathbb{R}^+$ são grupos aditivos, é homomofismo e $\mathrm{Tr}(a+bi) = \sigma_1(a+bi) + \sigma_2(a+bi) = 2a$

Tome agora a transformação linear $m_Z : \mathbb{C} \to \mathbb{C}$ tal que $m_Z(W) = W \cdot Z$, para todo

$W \in \mathbb{C}$ e $Z = a + bi \in \mathbb{C}$. É fácil verificar que a matriz dessa transformação linear na base canônica de $\mathbb{C}$, como $\mathbb{R}$-espaço vetorial, é

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

E assim verificamos que $\mathrm{N}(a+bi) = \det\ A$ *e* $\mathrm{Tr}(a+bi) = \mathrm{Tr}\ A$.

Observe que no exemplo acima, a norma não é um homomorfismo sobrejetor. Em geral, dada uma extensão L/K, a norma $\mathrm{N} : L^* \to K^*$, não é sobrejetora e o estudo do grupo quociente $K^*/\mathrm{N}(L^*)$ é um problema importante na teoria dos números.

2.8 Extensões Cíclicas e Abelianas

Uma extensão E é chamada de *cíclica* sobre um corpo K se E for uma extensão galoisiana e se seu grupo de Galois for um grupo cíclico. Da mesma forma, uma extensão galoisiana tal que seu grupo de Galois é abeliano, é chamada de extensão *abeliana*. Obviamente, toda extensão cíclica é também extensão abeliana.

Teorema 2.8.1. *Seja E uma extensão Galoisiana de K e F extensão de K tal que $K \subset F \subset E$. Então F é extensão normal de K se somente se, $G(E/F)$ é subgrupo normal de $G(E/K)$. E ainda, a aplicação $\varphi : G(E/K) \to G(F/K)$ é um homomorfismo sobrejetor onde $\varphi(\sigma) = \sigma_{|_F}$ e o núcleo de φ é $G(E/F)$. Isto é , $G(F/K) \simeq G(E/K)/G(E/F)$.*

Corolário 2.8.2. *Seja E uma extensão cíclica e F uma extensão tal que $K \subset F \subset E$. Então F é extensão Galoisiana sobre K também cíclica.*

Observação 2.8.3. *O resultado acima também vale se substituirmos extensão cíclica por extensão abeliana e a demonstração é análoga. Veja na referência [1], página 265.*

Teorema 2.8.4 (Teorema 90 de Hilbert)**.** *Sejam E uma extensão cíclica de grau n sobre um corpo K e $G(E/K)$ o seu grupo de Galois. Seja β um elemento de E. Então* *a norma* $\mathrm{N}_K^E(\beta) = 1$ *se somente se existe um elemento* $\alpha \neq 0$ *em* E *tal que* $\beta = \alpha/\sigma(\alpha)$ *onde* σ *é isomorfismo gerador de* $G(E/K)$.

Demonstração. Se considerarmos que tal elemento α existe, então se vermos a norma como um homomorfismo podemos obter da igualdade $\beta = \alpha/\sigma(\alpha)$ a seguinte igualdade $\mathrm{N}(\beta) = \mathrm{N}(\alpha/\sigma(\alpha))$ o que implica em $\mathrm{N}(\beta) = \mathrm{N}(\alpha)/\mathrm{N}(\sigma(\alpha))$. Mas

$$\mathrm{N}(\sigma(\alpha)) = \sigma_1(\sigma(\alpha)) \cdot \sigma_2(\sigma(\alpha)) \ldots \sigma_n(\sigma(\alpha))$$

pois o grau de inseparabilidade é 1.

Como σ é gerador de $G(E/K)$, $\sigma_i = \sigma^j$, para $i = 1, \ldots, n$ e para algum $j \in \{ 0, \ldots, n-1\}$. Além disso $\sigma_i \circ \sigma = \sigma_k$, para alguma $k \in \{ 0, \ldots, n\}$, ou seja $\mathrm{N}(\sigma(\alpha)) = \mathrm{N}(\alpha)$ e portanto $\mathrm{N}(\beta) = 1$.

Antes de terminar a demonstração do teorema, vamos definir caráter de um grupo G sobre um corpo K e anunciar um resultado importante.

Definição 2.8.5. *Um* Caráter *de um monoide* G *sobre um corpo* K *é um homomorfismo* $f : G \to K^*$.

Teorema 2.8.6 (Artin)**.** *Seja* G *um monide e* K *um corpo e* $f_1, f_2, \ldots, f_n$ *caráteres distintos de* G *sobre* K. *Esses caráteres formam um conjunto de elementos linearmente independentes sobre* K.

Demonstração. Suponha a relação $a_1 f_1 + \ldots + a_n f_n = 0$, com $a_i \in K$, $i = 1, \ldots, n$, de forma que nem todos $a_i's$ sejam nulos. Temos que, no mínimo dois $a_i's$ são diferentes de zero. Tomando o menor m possível tal que os $a_i's$ sejam diferentes de zero, $m \geq 2$.

Como f_1 e f_2 são distintos, existe $z \in G$ tal que $f_1(z) \neq f_2(z)$ e ainda

$$\begin{aligned} a_1 f_1(z) + \ldots + a_m f_m(z) &= 0 \\ a_1 f_1(xz) + \ldots + a_m f_m,(xz) &= 0 \ \forall \ x \in G \\ a_1 f_1(z) f_1(x) + \ldots + a_m f_m(z) f_n(x) &= 0 \end{aligned}$$

pois f_i é homomorfismo.

Se dividirmos a relação acima por $f_1(z)$ teremos

$$a_1 f_1 + a_2 \frac{f_2(z)}{f_1(z)} f_2 \ldots + a_m \frac{f_m(z)}{f_1(z)} f_m = 0$$

(usamos simplesmente f_i no lugar de $f_i(x) \ \forall \ x \in G$).

Subtraindo $a_1 f_1 + \ldots + a_m f_m = 0$, temos

$$\left(a_2 \frac{f_2(z)}{f_1(z)} - a_2 \right) f_2 + \ldots + \left(a_m \frac{f_m(z)}{f_1(z)} - a_m \right) f_m = 0$$

onde $a_i \frac{f_i(z)}{f_1(z)} - a_i = \beta_i \ \in K$, pois $f_i(z), f_1(z) \ \in K, \forall \ i = \ 2, 3, \ldots, m$. Observe que, pelo menos, $\beta_2 \neq 0$ pois $\dfrac{f_2(z)}{f_1(z)} \neq 1$. Logo obtemos $\beta_2 f_2 + \ldots + \beta_m f_m = 0$, com $m-1$ termos e $\beta_i{}'s$ não simultaneamente nulos, isto é, obtemos uma relação com menos termos que a primeira relação tomada. Absurdo, pois supomos m o menor possível.

Portanto, $a_1 f_1 + \ldots + a_n f_n = 0 \ \Leftrightarrow \ a_i = 0 \ \forall \ i = \ 1, 2, \ldots, n$. Logo $f_1, \ldots, f_n$ são L.I. sobre K. ■

Voltando à demonstração do Teorema (2.8.4), supomos que $N(\beta) = 1$. Temos $G(E/K)$ cíclico gerado por σ. Sejam

$$\sigma_0 = \sigma^n = \mathrm{Id}, \ \sigma_1 = \sigma, \ \sigma_2 = \sigma^2, \ldots, \ \sigma_{\mathrm{n-1}} = \sigma^{\mathrm{n-1}}$$

os elementos de $G(E/K)$. Cada σ_i é um carácter de E sobre E^* e

$$\mathrm{Id} + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3 + \ldots + \beta\sigma(\beta)\cdot\ldots\cdot\sigma^{\mathrm{n}-2}(\beta)\sigma^{\mathrm{n}-1}$$

é uma aplicação não identicamente nula, pois Id, $\sigma, \ldots, \sigma^{\mathrm{n}-1}$ são L.I. (Teorema (2.8.6)) e

$$1,\ \beta,\ \beta\sigma(\beta), \ldots,\ \beta\sigma(\beta)\cdot\ldots\cdot\sigma^{n-2}(\beta)$$

pertencem a E.

Portanto, existe $\theta \in E$ tal que o elemento

$$\alpha = \theta + \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta)\cdot\ldots\cdot\sigma^{n-2}(\beta)\sigma^{n-1}(\theta) \neq 0.$$

Assim

$$\beta\sigma(\alpha) = \beta\cdot\sigma(\theta) + \beta\cdot\sigma(\beta)\cdot\sigma^2(\theta) + \ldots + \beta\cdot\sigma(\beta)\cdot\sigma^2(\beta)\cdot\ldots\cdot\sigma^{n-1}(\beta)\cdot\sigma^n(\theta).$$

Como $\sigma^n(\beta) = \mathrm{Id}(\beta) = \beta$,

$$\sigma(\beta)\cdot\sigma^2(\beta)\cdot\ldots\cdot\sigma^{n-1}(\beta)\cdot\sigma^n(\beta) = N(\beta) = 1,$$

$\sigma^n(\theta) = \mathrm{Id}(\theta) = \theta$, temos que

$$\beta\sigma(\theta) = \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \ldots + \beta\sigma(\beta)\cdot\ldots\cdot\sigma^{n-2}(\beta)\sigma^{n-1}(\theta) + \theta = \alpha$$

e $\beta\sigma(\alpha) = \alpha$, então $\beta = \alpha/\sigma(\alpha)$.

■

Exemplo 2.8.7. *Tome a extensão $\mathbb{Q}(i)/\mathbb{Q}$ galoisiana. Temos que $G(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{Id}, \sigma\}$ tal que $\sigma(i) = -i$. Agora, tome $\beta = (x+iy) \in \mathbb{Q}(i)$. Temos que $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(i)}(\beta) = [\mathrm{Id}(\beta).\sigma(\beta)]^{[\mathbb{Q}(\mathrm{i}):\mathbb{Q}]_{\mathrm{i}}}$, como $\mathbb{Q}$ tem característica 0, $[\mathbb{Q}(i):\mathbb{Q}]_i = 1$ e $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(i)}(\beta) = \beta.\sigma(\beta) = (x+iy).(x-iy) = x^2+y^2$.*

Se a norma de β é igual a 1, significa que o par $(x,y) \in \mathbb{R}^2$ é ponto racional no círculo unitário. Nesse caso, o Teorema 2.8.4 garante a existência de $\alpha \neq 0$, $\alpha \in \mathbb{Q}(i)$, tal que $\beta = \dfrac{\alpha}{\sigma(\alpha)}$. Sendo $\alpha = a + bi$, para simplificar, podemos supor a e b inteiros (multiplicamos por um inteiro apropriado, por exemplo o produto dos denominadores de a e b, ou o mmc deles) e temos $\beta = \dfrac{a+bi}{a-bi} = \dfrac{a^2+2abi-b^2}{a^2+b^2}$, e portanto encontrar $\beta \in \mathbb{Q}(i)$ que satisfaz $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(i)}(\beta) = 1$ é encontrar a solução racional $\left(\dfrac{a^2-b^2}{a^2+b^2}, \dfrac{2ab}{a^2+b^2}\right)$ que por sua vez corresponde à tripla ou terna pitagórica $(a^2-b^2, 2ab, a^2+b^2)$.

O teorema abaixo utilizará diretamente o resultado obtido no Teorema 90 de Hilbert acima e é fundamental para a teoria multiplicativa que veremos nos capítulos de Cohomologia Galoisiana e Teoria de Kummer.

Teorema 2.8.8. *Seja K um corpo de característica $p \geq 0$ e assuma que exista uma raiz n-ésima primitiva da unidade em K, com n primo com p.*

i) *Seja E uma extensão cíclica sobre K de grau n. Então existe $\alpha \in E$ tal que $E = K(\alpha)$ e α satisfaz a equação $x^n - a = 0$ para algum $a \in K$.*

ii) *Por outro lado, seja $a \in K$. Seja α uma raiz de $x^n - a = 0$. Então $K(\alpha)$ é cíclico sobre K, de grau d, d divisor de n e $\alpha^d \in K$.*

Demonstração. i) Seja ζ a raiz n-ésima primitiva da unidade em K e seja $G(E/K)$ o grupo cíclico.

Temos que $\mathrm{N}(\zeta^{-1}) = (\zeta^{-1})^n = 1$, já que ζ^{-1} está em K, isto é, é fixo pelos automorfismos de $G(E/K)$, e também é uma raíz n-ésima da unidade. Aplicando o Teorema (2.8.4), temos que $\exists\ \alpha \in E$ tal que $\zeta^{-1} = \alpha/\sigma(\alpha)$, então $\sigma(\alpha) = \zeta\alpha$.

Como ζ está em K,

$$\begin{aligned}
\sigma^i(\alpha) &= \underbrace{\sigma\circ\sigma\circ\ldots\circ\sigma(\alpha)}_{i\ vezes}\\
&= \underbrace{\sigma\circ\sigma\circ\ldots\circ\sigma}_{i-1\ vezes}(\zeta\alpha)\\
&= \underbrace{\sigma\circ\sigma\circ\ldots\circ\sigma}_{i-2\ vezes}(\zeta\sigma(\alpha))\\
&= \underbrace{\sigma\circ\sigma\circ\ldots\circ\sigma}_{i-2\ vezes}(\zeta^2\alpha)\\
&= \sigma(\zeta^{i-1}\alpha) = \zeta^{i-1}\sigma(\alpha) = \zeta^{i-1}\zeta\alpha = \zeta^i\alpha
\end{aligned}$$

para $i = 1,\ldots,n$.

Seja $f(x)$ o polinômio minimal de α sobre K. Então, os elementos $\sigma^i(\alpha) = \zeta^i\alpha$ também são raízes de $f(x)$ e, portanto, $f(x)$ tem grau no mínimo n. Mas como $\zeta^i \in K\ \forall i$, $\zeta^i\alpha$ será elemento de $K(\alpha)$ para todo i. Portanto, $K(\alpha)$ é corpo de decomposição de $f(x)$ e, portanto, $[K(\alpha) : K] \leq n$. Como $[E : K] = n$, segue que $E = K(\alpha)$.

Além disso,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \zeta^n\alpha^n = \alpha^n,$$

isto é, α^n é fixo por σ e por todas as potências de σ. Logo $\alpha^n \in K$ e tomando $\alpha^n = a$, α satisfaz $x^n - a = 0$.

ii) Por outro lado, seja $a \in K$ e α raiz de $x^n - a = 0$. Então $\zeta^i\alpha$ também é raiz de $x^n - a = 0$, para todo $i = 1, \ldots, n$. De fato,

$$(\zeta^i\alpha)^n - a = (\zeta^n)^i\alpha^n - a = \alpha^n - a = 0,$$

portanto todas as raízes de $x^n - a$ estão em $K(\alpha)$, pois $\zeta^i \in K\ \forall\ i = 1, \ldots, n$ e assim $K(\alpha)$ é Galoisiana.

Seja $G(K(\alpha)/K)$, o grupo de Galois. Então

$$\sigma \in G(K(\alpha)/K) \ \Rightarrow \ (\sigma(\alpha))^n - a = \sigma(\alpha^n) - a = a - a = 0,$$

isto é, $\sigma(\alpha)$ é uma raiz de $x^n - a$. Se $\sigma(\alpha) = \omega_\sigma \alpha$, $\omega_\sigma^n \alpha^n - a = 0$ como $\alpha^n = a$, $\omega_\sigma^n = 1$, isto é ω_σ é uma raiz n-ésima da unidade.

Uma aplicação φ que leva $\sigma \mapsto \omega_\sigma$ é um homomorfismo de $G(K(\alpha)/K)$ no grupo das raízes n-ésimas da unidade, que é cíclico. Como φ é injetiva, $\varphi(G(K(\alpha)/K))$ é subgrupo de um grupo cíclico de ordem d, com d divisor de n. Se σ é o gerador de $G(K(\alpha)/K)$, então ω_σ é a raiz d-ésima primitiva da unidade. No que temos,

$$\sigma(\alpha^d) = (\sigma(\alpha))^d = (\omega_\sigma \alpha)^d = \alpha^d$$

isto é α^d é fixo por σ e portanto fixo por $G(K(\alpha)/K)$. Logo $\alpha^d \in K$.

■

Teorema 2.8.9 (Forma aditiva do Teorema 90 de Hilbert)**.** *Sejam K um corpo, E uma extensão cíclica sobre K, $[E : K] = n$. Seja σ o gerador de $G(E/K)$ e $\beta \in E$. O traço $\mathrm{Tr}_K^E(\beta)$ é igual a 0, se e só se, existir $\alpha \in E$ tal que $\beta = \alpha - \sigma(\alpha)$.*

Demonstração. ($\Leftarrow$) Se $\beta = \alpha - \sigma(\alpha)$, então

$$\mathrm{Tr}_K^E(\beta) = [E : K]_i \sum_{i}^{n} \sigma_j(\beta),$$

$[E : K]_i = 1$ pois E é Galoisiana, $\sigma_j \in G(E/K)$ $\forall\, j \in \{1, \dots, n\}$. Considere

$$\sigma_1 = \sigma,\ \sigma_2 = \sigma^2, \dots, \sigma_{n+1} = \sigma_1$$

$$\begin{aligned}
\mathrm{Tr}_K^E(\beta) &= \sigma_1(\beta)+\sigma_2(\beta)+\ldots+\sigma_n(\beta)\\
&= \sigma_1(\alpha-\sigma(\alpha))+\sigma_2(\alpha-\sigma(\alpha))+\ldots+\sigma_n(\alpha-\sigma(\alpha))\\
&= \sigma_1(\alpha)-\sigma_2(\alpha)+\sigma_2(\alpha)-\sigma_3(\alpha)+\ldots+\sigma_n(\alpha)-\sigma_1(\alpha)=0.
\end{aligned}$$

($\Rightarrow$) Se $\mathrm{Tr}_K^E(\beta)=0$, considere $\theta\in K$ tal que $\mathrm{Tr}_K^E(\theta)\neq 0$, a existência de tal elemento θ está garantida pela independência linear dos elementos de $G(E/K)$, como vimos no Teorema 2.8.6. Seja α elemento de E tal que

$$\alpha=\frac{1}{\mathrm{Tr}(\theta)}[\beta\sigma(\theta)+(\beta+\sigma(\beta))\sigma^2(\theta)+\ldots+(\beta+\sigma(\beta)+\ldots+\sigma^{n-2}(\beta))\cdot\sigma^{n-1}(\theta)].$$

Como σ é homomorfismo de corpos e $G(E/K)$ é cíclico, $\sigma(\mathrm{Tr}(\theta))=\mathrm{Tr}(\theta)$, e vale

$$\sigma(\alpha)=\frac{1}{\mathrm{Tr}(\theta)}[\sigma(\beta)\sigma^2(\theta)+\sigma(\beta)\sigma^3(\theta)+\sigma^2(\beta)\sigma^3(\theta)+\ldots+$$

$$+\sigma(\beta)\sigma^n(\theta)+\sigma^2(\beta)\sigma^n(\theta)+\ldots+\sigma^{n-1}(\beta)\sigma^n(\theta)].$$

Logo $\alpha-\sigma(\alpha)=\beta-\frac{\sigma^n(\theta)}{\mathrm{Tr}(\theta)}\cdot\mathrm{Tr}(\beta)$ e então vale $\beta=\alpha-\sigma(\alpha)$, já que $\mathrm{Tr}(\beta)=0$ por hipótese.

■

O seguinte teorema assemelha-se ao Teorema 4.1.2 e ambos podem ter em suas demonstrações elementos das formas multiplicativa e aditiva do Teorema 90 de Hilbert. Além disso, mostra a possibilidade de outra raiz de polinômio em corpos de característica $p>0$. Esse teorema será essencial quando trabalharmos resultados de Cohomologia Galoisiana e da Teoria de Kummer nos casos em que consideraremos os grupos aditivos obtidos a partir do corpo base.

Teorema 2.8.10 (Artin-Schreier)**.** *Seja K um corpo de característica p.*

i) Seja E uma extensão cíclica de K de grau p. Então existe $\alpha\in E$ tal que $E=K(\alpha)$ e α satisfaz a equação $x^p-x-a=0$ para algum $a\in K$.

ii) Por outro lado, dado $a\in K$, se o polinômio $f(x)=x^p-x-a$ tem uma raiz em

K, todas as raízes estão em K. Se $f(x)$ não tem raiz em K, é irredutível e, nesse caso, se α é uma raiz, então $K(\alpha)$ é cíclico de grau p sobre K.

Demonstração. Para provar o item $i)$, novamente iremos considerar

$$\sigma_1 = \sigma,\ \sigma_2 = \sigma \circ \sigma, \ldots,\ \sigma_p = \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{p\ vezes},$$

onde σ é um gerador do grupo de galois $G(E/K)$.

Seja $-1 \in K$, então $\sigma_i(-1) = -1$, $\forall\ i \in \{1, \ldots, p\}$ e, por conseguinte,

$$\mathrm{Tr}_K^E(-1) = \sigma_1(-1) + \sigma_2(-1) + \ldots + \sigma_p(-1) = p \cdot (-1) = 0.$$

Pelo Teorema (2.8.9), temos que $\exists\ \alpha \in E$ tal que $-1 = \alpha - \sigma(\alpha)$, ou seja, $\sigma(\alpha) = \alpha + 1$. Logo, temos que

$$\sigma_i(\alpha) = \sigma_{i-1}(\alpha+1) = \sigma_{i-1}(\alpha) + 1 = \sigma_{i-2}(\alpha+1) + 1 = \sigma_{i-2}(\alpha) + 2 = \ldots = \alpha + i \quad \forall\ i \in\ \{1,\ldots,p\}$$

Como α tem p conjugações, isto é, $\sigma_1(\alpha)$,$\sigma_2(\alpha)$,$\ldots$,$\sigma_p(\alpha)$, que são raízes do polinômio minimal de α, logo $[K(\alpha) : K] \geq p$, como $[E : K] = p$ e $\alpha \in E$, $K(\alpha) = E$.

Além disso, temos que

$$\begin{aligned} \sigma(\alpha^p - \alpha) &= \sigma(\alpha^p) - \sigma(\alpha) \\ &= \sigma(\alpha)^p - \sigma(\alpha) \\ &= (\alpha+1)^p - (\alpha+1) \\ &= \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha \end{aligned}$$

Mas se $\alpha^p - \alpha$ é fixo por σ, temos que $(\alpha^p - \alpha) \in K$. Tomemos $a = \alpha^p - \alpha$ e concluímos que α é a raiz de

$$x^p - x - a = 0,$$

concluindo o item i).

Para provar o item ii) tome $a \in K$ e considere α uma raiz de $f(x)$, então

$$\alpha^p - \alpha - a = 0$$

e portanto

$$(\alpha+i)^p - (\alpha+i) - a = \alpha^p + i^p - \alpha - i - a = (\alpha^p - \alpha - a) + i^p - i = 0, \forall\, i \in \{1, 2, ..., p-1\}.$$

Logo $f(x)$ tem p raízes distintas.

Devemos lembrar que todo corpo de característica p possui uma cópia de $\mathbb{F}_p$ e os elementos inteiros $i = 1, 2, ..., p$ em K são vistos como elementos de $\mathbb{F}_p$, por isso $i^p = i$ para todo i. Observemos também que, se alguma raiz de $f(x)$ está em K, então todas as outras raízes também estarão, pois $\alpha + i \in K \Rightarrow \alpha \in K$ para todo $i \in K$.

Supondo que nenhuma das raízes estão em K, então o polinômio $f(x)$ é irredutível. De fato, se $f(x)$ não for irredutível poderíamos escrever $f(x) = g(x)h(x)$, com $g(x)$, $h(x)$ $\in K[x]$ e o grau de $g(x)$ é igual a um d com $1 \leq d < p$. Temos ainda que $g(x)$ é da forma

$$g(x) = (x - (\alpha + i_1))(x - (\alpha + i_2)) \dots (x - (\alpha + i_d))$$

com $i_j = 1, 2, \dots, p$ e $j = 1, 2, \dots, d$ e portanto $g(x)$ terá o termo x^{d-1} com coeficiente igual a

$$\sum_{j=1}^{d} (-(\alpha + i_j)) = -d\alpha + l$$

para algum $l \in \mathbb{F}_p$. Como $d \neq 0$ em K e $(-d\alpha + l) \in K$, temos que $\alpha \in K$, o que é um absurdo. Logo $f(x)$ é irredutível.

Agora, adjuntando α a K, temos que $K(\alpha)$ contém todas as raízes de $f(x)$, logo $K(\alpha)$

é normal e galoisiana. Seja $G(K(\alpha)/K)$ o grupo de Galois correspondente. Então $\sigma(\alpha) = \sigma(\alpha + 1)$ para algum $\sigma \in G(K(\alpha)/K)$, pois $\alpha + 1$ também é raiz de $f(x)$, assim

$$\sigma_i(\alpha) = \sigma_{i-1}(\alpha + 1) = \sigma_{i-1}(\alpha) + 1 = \ldots = \alpha + i$$

$\forall\, i \in \{1, \ldots, p\}$, ou seja, $G(K(\alpha)/K)$ é gerado por σ e portanto $K(\alpha)$ é extensão cíclica.

$\blacksquare$

Capítulo 3

Cohomologia Galoisiana

3.1 Cohomologia Galoisiana

Dado um grupo G, um *G-módulo* à esquerda é um grupo abeliano A, tal que para cada $\sigma \in G$ e $a \in A$ existe uma única correspondência $\sigma(a) \in A$ que cumpre:

i) $\sigma(a+b) = \sigma(a) + \sigma(b) \ \forall \ a, \ b \ \in \ A$

ii) $(\sigma\tau)(a) = \sigma(\tau(a)) \ \forall \ \sigma, \ \tau \ \in \ G$ e $a \ \in \ A$

Na definição acima, optamos por escrever o grupo A com a operação adição.

Sejam A um G-módulo e n um inteiro não-negativo. Uma *n-cocadeia de G sobre A* é uma função f de n variáveis de G em A se $n > 0$, isto é $f : G^n \to A$, e é um elemento de A se $n = 0$.

Denotamos por $C^n(G,A)$ ao conjunto formado por n-cocadeias de G em A. Podemos verificar que o conjunto $C^n(G,A)$ forma um grupo com a operação adição. Observe que este grupo também é abeliano.

Podemos ainda definir uma $(n+1)$-cocadeia a partir de uma n-cocadeia da seguinte maneira:

Dada uma $f \in C^n(G,A)$, tomamos

$$\delta f(\sigma_1,...,\sigma_{n+1}) := \sigma_1 f(\sigma_2,...,\sigma_{n+1}) + \sum_{i=1}^{n}(-1)^i f(\sigma_1,...,\sigma_i\sigma_{i+1},...,\sigma_{n+1}) +$$
$$+(-1)^{n+1} f(\sigma_1,...,\sigma_n).$$

Assim definida, δ é um homomorfismo de $C^n(G,A)$ em $C^{n+1}(G,A)$ como consequência de que $(f+g)(\bullet) = f(\bullet) + g(\bullet)$ e também da propriedade i) de G-módulos.

Verifica-se também que $\delta\delta f = 0$ com $f \in C^n(G,A)$. De fato,

$$\delta f(\sigma_1,...,\sigma_{n+1}) = \sigma_1 f(\sigma_2,...,\sigma_{n+1}) + \sum_{i=1}^{n}(-1)^i f(\sigma_1,...,\sigma_i\sigma_{i+1},...,\sigma_{n+1}) +$$
$$+(-1)^{n+1} f(\sigma_1,...,\sigma_n),$$

uma soma com $n+2$ termos e portanto $\delta\delta f$ é uma soma com $(n+2)(n+3)$ termos, isto é, tem um número par de termos somados para todo n natural e isso é importante para nos certificarmos que os termos irão se anular. Agora,

$$\delta\delta f(\sigma_1,...,\sigma_{n+2}) = \sigma_1 \delta f(\sigma_2,...,\sigma_n+2) + \sum_{i=1}^{n+1}(-1)^i \delta f(\sigma_1,...,\sigma_i\sigma_{i+1},...,\sigma_{n+2}) +$$
$$+(-1)^{n+2}\delta f(\sigma_1,...,\sigma_{n+1})$$

$$\Rightarrow \delta\delta f(\sigma_1,...,\sigma_{n+2}) = \sigma_1 \delta f(\sigma_2,...,\sigma_n+2) + (-1)^1 \delta f(\sigma_1\sigma_2,...,\sigma_{n+2}) +$$
$$+(-1)^2 \delta f(\sigma_1,\sigma_2\sigma_3,...,\sigma_{n+2}) + ... + (-1)^{n+1}\delta f(\sigma_1,...,\sigma_{n+1}\sigma_{n+2}) +$$
$$+(-1)^{n+2}\delta f(\sigma_1,...,\sigma_{n+1})$$

e se substituirmos cada δf acima, teremos

$$\delta\delta f(\sigma_1,...,\sigma_{n+2}) = \sigma_1[\sigma_2 f(\sigma_3,...,\sigma_{n+2}) + (-1)^1 f(\sigma_2\sigma_3,...,\sigma_{n+2}) + ...+$$

$$+(-1)^n f(\sigma_2, ..., \sigma_{n+1}\sigma_{n+2}) + (-1)^{n+1} f(\sigma_2, ..., \sigma_{n+1})] + (-1)^1[\sigma_1\sigma_2 f(\sigma_3, ..., \sigma_{n+2})+$$

$$+(-1)^1 f(\sigma_1\sigma_2\sigma_3, ..., \sigma_{n+2}) + ... + (-1)^n f(\sigma_1\sigma_2, \sigma_3, ..., \sigma_{n+1}\sigma_{n+2})+$$

$$+(-1)^{n+1} f(\sigma_1\sigma_2, \sigma_3, ..., \sigma_{n+1})]+(-1)^2[\sigma_1 f(\sigma_2\sigma_3, ..., \sigma_{n+2})+(-1)^1 f(\sigma_1\sigma_2\sigma_3, ..., \sigma_{n+2})+$$

$$+... + (-1)^n f(\sigma_1,\sigma_2\sigma_3,\sigma_4, ..., \sigma_{n+1}\sigma_{n+2}) + (-1)^{n+1} f(\sigma_1, \sigma_2\sigma_3, \sigma_4..., \sigma_{n+1})] + ...+$$

$$+(-1)^{n+1}[\sigma_1 f(\sigma_2, ..., \sigma_{n+1}\sigma_{n+2}) + (-1)^1 f(\sigma_1\sigma_2, \sigma_3, ..., \sigma_{n+1}\sigma_{n+2})+$$

$$+(-1)^2 f(\sigma_1,\sigma_2\sigma_3, \sigma_4, ..., \sigma_{n+1}\sigma_{n+2}) + ... + (-1)^n f(\sigma_1, ..., \sigma_n\sigma_{n+1}\sigma_{n+2})+$$

$$+(-1)^{n+1} f(\sigma_1, ...,\sigma_n)] + (-1)^{n+2}[\sigma_1 f(\sigma_2, ..., \sigma_{n+1}) + (-1)^1 f(\sigma_1\sigma_2, \sigma_3,...,\sigma_{n+1})+$$

$$+(-1)^2 f(\sigma_1, \sigma_2\sigma_3, \sigma_4, ..., \sigma_{n+1}) + ... + (-1)^n f(\sigma_1, ..., \sigma_n\sigma_{n+1}) + (-1)^{n+1} f(\sigma_1, ..., \sigma_n)]$$

Os resultados obtidos em cada par de colchetes acima podem ser organizados em $n+3$ linhas de uma matriz. Observe ainda que cada linha dessas possuirá $n+2$ fatores, dos quais podemos organizar em colunas. Dessa forma, teremos uma matriz como no anexo 1. Se denotarmos tal matriz por $(a_{[i;j]})_{[n+3;n+2]}$ com linhas representadas por $i \in \{1, ..., n+3\}$ e colunas representadas por $j \in \{1, ..., n+2\}$, então são inversos os elementos:

$$\begin{gathered}
a_{[1;1]} \text{ e } a_{[2;1]},\ a_{[2;2]} \text{ e } a_{[3;2]} \ \cdots\ a_{[n+2;n+2]} \text{ e } a_{[n+3;n+2]};\\
a_{[1;2]} \text{ e } a_{[3;1]},\ a_{[2;3]} \text{ e } a_{[4;2]} \ \ldots a_{[n+1;n+2]} \text{ e } a_{[n+3;n+1]};\\
\vdots\\
a_{[1;n+2]} \text{ e } a_{[n+3;1]}.
\end{gathered}$$

E portanto a soma dos termos se reduz a 0.

Sejam $Z^n(G,A) := \{f \in C^n(G,A) \mid \delta f = 0\}$, $B^n(G,A) := \{\delta f \mid f \in C^{n-1}(G,A)\}$ para $(n > 0)$, $B^0(G,A) := 0$.

Chamamos $f \in Z^n(G,A)$ de *n-cociclo* e $\delta f \in B^n(G,A)$ de *n-cobordo*.

Agora, pelo fato de δ ser homomorfismo, temos que $Z^n(G,A)$ é um subgrupo de $C^n(G,A)$, pois é núcleo de δ aplicado em $C^n(G,A)$ e $B^n(G,A)$ é um subgrupo de $C^n(G,A)$, pois é imagem de δ aplicado em $C^{n-1}(G,A)$. Mas como $\delta\delta f = 0$, temos que $B^n(G,A) \subset Z^n(G,A)$.

Já que $C^n(G,A)$ é abeliano, seus subgrupos são normais e podemos definir o grupo quociente $H^n(G,A) = Z^n(G,A)/B^n(G,A)$ o qual chamamos de *n-ésimo Grupo de Cohomologia de G sobre A.*

Estamos especialmente interessados nos casos em que $n = 0$ e $n = 1$. Observe que, para $f \in Z^1(G,A)$, diante das definições acima, temos

$$\delta f(\sigma, \tau) = \sigma f(\tau) - f(\sigma\tau) + f(\sigma) = 0 \ \forall \ \sigma \ \tau \ \in \ G$$

$$\Rightarrow f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$$

Encontramos assim uma condição para os elementos de $Z^1(G,A)$ e chamamos de *homomorfismo cruzado* à função que cumpre tal condição. (Note que f homomorfismo cruzado implica $f(1) = 0$.)

Agora, para $g \in B^1(G,A)$ temos que $g = \delta f$ com $f \in C^0(G,A) = A$, isto é $f = a \in A$ e assim $g(\sigma) = \sigma a - a$, onde a notação σa representa a ação de σ em a. Por sua vez, chamamos a função que cumpre tal condição de *homomorfismo cruzado principal.*

Podemos também usar a seguinte notação para uma n-cocadeia: $\{\alpha_\sigma\}_{\sigma \in G}$, que equivale à imagem de uma função f como usamos acima, isto é, $f(\sigma) = \alpha_\sigma$.

Nesse caso, também podemos avaliar o G agindo em A ou, equivalentemente, podemos assumir um homomorfismo $G \to \mathrm{Aut}(A)$. (essa equivalência pode ser mostrada de forma análoga à demonstrada na observação 1.1.3).

E portanto um 1-cociclo de G em A será uma família de elementos $\{\alpha_\sigma\}_{\sigma \in G}$ com $\alpha_\sigma \in A$, satisfazendo a seguinte relação

$$\alpha_\sigma + \sigma\alpha_\tau = \alpha_{\sigma\tau} \ \forall \ \sigma, \ \tau \ \in G.$$

Se $\{\alpha_\sigma\}_{\sigma \in G}$ e $\{\beta_\sigma\}_{\sigma \in G}$ são 1-cociclos, então podemos usar a soma em $Z^1(G,A)$ da seguinte maneira $\{\alpha_\sigma\}_{\sigma \in G} + \{\beta_\sigma\}_{\sigma \in G} = \{\alpha_\sigma + \beta_\sigma\}_{\sigma \in G}$.

Similarmente, 1-cobordo de G em A é uma família de elementos $\{\alpha_\sigma\}_{\sigma \in G}$ tal que para cada α_σ, $\exists \ \beta \ \in A$ para o qual $\alpha_\sigma = \sigma\beta - \beta$. Ou seja, α_σ é a imagem de σ por uma aplicação $f : G \to A$ que satisfaz $f(\sigma) = \sigma\beta - \beta$ para algum $\beta \ \in \ A$.

Observação 3.1.1. *Suponha que G é um grupo cíclico e finito e A um G-módulo. Seja*

$$\begin{array}{rccc} \mathrm{Tr}_G : & A & \to & A \\ & a & \mapsto & \sum\limits_{\sigma \in G} \sigma a \end{array}$$

Seja γ o gerador de G e considere o subconjunto

$$(1-\gamma)A := \{a \in A \mid a = b - \gamma b \text{ para algum } b \in A\}.$$

É fácil ver que $(1-\gamma)A$ é um subgrupo de A e como A é abeliano, é subgrupo normal. Então temos o seguinte isomorfismo

$$\frac{\ker \mathrm{Tr}_G}{(1-\gamma)A} \simeq H^1(G, A)$$

De fato, se $\{\alpha_\sigma\}_{\sigma \in G} \ \in \ Z^1(G,A)$ então α_γ é um elemento de $\ker \mathrm{Tr}_G$*, pois*

$$\alpha_{\gamma^2} = \alpha_{\gamma\gamma} = \gamma\alpha_\gamma + \alpha_\gamma$$

$$\alpha_{\gamma^3} = \alpha_{\gamma^2\gamma} = \gamma^2\alpha_\gamma + \alpha_{\gamma^2} = \gamma^2\alpha_\gamma + \gamma\alpha_\gamma + \alpha_\gamma$$

$$\vdots$$

$$\alpha_{\gamma^n} = \alpha_{\gamma^{n-1}\gamma} = \gamma^{n-1}\alpha_\gamma + ... + \alpha_\gamma.$$

Isto é, $\alpha_{\gamma^n} = \mathrm{Tr}_G(\alpha_\gamma)$, *mas* $\alpha_{\gamma^n} = \alpha_{\mathrm{Id}} = 0$.

Agora, $\forall\ a \in \mathrm{Ker\ Tr}_G$, $\alpha_{\gamma^i} = \gamma^{i-1}a + \gamma^{i-2}a + ... + \gamma a + a$ *define um elemento de* $Z^1(G,A)$. *Temos portanto* $Z^1(G,A) \simeq \mathrm{Ker\ Tr}_G$.

Basta verificar que $B^1(G,A) \simeq (1-\gamma)A$, *mas para* $a \in (1-\gamma)A$, $\exists\ b \in A$ *tal que* $a = b - \gamma b$ *e portanto* $\alpha_\gamma = -b + \gamma b$ *vai definir um elemento de* $B^1(G,A)$. *Reciprocamente para um elemento* $\{\alpha_{\gamma^i}\}_{i \in \{1,...,n\}} \in B^1(G,A)$ *tomamos* α_γ, *que obviamente pertence à* $(1-\gamma)A$.

Proposição 3.1.2. *Seja* A *um* G*-módulo. Suponha que dado* $a \in A$ *temos* $\sigma a = a$, $\forall\ \sigma \in G$ *ou, dito de outra maneira, suponha que* G *age trivialmente sobre* A. *Então* $H^1(G,A) \cong Z^1(G,A) = \mathrm{Hom}(G,A)$.

Demonstração. Basta observar que $\forall\ g \in B^1(G,A)$, temos $g(\sigma) = \sigma a - a$, mas $\sigma a = a$, então g é identicamente nulo e portanto $Z^1(G,A)/B^1(G,A) = Z^1(G,A)$. Agora, $\forall\ f \in Z^1(G,A)$ temos $f(1) = 0$ e ainda $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$. Como $\sigma f(\tau) = f(\tau)$, vale $f(\sigma\tau) = f(\tau) + f(\sigma)$, característica de todo homomorfismo de grupos de G em A. ■

Antes do próximo resultado, observe que dada uma extensão galoisiana de corpos E sobre K, o grupo de galois $G(E/K)$ age cononicamente nos grupos E^* ($E \setminus \{0\}$, grupo com a multiplicação) e E^+ (E visto como grupo, com a adição).

Teorema 3.1.3. *Seja* E/K *uma extensão galoisiana finita com grupo de galois* $G = G(E/K)$. *Então, pelas ações canônicas de* G *nos grupos* E^* *e* E^+ *nós temos, respectivamente,* $H^1(G, E^*) = 1$ *e* $H^1(G, E^+) = 0$. *Em outras palavras, o primeiro grupo de cohomologia é trivial em ambos os casos.*

Demonstração. Seja $\{\alpha_\sigma\}_{\forall \sigma \in G}$ um 1-cociclo de G em E^*, isto é, $\{\alpha_\sigma\}_{\forall\sigma\in G} \in Z^1(G, E^*)$.

O cociclo multiplicativo nos dá a seguinte relação:

$$\alpha_\sigma \alpha_\tau^\sigma = \alpha_{\sigma\tau}$$

Nesta relação, $\alpha_\sigma = f(\sigma)$, com f homomorfismo cruzado e $\alpha_\tau^\sigma = \sigma\alpha_\tau$ (σ agindo em α_τ), ou seja, $\alpha_\tau^\sigma = \sigma f(\tau)$. Observe que os elementos de G comportam-se como expoentes nos elementos de E^* ao considerarmos $(\sigma \circ \tau)(\alpha) = \alpha^{\tau\sigma} = (\alpha^\tau)^\sigma$.

Vamos agora considerar os elementos de G como caráteres distintos de E^* em E^* e, pela independência linear desses elementos, garantida pelo Teorema 2.8.6, vai existir um elemento $\theta \in E^*$ tal que,

$$\sum_{\tau \in G} \alpha_\tau \tau(\theta) = \beta \neq 0.$$

Então $\sigma(\beta) = \sum\limits_{\tau \in G} \sigma(\alpha_\tau \tau(\theta))$, $\sigma \in G$ qualquer.

$$\Rightarrow \sigma(\beta) = \sum_{\tau \in G} \alpha_\tau^\sigma \sigma \circ \tau(\theta) = \sum_{\tau \in G} \alpha_\tau^\sigma \theta^{\tau\sigma} = \sum_{\tau \in G} \alpha_\sigma^{-1} \alpha_\sigma \tau \theta^{\tau\sigma} = \alpha_\sigma^{-1} \sum_{\tau \in G} \alpha_\sigma \tau \theta^{\tau\sigma}.$$

Observe que enquanto τ percorre todo o G, $\sigma\tau$ também percorre, portanto temos $\sigma(\beta) = \alpha_\sigma^{-1}\beta$, ou seja, $\exists\ \beta \in E^*$ tal que $\alpha_\sigma^{-1} = \sigma(\beta)\beta^{-1}$ $\forall\ \sigma \in G$

$$\Rightarrow \alpha_\sigma^{-1} \in B^1(G,E^*) \Rightarrow \alpha_\sigma \in B^1(G,E^*).$$

Concluímos daí que $H^1(G,E^*) = 1$.

Analogamente, para a forma aditiva, tomamos θ tal que $\mathrm{Tr}(\theta) = \sum\limits_{\tau \in \mathrm{G}} \tau(\theta) \neq 0$ e fazemos $\beta = \frac{1}{\mathrm{Tr}(\theta)} \sum\limits_{\tau \in G} \alpha_\tau \tau(\theta) \Rightarrow \sigma(\beta) = \sigma(\mathrm{Tr}(\theta)^{-1}) \sum\limits_{\tau \in \mathrm{G}} \sigma(\alpha_\tau)\sigma(\tau(\theta))$.

Como $\alpha_\sigma + \sigma(\alpha_\tau) = \alpha_{\sigma\tau}$, temos $\sigma(\alpha_\tau) = \alpha_\sigma\tau - \alpha_\sigma$.

$$\begin{aligned}
\Rightarrow \sigma(\beta) &= \sigma(\mathrm{Tr}(\theta)^{-1})\sum_{\tau\in \mathrm{G}}(\alpha_{\sigma\tau} - \alpha_\sigma)(\sigma\circ\tau)(\theta)) \\
&= \sigma(\mathrm{Tr}(\theta)^{-1})(\sum_{\tau\in \mathrm{G}}\alpha_{\sigma\tau}(\sigma\circ\tau)(\theta) - \sum_{\tau\in \mathrm{G}}\alpha_\sigma(\sigma\circ\tau)(\theta)) \\
&= \sigma(\mathrm{Tr}(\theta)^{-1})(\sum_{\tau\in \mathrm{G}}\alpha_{\sigma\tau}(\sigma\circ\tau)(\theta) - \alpha_\sigma\sum_{\tau\in \mathrm{G}}(\sigma\circ\tau)(\theta)) \\
&= \beta - \alpha_\sigma \mathrm{Tr}(\theta)\sigma(\mathrm{Tr}(\sigma)^{-1}) \\
&= \beta - \alpha_\sigma
\end{aligned}$$

Usamos acima o fato de que $\sigma(\mathrm{Tr}\theta) = \mathrm{Tr}\theta$ e $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1}$, pois σ é automorfismo de anéis e portanto preserva soma e produto.

Logo, $Z^1(G,E^+) = B^1(G,E^+) \Rightarrow H^1(G,E^+) = 0$.

∎

Lema 3.1.4. *(Lema de Sah) Seja G um grupo e seja E um G-módulo. Seja τ um elemento pertencente ao centro de G. Então todo elemento de $H^1(G,E)$ é levado ao zero pela composição da aplicação $\Psi : E \to E$ tal que $x \mapsto \tau x - x$ em E. Em particular, se esta aplicação é um automorf ismo de E, então $H^1(G,E) = 0$.*

Demonstração. Seja f um 1-cociclo de G em E. Como τ está no centro de G, então

$$\begin{aligned}
f(\sigma) = f(\tau\sigma\tau^{-1}) &= f(\tau) + \tau f(\sigma\tau^{-1}) \\
&= f(\tau) + \tau(f(\sigma) + \sigma f(\tau^{-1}))
\end{aligned}$$

Portanto,

$$\begin{aligned}
\tau f(\sigma) - f(\sigma) &= -\tau\sigma f(\tau^{-1}) - f(\tau) \\
&= -\sigma\tau f(\tau^{-1}) - f(\tau) \\
\Rightarrow \Psi\circ f(\sigma) &= \tau f(\sigma) - f(\sigma) = -\sigma\tau f(\tau^{-1}) - f(\tau)
\end{aligned}$$

Mas $f(1) = 0$, e vale

$$\begin{aligned} f(1) = f(\tau\tau^{-1}) &= 0 \\ f(\tau) + \tau f(\tau^{-1}) &= 0 \\ \Rightarrow f(\tau) &= -\tau f(\tau^{-1}) \end{aligned}$$

E assim temos

$$\Psi \circ f(\sigma) = \sigma f(\tau) - f(\tau), \ \forall \, \sigma \ \in \ G$$

Concluímos que $\Psi \circ f$ está em $B^1(G,E)$.

Agora, se Ψ é automorfismo, implica que todo elemento de E pode ser escrito como $\tau x - x$ e assim $H^1(G,E) = 0$.

■

Capítulo 4

Teoria de Kummer

4.1 Extensões de Kummer

Consideremos agora o corpo de decomposição de $f(x) = x^p - a$ sobre um corpo K, com p primo. Assumiremos que o corpo K está contido em $\mathbb{C}$ e que K contém raiz p-ésima primitiva da unidade ζ_p. Seja α uma particular raiz p-ésima de a, então as raízes de $f(x)$ são

$$\alpha,\, \zeta_p\alpha,\, \zeta_p^2\alpha, \ldots,\, \zeta_p^{p-1}\alpha, \text{ pois } (\zeta_p^n)^p = 1 \;\; \forall \;\; n.$$

Portanto o corpo de decomposição de $f(x)$ sobre K é gerado por uma única raiz α, ou seja, é o corpo $F = K(\alpha)$.

Proposição 4.1.1. *Seja K um subcorpo de $\mathbb{C}$ que contém a raiz p-ésima primitiva da unidade ζ_p e seja* **a** *um elemento de K que não é uma potência de p em K. Então o corpo de decomposição de $f(x) = x^p - \mathbf{a}$ tem grau p sobre K, e seu grupo de Galois é cíclico de ordem p.*

Demonstração. Seja F o corpo de decomposição de f sobre K e seja $\alpha \in F/K$ uma das raízes de f. Então existe um automorfismo $\psi \in G(F/K)$ tal que $\psi(\alpha) \neq \alpha$. Uma vez que as raízes de f são da forma $\zeta_p^i\alpha$, com $i \in \{0, \ldots, p-1\}$, $\psi(\alpha) = \zeta_p^r\alpha$, para algum $r \neq 0$, pois ψ deve levar raízes de f em raízes de f. Assim os automorfismos de $G(F/K)$ são encontrados da seguinte maneira:

$$\psi(\zeta_p^i \alpha) = \psi(\zeta_p^i) \cdot \psi(\alpha) = \psi(\zeta_p)^i \psi(\alpha),$$

como $\psi(\zeta_p) = \zeta_p$ pois $\zeta_p \in K$, temos

$$\psi(\zeta_p^i \alpha) = \psi(\zeta_p)^i \psi(\alpha) = \zeta_p^i \psi(\alpha) = \zeta_p^{i+r} \alpha$$

e ainda

$$\psi^2(\alpha) = \psi(\psi(\alpha)) = \psi(\zeta^r \alpha) = \psi_p^r \psi(\alpha) = \zeta_p^{2r} \alpha$$

e logo

$$\psi^j(\alpha) = \zeta_p^{jr} \alpha, \text{ para } j \in \{0, 1, \ldots, p-1\}.$$

Como ζ_p é raiz p-ésima primitiva da unidade, a menor potência do automorfismo ψ que fixa α é ψ^p. Logo, ψ tem ordem pelo menos p em $G(F/K)$. Por outro lado, α é um dos elementos da base de F sobre K, e $f(\alpha) = 0$, logo $[F : K] \leq p$, pois f tem grau p. Como $G(F/K)$ tem no mínimo p elementos, $[F : K] = p$, $f(x)$ é irredutível sobre K e $G(F/K)$ é cíclico de ordem p.

■

Teorema 4.1.2. *Sejam K um subcorpo de $\mathbb{C}$, $\zeta_p \in \mathbb{C} \setminus K$ uma raiz p-ésima primitiva da unidade e F uma extensão galoisiana sobre K de grau p. Então obtemos F pela adjunção, ao corpo K, de uma p-ésima raiz.*

Demonstração. Sendo $G(F/K)$ um grupo de ordem prima, é cíclico. Dado $\phi \in G(F/K)$, $\phi \neq \mathrm{Id}$, então ϕ gera $G(F/K)$. Se tomarmos F como um espaço vetorial sobre K, temos que ϕ é um operador linear de F, pois

$$\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta) \text{ e } \phi(c \cdot \alpha) = c\phi(\alpha) \ \forall\ \alpha, \beta \in F \ e \ c \in K.$$

Como $G(F/K)$ é cíclico de ordem p, $\phi^p = \mathrm{Id}$. Além disso, tomando λ um autovalor de ϕ, então $\lambda^p = 1$, isto é, λ é uma potência de ζ_p. Os autovalores pertencem a K e pelo menos um deles é diferente de 1. De fato, seja T a matriz correspondente ao operador linear ϕ, então temos que $T^p = \mathrm{Id}$. Assim, temos que T é diagonalizável e portanto existe uma matriz diagonal A semelhante a T. Como $T \neq \mathrm{Id}$, $A \neq \mathrm{Id}$ e assim alguma entrada da diagonal de A é diferente de 1.

Escolhemos α autovetor com autovalor $\zeta_p^i \neq 1$. então $\phi(\alpha) = \zeta_p^i\alpha$ e portanto

$$\phi(\alpha^p) = \phi(\alpha)^p = (\zeta_p^i\alpha)^p = (\zeta_p^i)^p\alpha^p = \alpha^p,$$

logo ϕ fixa α^p. Como ϕ gera $G(F/K)$, o elemento $\alpha^p \in F_{G(F/K)}$ (Corpo fixo de $G(F/K)$ em F) que é o próprio K. Portanto α é um elemento de F cuja p-ésima potência está em K. Já que $\phi(\alpha) = \zeta_p^i\alpha$ e $\zeta_p^i \notin K$, então $\phi(\alpha) \neq \alpha$ e o elemento $\alpha \notin K$. Como $[F : K]$ é primo, α gera F, ou seja $F = K(\alpha)$.

■

Definição 4.1.3. *Se K é um corpo que contem as n-ésimas raízes da unidade, então a extensão F, obtida pela adjunção ao corpo base K de uma raiz n-ésima ou de várias raízes n-ésimas de elementos de K^*, é frequentemente chamada de* extensão de Kummer.

Vamos apresentar agora a teoria mais geral, que inclui extensões de corpos de característica p.

4.2 Teoria Abeliana

Nesta seção apresentaremos os Teoremas de Correspondência. Duas provas distintas serão exibidas para a forma multiplicativa, a primeira não depende dos resultados do Capítulo de Cohomologia.

Em ambas as subseções, consideramos o fato de que, se E/K é uma extensão galoisiana e $G(E/K)$ é o seu grupo de galois, E/K *tem expoente* m se $G(E/K)$ tem expoente m (ver definição no início da seção 1.2).

Vamos considerar m coprimo com a característica de K e que a m-ésima raiz primitiva de unidade está em K. Denotamos por μ_m o grupo das m-ésimas raízes da unidade e, nesse caso, $\mu_m \subseteq K$.

Se $a \in K$, $a^{1/m}$ ou $\sqrt[m]{a}$ fará sentido se $\alpha^m = a$ para $\alpha \in E$ e assim também vale $(\xi\alpha)^m = a$, com ξ raiz m-ésima da unidade. Nesse caso, $K(\alpha) = K(a^{1/m})$. Denotamos também como K^{*m} ao subgrupo de K^* formado por todas as m-ésimas potências de elementos não nulos de K. Isto é, $K^{*m} = \mathrm{Im}\phi$ onde ϕ é homomorfismo tal que $\phi : K^* \longrightarrow K^*$ com $x \mapsto x^m$.

Se B é subgrupo de K^* contendo K^{*m}, denotamos por $K(B^{1/m})$ ou K_B a extensão composta de todas as extensões $K(a^{1/m})$ com $a \in B$ (veja Definição 2.6.13). Dessa forma, K_B é unicamente determinada pelo subgrupo B.

4.2.1 Teorema de Correspondência, forma multiplicativa

Com as notações acima, considere $a \in B$ e $\alpha^m = a$, então $x^m - a$ é um polinômio de $K[x]$ que pode ser decomposto em fatores lineares em $K(a^{1/m})$, pois as raízes m-ézimas da unidade estão em K, e portanto $K(a^{1/m})$ é uma extensão galoisiana sobre K. Já que isso vale para todo $a \in B$, todo elemento de K_B que está contido em alguma extensão $K(a^{1/m})$ será separável e seu polinômio minimal possuirá todas as raízes nesse corpo, pois extensão galoisiana também é normal. Mas todo elemento de K_B está contido em uma extensão finita que é gerada por elementos $a_1^{1/m}, \cdots, a_l^{1/m}$, com $a_i \in B$ para todo $i \in \{1, \cdots, l\}$.

Tal extensão, por sua vez, é corpo de decomposição do polinômio

$$(x^m - a_1).(x^m - a_2).\cdots.(x^m - a_l),$$

isto é, é galoisiana e portanto normal. Concluímos que todo elemento de K_B é separável e seu polinômio minimal tem todas suas raízes contidas nesse corpo, portanto K_B é extensão normal e separável, isto é, é extensão galoisiana.

Observe ainda que, se $\sigma \in G(K_B/K)$ e $\alpha^m = a \in B$, então $\sigma(\alpha) = \omega_\sigma \alpha$ onde ω_σ é m-ésima raiz da unidade, ou seja, $\omega_\sigma \in \mu_m \subset K^*$. A aplicação que leva σ em ω_σ é um homomorfismo de $G(K_B/K)$ em μ_m.

Além disso, tomando dois elementos σ e τ em $G(K_B/K)$, temos que $\sigma\tau(\alpha) = \omega_\sigma\omega_\tau\alpha = \omega_\tau\omega_\sigma\alpha$, pois K é corpo. Como os geradores de K_B são os elementos do tipo $\alpha = a^{1/m}$, concluímos que $G(K_B/K)$ é abeliano.

Como vimos, $\sigma(\alpha) = \omega_\sigma\alpha$, portanto podemos considerar o elemento ω_σ como $\sigma(\alpha)/\alpha$.

Verificamos que ω_σ não depende da m-ésima raiz de a, pois se α' é outra m-ésima raiz de a, $\omega_\sigma = \sigma(\alpha')/\alpha' = \sigma(\alpha)/\alpha$.

Podemos usar aqui a notação $\omega_\sigma = \langle \sigma, a \rangle$ e temos o emparelhamento (ver definição na seção 1.2):

$$\begin{array}{rcl} G(K_B/K) \times B & \to & \mu_m \\ (\sigma, a) & \mapsto & \langle \sigma, a \rangle \end{array}.$$

Nessa aplicação, se $a \in K^{*m}$, $\langle \sigma, a \rangle = 1$. De fato, pois $a \in K^{*m}$ implica que $a = b^m$ para algum $b \in K^*$. Como $\langle \sigma, a \rangle = \omega_\sigma$ e ω_σ não depende da raiz m-ésima de a escolhida, $\sigma(b) = \omega_\sigma b$, mas $b \in K$ implica que $\sigma(b) = b$, para todo σ em $G(K_B/K)$, portanto $\omega_\sigma = 1$.

No teorema abaixo vamos usar a notação $(B : K^{*m})$ para denotar a ordem do grupo quociente B/K^{*m}, isto é, $(B : K^{*m}) = |B/K^{*m}|$.

Teorema 4.2.1. *Seja K um corpo, $m \in \mathbb{Z}$, $m > 0$, $\mathrm{mdc}(m,p) = 1$, onde p é a característica de K, tal que K contém a m-ésima raiz primitiva da unidade. Seja ainda B subgrupo de K^* que contém K^{*m}, e considere $K_B = K(B^{1/m})$. Então temos:*

1) K_B é extensão galoisiana, abeliana de expoente m;

2) Seja $G = G(K_B/K)$. A aplicação

$$\begin{array}{rcl} G \times B & \rightarrow & \mu_m \\ (\sigma, a) & \mapsto & \langle \sigma, a \rangle = \omega_\sigma = \sigma(\alpha)/\alpha \end{array}$$

com $\alpha^m = a$, é um emparelhamento;

3) O núcleo à esquerda da aplicação dada no item 2) é 1 e o núcleo à direita é K^{*m}.

4) $[K_B : K] < \infty \Leftrightarrow (B : K^{*m}) < \infty$ e, nesse caso, $B/K^{*m} \simeq G^\wedge$ e vale $[K_B : K] = (B : K^{*m})$.

Demonstração. 1) Mostramos anteriormente que K_B é extensão galoisiana e abeliana. Vamos mostrar que tem expoente m.

Observe que K_B é composição de todas as extensões $K(a^{1/m})$ tal que $a \in B$ e $K(a^{1/m})/K$ é extensão galoisiana, logo normal. Pelo Teorema Fundamental da teoria de Galois temos $G(K_B/K)/G(K_B/K(a^{1/m})) \simeq G(K(a^{1/m})/K)$.

Agora, para $\sigma \in G(K(a^{1/m})/K)$ temos $\sigma^m = \mathrm{Id}$, pois $G(K(a^{1/m})/K)$ tem ordem m. Portanto, se $\sigma \in G(K_B/K)$, tomamos $\overline{\sigma^m} \in G(K_B/K)/G(K_B/K(a^{1/m}))$ e temos $\overline{\sigma^m} = \overline{\sigma}^m = \mathrm{Id}$. Assim, $\sigma^m \in G(K_B/K(a^{1/m}))$.

Logo, concluímos que $\sigma^m(a^{1/m}) = a^{1/m}\ \forall\ a \in B$. Mas os geradores de K_B são os elementos do tipo $a^{1/m}$, então $\sigma^m = \mathrm{Id}$. Como σ foi tomado arbitrariamente, obtemos que $G(K_B/K)$ tem expoente m.

2) Agora vamos mostrar que, de fato, temos homomorfismos nas aplicações $\sigma \mapsto \langle \sigma, a \rangle$ com a fixo, e $a \mapsto \langle \sigma, a \rangle$ com σ fixo.

$(\sigma \circ \tau, a) \mapsto \langle \sigma \circ \tau, a \rangle = \omega_{\sigma \circ \tau} = (\sigma \circ \tau)(\alpha)/\alpha = \sigma(\omega_\tau \alpha)/\alpha = \omega_\tau \omega_\sigma \alpha/\alpha = \omega_\tau \omega_\sigma = \langle \sigma, a \rangle \langle \tau, a \rangle$, onde $\alpha^m = a$.

Por outro lado, $(\sigma, ab) \mapsto \langle \sigma, ab \rangle = \omega_\sigma = \sigma(\beta)/\beta$, onde $\beta^m = ab$ e $\beta = \beta_1\beta_2$ com $\beta_1^m = a$ e $\beta_2^m = b$. Ou seja, $\sigma(\beta)/\beta = \sigma(\beta_1\beta_2)/\beta_1\beta_2 = \sigma(\beta_1)\sigma(\beta_2)/\beta_1\beta_2 = \xi_\sigma\beta_1\zeta_\sigma\beta_2/\beta_1\beta_2 = \xi_\sigma\zeta_\sigma = \langle \sigma, a \rangle \langle \sigma, b \rangle$, com ξ_σ e ζ_σ elementos de μ_m.

3) Para que $\sigma \in G(K_B/K)$ seja um elemento do núcleo à esquerda da aplicação dada no item 2) devemos ter $\langle \sigma, a \rangle = 1 \ \forall \ a \in B$, com $\alpha^m = a$. Isso significa que $\sigma(\alpha)/\alpha = 1$ e assim $\sigma(\alpha) = \alpha$. Portanto, $\sigma(a^{1/m}) = a^{1/m} \ \forall \ a \in B$.

Então σ deve fixar todo elemento de tipo $a^{1/m}$, $a \in B$, isto é, σ deve fixar todo elemento gerador de K_B. Temos portanto que $\sigma = \mathrm{Id}$ em $G(K_B/K)$.

Agora, se um elemento $a \in B$ estiver no núcleo a direita da aplicação dada no item 2), devemos ter $\langle \sigma, a \rangle = 1$, $\forall \ \sigma \in G(K_B/K)$, e assim $\sigma(\alpha)/\alpha = 1$. Portanto $\sigma(\alpha) = \alpha \ \forall \ \sigma \in G(K_B/K)$ e então α está no corpo fixo de $G(K_B/K)$, isto é, $\alpha \in K$.

Mas $\alpha^m = a$, então $a \in K^{*m}$. Já mostramos, antes de enunciar este teorema, que se $a \in K^{*m}$ implica que $\langle \sigma, a \rangle = 1$.

Concluímos que K^{*m} é o núcleo à direita.

4) Supondo K_B/K finito, temos $G(K_B/K) = G(K_B/K)/\{\mathrm{Id}\}$ finito. Aplicamos o Teorema de Dualidade (1.2.2) para concluir que a ordem de B/K^{*m} é finita e que $B/K^{*m} \cong G(K_B/K)^\wedge$ e portanto $[K_B : K] = (B : K^{*m})$.

■

Teorema 4.2.2. *Seja K um corpo, $m \in \mathbb{Z}$, $m > 0$, $\mathrm{mdc}(m,p) = 1$, onde p é a característica de K, tal que K contém a m-ésima raiz primitiva da unidade, e considere os conjuntos $\Lambda = \{B \subseteq K^*$ subgrupo $\mid K^{*m} \subset B\}$ e $\Theta = \{E/K \mid E$ é extensão abeliana sobre K de expoente $m\}$, então a aplicação*

$$\begin{array}{rccc} \psi : & \Lambda & \to & \Theta \\ & B & \mapsto & K_B \end{array}$$

é uma bijeção.

Demonstração. Vamos mostrar primeiro a sobrejetividade de ψ. Se E é extensão de K abeliana de expoente m, temos que mostrar que $E = K_B$ para algum $B \in \Lambda$.

Observe que toda extensão abeliana E de K admite uma subextensão finita L sobre

K, que é abeliana e de expoente m, como consequência do Teorema 2.8.1. Sendo $G(L/K)$ abeliano e finito é portanto produto de grupos cíclicos de expoente m, e, pelo Corolário 2.6.18, L é extensão composta de extensões cíclicas. Podemos então tomar a extensão E como a composta de extensões cíclicas. Além disso, pelo Teorema 2.8.8, toda extensão cíclica pode ser obtida pela adjunção de uma m-ésima raiz. Portanto E pode ser escrita como a composta de extensões do tipo $K(\alpha_j)$ tal que $\alpha_j^m = b_j$ com $b_j \in K^*$. Seja B o subgrupo de K^* gerado por todos esses $b_j's$ e por K^{*m}. Temos portanto, $K^{*m} \subset B \subset K^*$ e $E = K_B$ como queríamos.

Outra forma de mostrar a sobrejetividade é mostrar que $E \in \Theta$ é igual à extensão $K_B \in \Lambda$ onde $B = E^{*m} \cap K^*$.

Agora, para mostrar a injetividade, dados B_1 e B_2 em Λ e supondo $K_{B_1} = K_{B_2}$. Temos, em particular, $K_{B_1} \subset K_{B_2}$. Vamos mostrar que $B_1 \subset B_2$. De fato, tome $b \in B_1$, então $K(b^{1/m}) \subset K_{B_2}$ e $K(b^{1/m})$ está contida numa subextensão finitamente gerada de K_{B_2}. Vamos chamar de E tal extensão. Então $K_{b^{1/m}} \subset E \subset K_{B_2}$, e $E = K(\alpha_1, \cdots, \alpha_l)$ tal que $\alpha_i^m = b_i$ onde $i \in \{1, \cdots, l\}$ e $b_i \in B_2$.

Considere agora N o subgrupo de B_2 gerado por K^{*m} e pelos elementos $b_1, \cdots, b_l$. Então temos que $E = K_N$.

Tomando B_3 o subgrupo de K^* gerado pelo subgrupo N e pelo elemento b, então $K^{*m} \subset B_3 \subset K^*$ e como $K(b^{1/m}) \subset K_N \subset K_{B_3}$ temos que $K_{B_3} = K_N$. Então, pelo teorema anterior, podemos concluir que $(B_3 : K^{*m}) = (N : K^{*m})$. Isso implica que $B_3 = N$, pois $N \subset B_3$. Portanto, $b \in N$ e, como $b \in B_1$ foi tomado arbitrariamente, concluímos que $B_1 \subset N \subset B_2$.

Analogamente, considerando que $K_{B_2} \subset K_{B_1}$, concluiremos que $B_2 \subset B_1$. Isto é $K_{B_1} = K_{B_2}$ implica $B_1 = B_2$, ou seja, ψ é injetiva.

Logo ψ é bijetiva.

■

4.2.2 Teorema de Correspondência, forma multiplicativa (Bis)

Teorema 4.2.3. *Seja E/K uma extensão de galois finita, com grupo de galois G e suponha $\mu_m \subseteq K$. Então $(K^* \cap E^{*m})/K^{*m} \cong \mathrm{Hom}(G, \mu_m)$.*

Demonstração. Observe a seguinte sequência de homomorfismos:

$$0 \xrightarrow{f_0} \mu_m \xrightarrow{f_1} E^* \xrightarrow{f_2} E^{*m} \xrightarrow{f_3} 0$$

Com $f_0(0) = 1$, $f_1(\zeta) = \zeta\ \forall\ \zeta\ \in\ \mu_m$ homomorfismo inclusão, $f_2(\beta) = \beta^m\ \forall\ \beta\ \in\ E^*$ e $f_3(\alpha) = 0\ \forall\ \alpha\ \in\ E^{*m}$.

Temos portanto que $\mathrm{Im} f_i = \mathrm{Ker} f_{i+1}\ \forall\ i\ \in\ \{0,1,2\}$. Sequência com tal característica é chamada de *sequência exata*, e induz, sobre os invariantes por G, a seguinte sequência exata (ver [14], pg 95 ou [4] Teorema 5.4):

$$0 \xrightarrow{f_0'} \mu_m^G \xrightarrow{f_1'} (E^*)^G \xrightarrow{f_2'} (E^{*m})^G \xrightarrow{f_3'} H^1(G,\mu_m) \xrightarrow{f_4'} H^1(G,E^*) \longrightarrow \cdots$$

Como K é corpo fixo de E sobre G, $\mu_m^G = \mu_m$, $(E^*)^G = K^*$ e $((E^{*m})^G = K^* \cap E^{*m}$. Além disso, G age trivialmente sobre os elementos de μ_m, então podemos usar a Proposição 3.1.2 e temos $H^1(G, \mu_m) \cong \mathrm{Hom}(G,\mu_m)$. Pelo Teorema 3.1.3, $H^1(G, E^*) = 0$, e portanto temos

$$0 \xrightarrow{f_0'} \mu_m \xrightarrow{f_1'} K^* \xrightarrow{f_2'} K^* \cap E^{*m} \xrightarrow{f_3'} \mathrm{Hom}(G,\mu_m) \xrightarrow{f_4'} 0$$

sequência exata.

O homomorfismo f_2' tem imagem igual a K^{*m} que é núcleo do homomorfismo f_3', usamos o Teorema de isomorfismos para concluir que $(K^* \cap E^{*m})/K^{*m} \cong \mathrm{Im} f_3' = \mathrm{Hom}(G, \mu_m)$.

∎

Corolário 4.2.4. *Se L o fecho algébrico de K e $G = Gal(L/K)$, então $K^*/K^{*m} \cong$*

$\mathrm{Hom(G, \mu_m)}$.

Demonstração. Temos que $K^* = K^* \cap L^{*m}$. De fato, devemos mostrar apenas que $K^* \subset K^* \cap L^{*m}$. Tome $\alpha \in K^* \setminus (K^* \cap L^{*m})$ então $\alpha \neq \beta^m$ para qualquer $\beta \in L^*$ e assim o polinômio $x^m - \alpha \in K[x]$ não tem raízes em L, o que contradiz o fato de L ser algebricamente fechado.

Então $K^* \cap L^{*m} = K^{*m}$ e vale $(K^* \cap L^{*m})/K^{*m} = K^*/K^{*m}$, usando o teorema acima, obtemos $K^*/K^{*m} \cong \mathrm{Hom}(G, \mu_m)$.

■

Tomemos agora um fecho algébrico L de K e $G = G(L/K)$. Seja ainda $\phi \in \mathrm{Hom}(G,\mu_m)$ e considere Ker ϕ, que é um subgrupo normal de G. Tomemos então a extensão E_ϕ como sendo a extensão de K contida em L formada pelos elementos de L que são fixos por Ker ϕ.

Pela Teoria de Galois, tal extensão é galoisiana e vale que $G(E_\phi/K) \cong G/G(L/E_\phi)$, mas $G(L/E_\phi) = \ker \phi$ e portanto $G(E_\phi/K) \cong \mathrm{Im}\ \phi \subseteq \mu_m$.

Portanto $G(E_\phi/K)$ é grupo cíclico, ou seja, E_ϕ/K é extensão cíclica com $[E_\phi : K] = |G(E_\phi/K)| = d$, onde $d|\ m$, $m = |\mu_m|$. Como $\phi^d(\sigma) = (\phi(\sigma))^d\ \forall\ \sigma \in G$, temos que ϕ tem ordem d, pois $(\phi(\sigma))^d = 1\ \forall\ \phi \in G$, isto é, $\phi^d \equiv 1$. Seja n relativamente primo com d e suponha que $\phi(\sigma) = 1$, $\phi^n(\sigma) = \phi(\sigma)... \cdot \phi(\sigma) = 1$. Por outro lado, $\phi^n(\sigma) = 1$ implica que $\phi(\sigma) = 1$, caso contrário, teríamos $\phi(\sigma) \neq 1$ e, para que valha $\phi^n(\sigma) = 1$, deveríamos ter $n = \lambda \cdot d$ para algum inteiro λ, contrariando o fato de mdc$(n,d) = 1$. Concluímos que ϕ^n e ϕ tem o mesmo núcleo e portanto correspondem à mesma extensão E_ϕ de K, via Teorema fundamental de Galois.

Considere agora uma extensão E sobre K, cíclica de grau d, com $d|m$. Tomamos em $\mathrm{Hom}(G, \mu_m)$ o conjunto dos elementos que são triviais em $G(L/E)$, isto é, tomamos o conjunto $H_E = \{\phi \in \mathrm{Hom}(G, \mu_m) \mid \phi(\sigma) = 1\ \forall\ \sigma \in G(L/E) \subseteq G\}$.

Seja $\phi \in H_E$ e $\sigma \in G(E/K)$ tal que σ é o gerador. Pelo Teorema 2.8.1, temos que $G(E/K) \cong G(L/K)/G(L/E)$, isto é, podemos ver $G(E/K)$ como subgrupo de

$G(L/K)$. Como σ tem ordem d, $\phi(\sigma)$ tem ordem d em μ_m.

Desta forma, temos uma bijeção entre os subgrupos cíclicos de $\mathrm{Hom}(G,\mu_m) \cong K^*/K^{*m}$ tais que a ordem divide m e as extensões cíclicas de K, cujo grau divide m.

Acabamos de mostrar o seguinte resultado:

Teorema 4.2.5. *Existe uma correspondência bijetiva entre os subgrupos cíclicos de K^*/K^{*m} e as extensões cíclicas sobre K.*

Agora podemos melhorar esse resultado da seguinte forma:

Teorema 4.2.6. *Existe uma correspondência bijetiva entre os subgrupos abelianos de K^*/K^{*m} de expoente m e as extensões abelianas $finitas$ de expoente m.*

Demonstração. Suponha que E/K é uma extensão finita abeliana de grau d tal que $d|m$. Podemos decompor $G(E/K) = G_1 \times G_2 \times ... \times G_n$ tal que cada G_i é cíclico de ordem d_i e $d_i|m$. Tomamos E_i como o corpo fixo de $G_i \times ... \times G_{i-1} \times G_{i+1} \times ... \times G_n$ com $G(E_i/K)$ como no Corolário 2.6.18, isto é, $E = K_1K_2...K_n$, onde K_i é extensão cíclica e, pelo Teorema 4.2.5, temos ϕ_1, ϕ_2, ... ,$\phi_n \in \mathrm{Hom}(G,\mu_m)$ tais que ϕ_i tem núcleo $G(L/K_i)$, com L fecho algébrico de K. Cada ϕ_i corresponde à um subgrupo cíclico de K^*/K^{*m} de ordem d_i. Tomamos $\phi = \phi_1 \times ... \times \phi_n \in \mathrm{Hom}(G, \mu_m)$, então ϕ tem núcleo $G(L/E)$. Assim, ϕ corresponde à um subgrupo de K^*/K^{*m} com expoente m.

Por outro lado, dado um subgrupo finito H de K^*/K^{*m} de expoente m, tomamos $H = H_1 \times ... \times H_n$ tal que cada H_i é cíclico de ordem d_i, e cada um H_i corresponde à algum $\phi_i \in \mathrm{Hom}(G,\mu_m)$, ϕ_i com ordem d_i. Cada ϕ_i corresponde à uma extensão de Galois cíclica E_i sobre K tal que o grupo de Galois $G_i = G(E_i/K) \cong \mathrm{Im}\phi_i$ de ordem d_i, assim como fizemos no Teorema 4.2.5.

Tomamos então o produto $G_1 \times ... \times G_n = G$ como o grupo de Galois da composição de extensões $E = E_1E_2...E_n$ e assim G tem expoente m.

$\blacksquare$

Vamos agora apresentar dois exemplos em característica 0, onde o resultado acima também pode ser verificado.

Exemplo 4.2.7. *Considere o corpo dos reais* $\mathbb{R}$. *Sabemos que admite uma única extensão abeliana* $\mathbb{C}$ *de grau dois. E observe que o grupo multiplicativo* $\mathbb{R}^*$ *contém as raiz quadradas da unidade, e ainda que o grupo quociente* $\mathbb{R}^*/\mathbb{R}^{*2}$ *tem apenas os elementos* -1 *e* 1, *o que significa que temos apenas um subgrupo* B *tal que* $\mathbb{R}^{*2} \subset B \subseteq \mathbb{R}^*$ *que é o próprio* $\mathbb{R}^*$ *e assim* $K_B = \mathbb{C}$.

Exemplo 4.2.8. *Considere agora o corpo dos racionais* $\mathbb{Q}$. *O conjunto das extensões abelianas de grau dois será bijetivo com o cojunto dos subgrupos de* $\mathbb{Q}^*/\mathbb{Q}^{*2}$ *ou equivalentemente, com os subgrupos de* $\mathbb{Q}^*$ *que contém* $\mathbb{Q}^{*2}$. *Observe que*

$$\mathbb{Q}^*/\mathbb{Q}^{*2} \cong \{-1{,}1\} \times \bigoplus_{p\ primo} \mathbb{Z}/2\mathbb{Z}$$

onde o grupo à direita é a soma direta de $\{-1, 1\}$ *com infinitas cópias de* $\mathbb{Z}/2\mathbb{Z}$ *indexadas por números primos. Um elemento desse grupo tem toda entrada* $a_i = 0$, *exceto por um número finito de entradas.*

Para verificar o isomorfismo, observe que cada elemento em $\mathbb{Q}^*/\mathbb{Q}^{*2}$ *pode ser escrito como o produto finito de* r *primos* $p_1 \cdot p_2 \cdot \ldots \cdot p_r$ *a menos de sinal. E, para cada elemento* $(\pm 1, a_2, a_3, a_5, \ldots)$ *em* $\{-1{,}1\} \times \bigoplus_{p\ primo} \mathbb{Z}/2\mathbb{Z}$ *identificamos com o elemento de* $\mathbb{Q}^*/\mathbb{Q}^{*2}$ *que é o produto de primos* p_i *nos quais* a_{p_i} *é diferente de zero, e o respectivo sinal.*

As extensões de $\mathbb{Q}$ *de grau dois são obtidas pela adjunção de um elemento que é do tipo* $\sqrt{p_1 \cdot p_2 \cdot \ldots \cdot p_r}$, *a menos de sinal, com* p_i *primo para todo* $i \in \{1, \ldots, r\}$. *Tal extensão obviamente tem grupo de galois isomorfo a* $\mathbb{Z}/2\mathbb{Z}$, *portanto é abeliana. Daí podemos observar que as possibilidades de elementos a serem adjuntados para formar extensões de grau dois, coincidem com as possibilidades de subgrupos de* $\{-1{,}1\} \times \bigoplus_{p\ primo} \mathbb{Z}/2\mathbb{Z}$, *da seguinte maneira: dado um gerador de extensão abeliana de grau dois* $\sqrt{\pm 1 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r}$

tomamos

$$\{-1{,}1\} \times \{0\} \oplus ... \oplus \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{posição } p_1} \oplus \{0\} \oplus ... \oplus \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{posição } p_2} \oplus \{0\} \oplus ...$$

como subgrupo correspondente.

4.2.3 Teorema de Correspondência, forma aditiva

Seja K corpo de característica p, definimos o operador $\wp$ por $\wp(x) = x^p - x$ para $x \in K^+$ (K como grupo aditivo). Então $\wp$ é um homomorfismo de grupo de K^+ nele mesmo. De fato,

$$\wp(x+y) = (x+y)^p - (x+y) = x^p + y^p - x - y = x^p - x + y^p - y = \wp(x) + \wp(y)$$

Esse operador nos dá uma imagem em K^+ que desempenha papel semelhante à K^{*m} na teoria multiplicativa, toda vez que m for um número primo. A raiz do polinômio $x^p - x - a$, com $a \in K$, será denotada por $\wp^{-1}a$ (o elemento $\wp^{-1}a$ não é necessariamente um elemento de K). Se B é um subgrupo de K^+ contendo $\wp(K)$, tomamos $K_B = K(\wp^{-1}B)$ o corpo obtido quando adjuntamos $\wp^{-1}a$ à K para todo $a \in B$. Observe que B aqui é um subgrupo de K^+, olhando K^+ como grupo aditivo.

Teorema 4.2.9. *Seja K um corpo de característica p. Então temos:*

1) *A aplicação $B \mapsto K(\wp^{-1}B)$ é uma bijeção entre subgrupos de K^+contendo $\wp(K)$ e extensões abelianas de K de expoente p;*

2) *Seja $K_B = K(\wp^{-1}B)$ e seja $G(K_B/K)$ o seu grupo de galois. Se $\sigma \in G(K_B/K)$ e $a \in B$, com $\wp(\alpha) = a$ (observe que α não está necessariamente em K, pois basta que seja raiz de $x^p - x - a \in K[x]$), seja $\langle \sigma, a \rangle = \sigma\alpha - \alpha$. Então a aplicação*

$$\begin{array}{rcl} G \times B & \to & \mathbb{Z}/p\mathbb{Z} \\ (\sigma, a) & \mapsto & \langle \sigma, a \rangle \end{array}$$

é bilinear;

3) O núcleo à esquerda da aplicação dada no item 2) é 1 e o núcleo à direita é $\wp K$*;*

4) A extensão K_B/K *é finita se somente se* $(B : \wp K)$ *é finita e, nesse caso, vale* $[K_B : K] = (B : \wp K)$.

Demonstração. Devemos observar que $\sigma\alpha - \alpha$ realmente é um elemento de $\mathbb{Z}/p\mathbb{Z}$, já que $\wp(\sigma\alpha - \alpha) = 0$, isto é, $(\sigma\alpha - \alpha)^{p-1} = 1$, e portanto, como K^* é cíclico, admite apenas um subgrupo de ordem $p-1$ (ver [11], página 157) que é exatamente $\mathbb{Z}/p\mathbb{Z}^*$ o que implica que todo elemento que tem expoente $p-1$ está em $\mathbb{Z}/p\mathbb{Z}^*$. A prova do teorema acima é análoga à prova do Teorema de correspondência apresentado na Subseção 4.2.1, alterando a operação, usando raiz p-ésima ao invéz da raiz m-ésima, e o Teorema 2.8.10 no lugar do Teorema 2.8.8. ∎

O leitor interessado em conhecer mais sobre extensões de Kummer, em particular, sobre extensões abelianas de corpos de característica positiva p, de expoente potência de p, recomendamos a leitura das seções 8.10 e 8.11 de [15].

Capítulo 5

Considerações Finais

Fizemos aqui a apresentação dos Teoremas de Correspondência, como consequência da Teoria de Galois, utilizando ferramentas de Cohomologia de Grupos.

A relevância do tema proposto neste trabalho pode ser verificada nas aplicações em teoria dos números, como por exemplo, no artigo de Emmanuel Kowalski, "Some local-Global applications of Kummer Theory"[17] para responder se a afirmação "a pertence ao subgrupo gerado por b"obedece a um princípio local-global, onde a e b são pontos racionais de algum grupo algébrico sobre um corpo numérico.

Também podemos citar a aplicação da Teoria de Kummer para a lei da reciprocidade quadrática que verifica o fato de as extensões quadráticas estarem contidas em extensões ciclotômicas, sobre as quais tem-se maior controle (ver [18]).

Um trabalho interessante também foi apresentado por Vahid Shirbisheh, em seu artigo intitulado *A Relative Version of Kummer Theory* [16], que estabelece um isomorfismo entre os $\mathbb{F}_p[G]$-submódulos finitamente gerados de E^*/E^{*p} e o grupo de galois associado à extensão de Kummer sobre E como um $\mathbb{F}_p[G]$-módulo.

A expectativa agora é que este trabalho possa servir como subsídio para estudantes de Matemática. Esperamos que, de fato, as observações e os detalhes das demostrações possam facilitar a leitura e o entendimento dos principais teoremas aqui apresentados.

Referências Bibliográficas

[1] S. Lang, *Algebra.* Graduate texts in Mathematics. Springer Verlag, Third Edition, 2002.

[2] I. N. Herstein, *Topics in Algebra.* Xerox College Publishing, 2nd edition, 1975.

[3] M. Artin,*Algebra.* Prentice Hall, 1991.

[4] K. Harper, *Group Cohomology and Kummer Theory.* Disponível em: http://www.math.uchicago.edu/ may/ (14/08/2015). The University of Chigago, 2010.

[5] J. D. Dixon and B. Mortimer, *Permutation Groups.* Graduate Texts in Mathematics, Springer Verlag, 1996.

[6] J. S. Milne, *Fields and Galois Theory.* Disponível em: http://www.jmilne.org/math/ (14/09/2014). Version 4.30, 2012.

[7] J. S. Milne, *Class Field Theory.* Disponível em: http://www.jmilne.org/math/ (21/10/2014). Version 4.01, 2011.

[8] P. J. McCarthy, *Algebraic Extensions of Fields.* Dover Publications, 2014.

[9] E. Artin and J. Tate, *Class Field Theory.* American Mathematical Society, 2009.

[10] J. A. Gallian, *Contemporary Abstract Algebra.* 8th ed, 2012.

[11] A. Garcia, *Elementos de Álgebra.* IMPA, 2003.

[12] T. W. Hungerford, *Algebra.* Graduate Texts in Mathematics, Springer, 1980.

[13] D. G. Figueiredo, *Números Irracionais e Transcendentes.* Coleção Iniciação Científica, 3ª Edição, SBM, 2002.

[14] J. W. S. Cassels and A. Frölich, *Algebraic Number Theory.* Thompson Book Company Inc., 1967.

[15] N. Jacobson, *Basic Algebra II.* W. H. Freemam and Company, Second Edition, 1989.

[16] Vahid Shirbisheh, *A Relative Version of Kummer Theory.* Tarbiat Modares University, 2008. (arXiv:0808.1760 [math.NT])

[17] Emmanuel Kowalski, *Some Local-Global Aplications of Kummer Theory.* manuscripta mathematica, v. 111, n. 1, p. 105-139, 2003.

[18] Peter Stevenhagen. *Kummer Theory and Reciprocity Laws.* Universiteit Leiden, 2005. (mis.math.leidenuniv.nl)

ANEXO 1

$$\begin{bmatrix}
\sigma_1\sigma_2 f(\sigma_3,\ldots,\sigma_{n+2}) & (-1)^1\sigma_1 f(\sigma_2\sigma_3,\ldots,\sigma_{n+2}) & \cdots & (-1)^n\sigma_1 f(\sigma_2,\ldots,\sigma_{n+1}\sigma_{n+2}) & (-1)^{n+1}\sigma_1 f(\sigma_2,\ldots,\sigma_{n+1}) \\
(-1)^1\sigma_1\sigma_2 f(\sigma_3,\ldots,\sigma_{n+2}) & (-1)^2 f(\sigma_1\sigma_2\sigma_3, \sigma_4, \ldots,\sigma_{n+2}) & \cdots & (-1)^{n+1} f(\sigma_1\sigma_2,\sigma_3,\ldots,\sigma_{n+1}\sigma_{n+2}) & (-1)^{n+2} f(\sigma_1\sigma_2, \sigma_3, \ldots, \sigma_{n+1}) \\
(-1)^2\sigma_1 f(\sigma_2\sigma_3, \sigma_4,\ldots,\sigma_{n+2}) & (-1)^3 f(\sigma_1\sigma_2\sigma_3, \sigma_4,\ldots,\sigma_{n+2}) & \cdots & (-1)^{n+2} f(\sigma_1,\sigma_2\sigma_3, \sigma_4,\ldots,\sigma_{n+1}\sigma_{n+2}) & (-1)^{n+3} f(\sigma_1,\sigma_2\sigma_3, \sigma_4,\ldots,\sigma_{n+1}) \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
(-1)^{n+1}\sigma_1 f(\sigma_2, \sigma_3, \sigma_4,\ldots,\sigma_{n+1}\sigma_{n+2}) & (-1)^{n+2} f(\sigma_1\sigma_2, \sigma_3,\ldots,\sigma_{n+1}\sigma_{n+2}) & \ldots & (-1)^{2n+1} f(\sigma_1,\ldots,\sigma_n\sigma_{n+1}\sigma_{n+2}) & (-1)^{2n+2} f(\sigma_1,\ldots,\sigma_n) \\
(-1)^{n+2}\sigma_1 f(\sigma_2,\ldots,\sigma_{n+1}) & (-1)^{n+3} f(\sigma_1\sigma_2, \sigma_3, \ldots,\sigma_{n+1}) & \ldots & (-1)^{2n+2} f(\sigma_1, \ldots, \sigma_n\sigma_{n+1}) & (-1)^{2n+3} f(\sigma_1, \ldots, \sigma_n)
\end{bmatrix}$$