Universidade Federal do Rio Grande do Sul
Instituto de Matemática
Programa de Pós-Graduação em Matemática

Galois, Dedekind e Grothendieck

Dissertação de Mestrado

GRAZIELA LANGONE FONSECA

Porto Alegre, 24 de março de 2015

Dissertação submetida por Graziela Langone Fonseca[1], como requisito parcial para a obtenção do grau de Mestre em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Prof. Dr. Antonio Paques

Banca examinadora:
Prof. Dr. Alveri Alves Sant'Ana (UFRGS)
Prof. Dra. Bárbara Seelig Pogorelsky (UFRGS)
Prof. Dra. Thaísa Raupp Tamusiunas (UNISINOS)

[1]Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)

Agradecimentos

Agradeço e dedico este trabalho às minhas avós Maria Gonçalves Langone e Oly Ribeiro Fonseca. Ambas nasceram numa cidade do interior do Rio Grande do Sul chamada Canguçu. A vida era difícil e, para piorar, os invernos eram rigorosos. Na época as mulheres não tinham voz nem opinião, mas não para Dona Maria ou Dona Oly. Elas souberam se impor nos momentos decisivos, trabalharam duro e ajudaram no sustento da casa. Deram exemplo de honestidade aos seus filhos e filhas e mostraram que as vitórias são sempre possíveis, por mais humilde que seja a nossa origem. Elas também tiveram suas perdas mas, mesmo assim, ainda levantam todo dia de manhã mostrando ao mundo a força que elas tem. Força essa que carrego com muito orgulho no meu sangue, sempre pensando que as frágeis velhinhas que vejo hoje foram grandes mulheres no passado.

Resumo

Usando como ferramenta principal o Lema de Dedekind, apresentaremos o Teorema-Definição que caracteriza a noção de extensão de Galois, assim como o Teorema da Correspondência de Galois-Grothendieck que generaliza o Teorema Fundamental da Teoria de Galois. Este trabalho é baseado no texto de A. Dress "One more shortcut to Galois Theory"[4].

Abstract

We use the fundamental and well known tool called Dedekind's Lemma to present the Theorem-Definition that characterizes the notion of a Galois extension, as well as the Galois-Grothendieck Correspondence Theorem which generalizes the Fundamental Theorem of the Galois Theory. This work is based on the paper of A. Dress "One more shortcut to Galois Theory"[4].

Índice

Introdução

Évariste Galois foi um matemático francês que viveu entre 1811 e 1832. Apesar da sua morte prematura, sua contribuição para o avanço da pesquisa matemática foi imenso. Entretanto, seus trabalhos foram publicados apenas catorze anos após sua morte. Na época não se entendia a importância e a riqueza que seus manuscritos carregavam. De fato, Galois mostrou ao mundo o portal de entrada para a Álgebra como é vista hoje, a Álgebra Moderna.

Mais de um século se passou após as publicações dos resultados obtidos por Galois e ainda não conseguimos explorar por completo esse novo universo. A cada dia surgem mais questões a serem estudadas e mais teorias a serem desenvolvidas não só no campo da Álgebra mas em outras áreas da Matemática também. Por isso sempre existe uma importância, histórica e matemática, de se estudar a Teoria de Galois.

Na Teoria de Galois destacam-se dois teoremas: um Teorema-Definição, que apresenta as diversas equivalências da definição de extensão de Galois, e um Teorema de Correspondência, que estabelece uma bijeção entre os subcorpos intermediários de uma extensão de Galois L/K e os subgrupos do grupo $Aut_K L$ dos K-automorfismos de L. Esses teoremas são abordados em todos os textos que tratam de uma teoria de Galois para corpos e podem ser traduzidos da seguinte maneira:

Teorema-Definição: *Sejam L/K uma extensão de corpos e $G = Aut_K L$. L é dito uma extensão de Galois de K se satisfaz uma (e portanto todas) das seguintes condições equivalentes:*

- $L^G := \{x \in L \mid \sigma(x) = x \ \forall \sigma \in G\} = K$.
- $dim_K L = |G|$.
- *L é corpo de decomposição de um polinômio separável sobre K.*

- *L/K é extensão normal e separável.*

E o teorema da correspondência, também chamado de Teorema Fundamental da Teoria de Galois, se apresenta da seguinte forma:

Teorema da Correspondência: *Sejam L/K uma extensão de Galois e $G = Aut_K L$. Então existe uma bijeção que inverte inclusão entre o conjunto dos subgrupos de G e o conjunto dos subcorpos de L que contêm K, dada por:*

$$H \mapsto L^H := \{x \in L \mid \tau(x) = x,\ \forall \tau \in H\},$$

para todo subgrupo H de G, cuja inversa é dada por:

$$F \mapsto H_F := Aut_F L = \{\sigma \in G \mid \sigma(x) = x,\ \forall x \in F\ \},$$

para todo subcorpo F de L que contém K.

Graças a um resultado clássico da teoria de corpos conhecido e celebrado como Lema de Dedekind, o qual diz respeito à independência linear de homomorfismos de corpos, tornou-se possível uma ampliação da lista de definições equivalentes de extensão de Galois. Especificamente, o Lema de Dedekind, na forma em que é apresentado nos textos clássicos da teoria de corpos, diz o seguinte:

Lema de Dedekind: *Sejam K e L corpos e $\sigma_1, ..., \sigma_n$ distintos homomorfismos de K em L. Então $\sigma_1, ..., \sigma_n$ são linearmente independentes sobre L, isto é, se existem elementos $x_1, ..., x_n \in L$ tais que $\sum_{i=1}^{n} x_i \sigma_i(a) = 0$, $\forall a \in K$, então necessariamente $x_1 = ... = x_n = 0$.*

No Capítulo 1 deste trabalho apresentaremos em detalhes a lista complementar das novas definições de extensão de Galois obtidas direta ou indiretamente como consequência do uso do Lema de Dedekind.

Na realidade, o Teorema Fundamental da Teoria de Galois diz respeito a uma (anti-)equivalência entre categorias. Este enfoque decorre das ideias apresentadas por Alexander Grothendieck em [5]. Uma contextualização dessas ideias na linguagem específica de extensão de corpos foi desenvolvida por Andreas Dress, em [4]. Neste trabalho Dress apresenta o assim chamado Teorema da Correspondência de Galois-Grothendieck, o qual generaliza o Teorema Fundamental da Teoria de Galois. O propósito central desta dissertação é a apresentação detalhada desse resultado e isto é feito no Capítulo

3.

No Capítulo 2 trataremos de apresentar o material necessário para o desenvolvimento do Capítulo 3. Fazem parte desse material as noções e propriedades de G-conjunto, álgebra L-decomponível e fundamentalmente o Lema de Dedekind reinterpretado nesse novo contexto.

O trabalho de Galois teve como motivação inicial a solubilidade de equações por meio de radicais. Especificamente, o que se buscava era dar resposta à questão:

"Dado $f(x)$ um polinômio em $K[x]$ com K um corpo, quando podemos decidir se as soluções da equação $f(x) = 0$ podem ser expressas em termos de radicais, isto é, podem ser escritas a partir de um número finito de operações e elementos de K, envolvendo inclusive radiciação?"

Nessa busca foi utilizada a noção, ainda que implicitamente, do que hoje conhecemos como sendo o corpo de decomposição de um polinômio. Embora essa noção esteja em todos os textos básicos da teoria de corpos, para conforto do leitor, abordaremos novamente essa e outras noções tais como extensão finita, extensão separável, extensão normal, e as correspondentes propriedades que serão usadas ao longo do texto.

Capítulo 1

Extensão de Galois

Uma das grandes questões que intrigou os matemáticos ao longo dos séculos foi sobre a solubilidade de equações polinomiais por meio de radicais. A priori, o próprio questionamento pode parecer um tanto simples, mas sua resposta permaneceu obscura durante muito tempo.

Eis que em 1811 nasce em Bourg La Reine, no dia 25 de outubro, um menino chamado Évariste Galois que, a princípio não sabia, mas seria responsável pela transformação do pensamento algébrico matemático. A genialidade de muitos artistas e pesquisadores infelizmente só é compreendida anos depois de sua morte, e com Galois isso não foi diferente. A morte dele ocorreu em maio de 1832, e apenas em 1846 Liouville publicou suas interpretações acerca dos estudos de Galois que deram início ao que chamamos hoje de Teoria de Galois.

1.1 Preliminares

Nessa seção apresentaremos os conceitos e respectivas propriedades, bem como introduziremos novas ferramentas, decorrentes do Lema de Dedekind, necessárias para a demonstração do Teorema-Definição na Seção 1.2. Com intuito de não tornar o texto volumoso, iremos omitir as demonstrações desta seção, mas elas podem ser facilmente encontradas em [6], [7], [9] ou em [10].

Começamos com a noção de extensão de corpos. Dados dois corpos L e K, dizemos que L é uma extensão de K, e denotamos por L/K, se existir um monomorfismo $\pi : K \to L$, o que nos permite identificar K com a sua imagem $\pi(K)$ em L e assumir simplesmente, sem perda de generalidade, que K está contido em L.

Interessa-nos, em particular, para os propósitos deste texto, as extensões de corpos finitas, isto é, as extensões L/K tais que a dimensão de L como K-espaço vetorial é finita. Uma propriedade interessante e extremamente útil é a transitividade da noção de extensão finita, conforme é descrita no lema a seguir.

Lema 1.1.1. *Sejam F/K e L/F extensões finitas de corpos. Então L/K é também finita e*

$$dim_K L = dim_F L \cdot dim_K F.$$

A demonstração deste lema é bem simples, bastando para ver isso exibir uma base de L sobre K, a qual é obtida como produto das respectivas bases de F sobre K e de L sobre F.

O conceito de extensão finita de corpos estabelece uma relação íntima com um conceito mais amplo, o de extensão algébrica. Uma extensão L/K é chamada de algébrica se todo elemento de L for algébrico sobre K, isto é, se todo elemento de L é raiz de algum polinômio não nulo com coeficientes em K.

O lema a seguir nos dá uma excelente caracterização do que significa um elemento ser algébrico sobre um corpo.

Lema 1.1.2. *Sejam L/K uma extensão de corpos e $\alpha \in L$. Se α é algébrico sobre K então:*

(i) *Existe um polinômio mônico e de grau mínimo $p(x) \in K[x]$ tal que $p(\alpha) = 0$.*

(ii) *$p(x)$ é irredutível sobre K.*

(iii) *$K[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\}$ é corpo e $K[\alpha] \simeq \dfrac{K[x]}{< p(x) >}$.*

(iv) *$K[\alpha] = K(\alpha) := \{\dfrac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ e } g(x) \neq 0\}$.*

(v) *$K[\alpha]/K$ é uma extensão finita e $dim_K K[\alpha] = \partial(p(x))$.*

(vi) *O conjunto $\{\alpha^i \mid 0 \leq i \leq \partial(p(x)) - 1\}$ é uma base de $K[\alpha]$ sobre K.*

É fácil ver que toda extensão finita é algébrica. Para tanto basta observar que se L/K é extensão finita de dimensão n, então, dado qualquer elemento $\alpha \in L$, o conjunto $\{\alpha^i \mid 0 \leq i \leq n\}$ é necessariamente linearmente dependente sobre K.

Por outro lado, nem toda extensão algébrica é finita. Para se ter um exemplo, considere o fecho algébrico $\tilde{\mathbb{Q}}$ do corpo dos números racionais $\mathbb{Q}$, isto é, $\tilde{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ é algébrico sobre } \mathbb{Q}\}$. Se $dim_{\mathbb{Q}}\tilde{\mathbb{Q}} = n < \infty$ então temos uma contradição pois, para todo inteiro primo $p > n + 1$, denotando por ω_p a p-ésima raiz primitiva da unidade, temos:

$$\mathbb{Q}(\omega_p) \subset \tilde{\mathbb{Q}}$$

e

$$dim_{\mathbb{Q}}\mathbb{Q}(\omega_p) = p - 1 > n = dim_{\mathbb{Q}}\tilde{\mathbb{Q}} = dim_{\mathbb{Q}(\omega_p)}\tilde{\mathbb{Q}}.dim_{\mathbb{Q}}\mathbb{Q}(\omega_p).$$

Observação 1.1.3. O polinômio $p(x)$ do Lema 1.1.2 é chamado o polinômio mínimo de α sobre K e é denotado por $p_{\alpha/K}(x)$.

Dentre as extensões de corpos finitas iremos considerar, para os fins deste texto, apenas aquelas que são normais e separáveis.

Definição 1.1.4. Seja L/K um extensão de corpos. Dizemos que esta extensão é normal se todo o polinômio $f(x) \in K[x]$ que possui uma raiz em L se fatora completamente como um produto de fatores lineares em $L[x]$.

No caso de dimensão finita a noção de extensão normal coincide com a de corpo de decomposição de um polinômio, conforme estabelecido no próximo teorema.

Definição 1.1.5. Corpo de decomposição de um polinômio é o menor corpo que contém todas as raízes deste polinômio, isto é: se $f(x) \in K[x]$, com K um corpo, dizemos que L é corpo de decomposição de $f(x)$ sobre K se:

(i) L/K é extensão de corpos.

(ii) L possui todas as raízes de $f(x)$.

(iii) Se F é corpo intermediário da extensão L/K e F contém todas as raízes de $f(x)$, então $F = L$.

Teorema 1.1.6. *Uma extensão de corpos L/K é normal e finita se, e somente se, L é corpo de decomposição de algum polinômio não nulo com coeficientes em K.*

A separabilidade de extensões de corpos está intimamente relacionada ao conceito de simplicidade de raízes de polinômios.

Definição 1.1.7. Seja K um corpo.

- Um polinômio irredutível $f(x) \in K[x]$ é dito separável sobre K se não possuir raízes múltiplas, isto é, raízes repetidas, no seu corpo de decomposição.

- Sejam L/K uma extensão de corpos e $\alpha \in L$ um elemento algébrico sobre K. Então, α é dito um elemento separável sobre K se $p_{\alpha/K}(x)$ for separável.

- Uma extensão de corpos L/K é dita separável se todo elemento de L for separável sobre K.

Claramente, se a característica de K for igual a zero então toda extensão finita (ou mais geralmente, algébrica) de K é separável sobre K. Portanto, em geral, o estudo da separabilidade fica restrito às extensões de corpos de característica prima.

Observação 1.1.8. Note que nem toda extensão separável é normal. Para ver isso considere, por exemplo, a extensão $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Com relação aos conceitos de separabilidade e normalidade existem dois fatos fundamentais dados pelos teoremas seguintes.

Teorema 1.1.9. *Sejam N/K uma extensão normal e finita e $K \subset F$, $L \subset N$ subcorpos isomorfos. Então todo K-isomorfismo de F em L se estende a um K-automorfismo de N.*

Teorema 1.1.10. *Sejam L/K uma extensão separável de K e N/K uma extensão normal de K que contém L. Se $dim_K L = n$ então existem exatamente n K-imersões de L em N.*

Definição 1.1.11. Uma extensão finita de corpos L/K é dita extensão galoisiana (ou de Galois) de K se L é normal e separável.

Considere L/K uma extensão de corpos e $G = Aut_K L$ um grupo dos automorfismos de L que deixam os elementos de K fixos. Outra propriedade importante, que será extremamente útil na demonstração do Teorema-Definição na Seção 1.2, é a que afirma que se L/K é uma extensão de Galois então existe um elemento $\alpha \in L$ tal que o conjunto $\{\sigma(\alpha) \mid \sigma \in G\}$ é uma base de L sobre K. Tal conjunto é chamado de base normal. Dessa forma, temos os seguintes resultados.

Lema 1.1.12. *Sejam L/K uma extensão de Galois, $G = Aut_K L = \{\sigma_1, ..., \sigma_n\}$ e $\alpha \in L$. O conjunto $\{\sigma_1(\alpha), ..., \sigma_n(\alpha)\}$ é uma base normal de L sobre K se, e somente se, a matriz $(\sigma_i \sigma_j(\alpha))$ é invertível em $M_n(L)$, com $1 \leq i, j \leq n$.*

Teorema 1.1.13 (Teorema da Base Normal)**.** *Toda extensão de Galois tem base normal.*

Exemplo 1.1.14. Considere a extensão galoisiana $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ de dimensão 2. Facilmente pode-se ver que $G = Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}) = \{\sigma_1, \sigma_2\}$, com $\sigma_1 = 1_G$ e $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Assim, tomando $\alpha = 1 + \sqrt{2}$ temos que:

$$\sigma_1(\alpha) = 1 + \sqrt{2} \text{ e } \sigma_2(\alpha) = 1 - \sqrt{2}.$$

Como $1 + \sqrt{2}$ e $1 - \sqrt{2}$ são linearmente independentes sobre $\mathbb{Q}$, segue que $\{\sigma_1(\alpha), \sigma_2(\alpha)\}$ é uma base normal de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

Além dos conceitos e propriedades já vistos, temos ainda outra ferramenta, a qual é de fundamental importância para os propósitos deste texto, o celebrado Lema de Dedekind.

Lema 1.1.15 (Dedekind)**.** *Sejam K e L corpos e $\sigma_1, ..., \sigma_n$ distintos homomorfismos de K em L. Então $\sigma_1, ..., \sigma_n$ são linearmente independentes sobre L, isto é, se existem elementos $x_1, ..., x_n \in L$ tais que $\sum_{i=1}^{n} x_i\sigma_i(a) = 0$, $\forall a \in K$, então necessariamente $x_1 = ... = x_n = 0$.*

Graças a esse lema podemos afirmar que, dada uma extensão de corpos L/K finita, o grupo $G = Aut_K L$ dos K-automorfismos de L é um subconjunto da L-álgebra $End_K L$ linearmente independente sobre L. Este fato assegura que a L-álgebra $End_K L$ contém uma cópia isomorfa da L-álgebra $L \star G$, a qual é chamada a skew álgebra do grupo G sobre K. Como um L-espaço vetorial, $L \star G$ tem base indexada $\{u_\sigma | \sigma \in G\}$. Sua multiplicação é induzida pela regra:

$$(xu_\sigma)(yu_\tau) = x\sigma(y)u_{\sigma\tau}, \ \forall x, y \in L \text{ e } \sigma, \tau \in G$$

e tem por elemento identidade $1_L u_{1_G}$.

A aplicação L-linear que imerge $L \star G$ em $End_K L$ é dada por $\varphi : L \star G \to End_K L$ tal que para todo $x \in L$ tem-se:

$$\varphi(\sum_{\sigma \in G} a_\sigma u_\sigma)(x) = \sum_{\sigma \in G} a_\sigma \sigma(x).$$

É fácil ver que φ é um monomorfismo de L-álgebras, graças ao Lema de Dedekind. Mais ainda, veremos na próxima seção que φ é um epimorfismo de L-álgebras se, e somente se, L/K é galoisiana.

Mais uma importante consequência do Lema de Dedekind que será de suma importância no início da demonstração do Teorema-Definição é o lema que se segue.

Lema 1.1.16. *Sejam L um corpo e G um subgrupo finito do grupo dos automorfismos de L. Então,*

$$dim_{L^G} L = |G|,$$

onde $L^G = \{x \in L \mid \sigma(x) = x,\ \forall \sigma \in G\}$.

1.2 Teorema-Definição

Agora estamos em condições de apresentar as diversas equivalências da noção de extensão de Galois, as quais estão listadas no Teorema seguinte. Além disso, note que todas as afirmações do Teorema 1.2.1 são trivialmente equivalentes quanto $K = L$, portanto vamos apenas considerar os casos em que $K \neq L$.

Teorema 1.2.1. *Sejam L/K extensão finita de corpos e $G = Aut_K L$. As seguintes condições são equivalentes:*

(i) $K = L^G$.

(ii) $|G| = dim_K L$.

(iii) Todo polinômio irredutível $p(x) \in K[x]$ que tem uma raiz em L se decompõe em um produto de fatores lineares distintos em $L[x]$.

(iv) L é o corpo de decomposição de algum polinômio separável $f(x) \in K[x]$.

(v) A extensão L/K é normal e separável.

(vi) A aplicação $\varphi : L \star G \to End_K L$ induzida por:

$$\varphi(xu_\sigma)(y) = x\sigma(y), \forall x, y \in L \text{ e } \sigma \in G$$

é um isomorfismo de K-álgebras.

(vii) A aplicação $\psi : L \otimes_K L \to \overbrace{L \times ... \times L}^{|G| \text{ vezes}}$ induzida por:

$$\psi(x \otimes y) = (x\sigma(y))_{\sigma \in G}, \forall x, y \in L \otimes_K L$$

é um isomorfismo de K-álgebras.

(viii) Existem elementos $x_i, y_i \in L$, $1 \leq i \leq m$, tais que:

$$\sum_1^m x_i \sigma(y_i) = \delta_{1_G,\sigma},\ \forall \sigma \in G.$$

(ix) Para cada $\sigma \in G$, com $\sigma \neq 1_G$ existe $x \in L$ tal que:

$$\sigma(x) \neq x.$$

Demonstração. **(i)⇒(ii)**

Esta implicação segue direto do Lema 1.1.16.

(ii)⇒(i)

A ideia agora é mostrar que $dim_K L^G = 1$ e concluir que $K = L^G$. Para tal, usaremos o Lema 1.1.16. Considere a seguinte torre de extensão de corpos:

$$K \subseteq L^G \subseteq L.$$

Assim, podemos comparar as dimensões da seguinte forma:

$$\overbrace{K \subseteq \underbrace{L^G \subseteq L}_{dim_{L^G} L = |G|}}^{dim_K L \overset{(1)}{=} |G|}.$$

(1) Segue da hipótese de (ii). Assim temos que $dim_K L^G = 1$, como queríamos mostrar.

(iii) ⇒ (iv)

Seja $\alpha_1 \in L \setminus K$. Como L/K é uma extensão finita pela hipótese do Teorema, α_1 deve ser algébrico sobre K.

Então $p_{\alpha_1/K}(x)$ por hipótese é separável sobre L e L contém seu corpo de decomposição K_1.

Se $K_1 = L$ a demostração está feita.

Considere $K_1 \neq L$, escolha arbitrariamente $\alpha_2 \in L \setminus K_1$. Como L/K_1 é uma extensão finita, α_2 deve ser algébrico sobre K_1 e, por hipótese, o polinômio irredutível $p_{\alpha_2/K}(x)$ é separável sobre L e L contém seu corpo de decomposição K_2.

Se $K_2 = L$ a demostração está feita, caso contrário repetimos o argumento feito anteriormente.

Note que este processo deve ter fim, pois L/K é finita, portanto podemos assegurar que após um número finito de etapas obteremos elementos $\alpha_1, ..., \alpha_n \in L$ tais que $L = K(\alpha_1, ..., \alpha_n)$ e L será o corpo de decomposição do polinômio separável:

$$p(x) = \prod_1^n p_{\alpha_i/K}(x) \in K[x].$$

(iv) ⇒(ii)
Segue do Teorema 1.1.10.

(i)⇒(v)
Seja L/K uma extensão de Galois, isto é $K = L^G$. Considere $G = \{\sigma_1 = 1_G, ..., \sigma_n\}$, e $a \in L \setminus K$. Denote por $\{a_1 = a, ..., a_r\}$ os elementos distintos entre $\sigma_1(a), ..., \sigma_n(a)$, isto é, $r \leq n$. Como $(G, \circ)$ é um grupo, se nós aplicarmos um destes elementos, digamos σ_i, em $\{a_1 = a, ..., a_r\}$ nós obtemos:

$$\sigma_i(a_j) = \sigma_i(\sigma_j(a)) = \sigma_h(a)$$
$$com\ \sigma_h = \sigma_i \circ \sigma_j.$$

Então os elementos de G serão permutações de $\{a_1 = a, ..., a_r\}$. Além disso, temos como consequência que os coeficientes do polinômio $f(x) = (x-a_1)...(x-a_r)$ estão em $L^G = K$. Em outras palavras, $f(x) \in K[x]$ e suas raízes, além de estarem em $L \setminus K$, são distintas duas a duas. Na sequência, vamos mostrar que $f(x)$ é, de fato, o polinômio mínimo de a sobre K.

Para tanto, é suficiente provar que $f(x)$ é um polinômio irredutível em $K[x]$. Seja $g(x)$ um fator irredutível de $f(x)$ em $K[x]$ tal que $g(a_i) = 0$, para algum $i \in \{1, ..., r\}$. Como $a_i = \sigma_i(a)$ e $a_j = \sigma_j(a)$ com $i, j \in \{1, ..., r\}$ e $i \neq j$, então:

$$\begin{aligned} a_j &= \sigma_j(a) \\ &= \sigma_j\sigma_i^{-1}(a_i). \end{aligned}$$

Já que:

$$a_i = \sigma_i(a) \Leftrightarrow \sigma_i^{-1}(a_i) = a.$$

Assim, $a_j = \sigma_j\sigma_i^{-1}(a_i)$. Como $g(x) \in K[x]$ e $K = L^G$, temos que:

$$0 = \sigma_j\sigma_i^{-1}g((a_i)) = g(\sigma_j\sigma_i^{-1}(a_i)) = g(a_j).$$

Então ambos os polinômios $f(x)$ e $g(x)$ tem as mesmas raízes, o que implica que $f(x)$ é irredutível. Mostramos que todo o elemento $a \in L$ é separável e que $p_{a/K}$ se fatora totalmente em um produto de fatores lineares em $L[x]$, logo a extensão é normal e separável.

(v)⇒(iii)
Se L é extensão normal de K, então todo polinômio irredutível em $K[x]$ se fatora em produto de fatores lineares em $L[x]$. Além disso, como a extensão é separável, todo elemento $\alpha \in L$ é separável, isto é, $p_{\alpha/K}$ não possui

raízes repetidas, o que implica que todo polinômio irredutível $p(x) \in K[x]$ não possui raízes repetidas em L.

(ii)⇒(vi)

Primeiro vamos mostrar que segue imediatamente da sua definição que φ sempre será, de fato, um homomorfismo de K-álgebras. Para tal, considere $k \in K,\ x,\ y,\ z \in L$ e $\sigma,\ \tau \in G$:

- φ é K-linear.

$$\begin{aligned}\varphi(kxu_\sigma + zu_\sigma)(y) &= (kx\sigma + z\sigma)(y)\\ &= kx\sigma(y) + z\sigma(y)\\ &= k(x\sigma(y)) + (z\sigma(y))\\ &= k\varphi(xu_\sigma)(y) + \varphi(zu_\sigma)(y).\end{aligned}$$

- φ é homomorfismo de K-álgebras.

$$\begin{aligned}\varphi(xu_\sigma zu_\tau)(y) &= \varphi(x\sigma(z)u_{\sigma\tau})(y)\\ &= (x\sigma(z))(\sigma\circ\tau)(y)\\ &= (x\sigma(z))(\sigma(\tau(y)))\\ &= (x)(\sigma(z))(\sigma(\tau(y)))\\ &= (x)(\sigma(z\tau(y)))\\ &= \varphi(xu_\sigma)(z\tau(y))\\ &= \varphi(xu_\sigma)(\varphi(zu_\tau)(y))\\ &= \varphi(xu_\sigma)\circ\varphi(zu_\tau)(y).\end{aligned}$$

$$\begin{aligned}\varphi(1_L u_{1_G})(y) &= 1_L 1_G(y)\\ &= y,\ \forall y \in L\ \Rightarrow \varphi(1_L u_{1_G}) = id_L.\end{aligned}$$

- φ é bijeção.

A injetividade de φ segue do Lema de Dedekind. Já a sobrejetividade é uma consequência da comparação de dimensões. De fato, note que:

$$dim_K(L \star G) = dim_K L.dim_L(L \star G).$$

Mas sabemos que $L \star G$ é um L-espaço vetorial de base $\{u_\sigma | \sigma \in G\}$, então $dim_L L \star G = |G|$. E por hipótese sabemos que $dim_K L = |G|$. Assim:

$$dim_K(L \star G) = (|G|)^2.$$

Por outro lado, é bem conhecido que para $dim_K L = n$, $End_K L \simeq M_n(K)$, e que $dim_K M_n(K) = n^2$. Portanto:

$$dim_K(L \star G) = (|G|)^2 = n^2 = dim_K M_n(K) = dim_K End_K L.$$

(vi)⇒(ii)

Sabemos, por hipótese, que $L \star G \simeq End_K(L)$, então:

$$(dim_K L)^2 = dim_K M_n(K) = dim_K End_K(L) = dim_K L \star G = dim_K L|G|.$$

O que implica que:

$$|G| = dim_K L.$$

(ii)⇒(vii)

Primeiro observe que segue imediatamente da sua definição que ψ sempre será um homomorfismo de K-álgebras pelo fato de todos os elementos de G serem homomorfismos de K-álgebras.

Agora precisamos mostrar a injetividade. Seja $G = \{\sigma_1 = 1_G, \sigma_2, ..., \sigma_n\}$. Sabemos, pelo Teorema 1.1.13, que existe $\alpha \in L$ tal que $\{\alpha_i = \sigma_i(\alpha) \mid 1 \leq i \leq n\}$ é uma base normal da extensão L/K. Logo, para todo elemento $x \in L \otimes_K L$ existem elementos $x_i \in K$, $1 \leq i \leq n$, tais que:

$$x = \sum_{i=1}^{n} x_i \otimes \alpha_i.$$

Se $x \in Ker(\psi)$ então $\sum_{i=1}^{n} x_i \sigma_j(\alpha_i) = 0 \ \forall j \in \{1, ..., n\}$, ou ainda:

$$(\sigma_j(\alpha_i))(x_i) = 0.$$

Pelo Lema 1.1.12 a matriz $(\sigma_j(\alpha_i))$ é invertível em $M_n(L)$, portanto $x_i = 0 \ \forall i \in \{1, ..., n\}$, ou seja, $x = 0$.

Para mostrar que é sobrejetor basta observar que:

$$\begin{aligned} dim_K L \otimes L &= (dim_K L)^2 \\ &= dim_K L.(|G|) \\ &= dim_K L.dim_L L^{|G|} \\ &= dim_K L^{|G|}. \end{aligned}$$

(vii)⇒(ii)

Como ψ é um isomorfismo de K-álgebras temos que a igualdade (1) abaixo ocorre.

$$\begin{aligned} dim_K L \otimes L &= (dim_K L)^2 \\ &= dim_K L.dim_K L \\ &\overset{(1)}{=} dim_K L^{|G|} \\ &= dim_K L.dim_L L^{|G|} \\ &= dim_K L.(|G|). \end{aligned}$$

De onde segue que $dim_K L = |G|$.

(vii)⇒(viii)

Como ψ é um isomorfismo de K-álgebras sabemos que dado $(1, 0, ..., 0) \in \overbrace{L \times ... \times L}^{|G|=n}$, existe $\sum_{i=1}^{m} x_i \otimes y_i \in L \otimes_K L$ tal que:

$$\psi(\sum_{i=1}^{m} x_i \otimes y_i) = (1, 0, ..., 0).$$

Mas note que, pela definição de ψ, temos:

$$\psi(\sum_{i=1}^{m} x_i \otimes y_i) = (\sum_{i=1}^{m} x_i \sigma(y_i))_{\sigma \in G}$$

o que implica que:

$$(\sum_{i=1}^{m} x_i \sigma(y_i))_{\sigma \in G} = (1, 0, ..., 0)$$

que é o mesmo que dizer que:
$\exists x_i, y_i \in L$, com $1 \leq i \leq m$, tais que:

$$\sum_{i=1}^{m} x_i \sigma(y_i) = \begin{cases} 1, \ se \ 1_G = \sigma \\ 0, se \ 1_G \neq \sigma, \end{cases}$$

$\forall \sigma \in G$.

(viii)⇒(vi)

Note que φ é um homomorfismo de K-álgebras por definição. Além disso, a injetividade de φ segue do Lema de Dedekind. Portanto basta mostrar que φ é sobrejetor. Tome h um elemento qualquer em $End_K L$ e considere:

$$\omega = \sum_{\sigma \in G} \sum_{i=1}^{m} h(x_i)\sigma(y_i)u_\sigma,$$

com $x_i, \ y_i \in L$ satisfazendo (viii).

Assim, $\forall x \in L$, temos:

$$\begin{aligned}
\varphi(\omega)(x) &= \varphi(\sum_{\sigma\in G}\sum_{i=1}^{m} h(x_i)\sigma(y_i)u_\sigma)(x)\\
&= \sum_{\sigma\in G}\sum_{i=1}^{m} h(x_i)\sigma(y_i)\sigma(x)\\
&= \sum_{i=1}^{m} h(x_i)h(\sum_{\sigma\in G}\sigma(y_i)\sigma(x))\\
&= \sum_{i=1}^{m} h((x_i)\sum_{\sigma\in G}\sigma(y_i)\sigma(x))\\
&= h(\sum_{\sigma\in G}\sum_{i=1}^{m}(x_i)\sigma(y_i)\sigma(x))\\
&= h(1_G(x))\\
&= h(x).
\end{aligned}$$

Ou seja, $\varphi(w) = h$.

(ix)⇒(viii)

Por hipótese, dado $\tau \in G$, com $\tau \neq 1_G$, existem $a, b \in L$ tais que:

$$\tau(a) \neq a \;\; e \;\; b(\tau^{-1}(a) - a) = 1.$$

Então, tomando x_1, x_2, y_1, y_2:

$$x_1 = a,\; x_2 = 1 \; e \; y_1 = -b,\; y_2 = b\tau^{-1}(a)$$

temos que:

$$\sum_{i=1}^{2} x_i\tau(y_i) = \begin{cases} 1, \; se \; \tau = 1_G \\ 0, se \; \tau \neq 1_G. \end{cases}$$

De forma análoga, dados $\tau, \tau' \in G$, com ambos diferentes de 1_G, existem $x_i,\; x'_j, y_i,\; y'_j \in L$, com $i, j \in \{1, 2\}$, tais que:

$$\sum_{i=1}^{2} x_i\tau(y_i) = \begin{cases} 1, \; se \; \tau = 1_G \\ 0, se \; \tau \neq 1_G \end{cases}$$

$$\sum_{j=1}^{2} x'_j\tau'(y'_j) = \begin{cases} 1, \; se \; \tau' = 1_G \\ 0, se \; \tau' \neq 1_G. \end{cases}$$

Ou seja, $\forall \sigma \in \{1_G, \tau, \tau'\} = \{1_G, \tau\} \cup \{1_G, \tau'\}$ temos:

$$\sum_{i,j=1}^{2} x_i x'_j \sigma(y_i y'_j) = \begin{cases} 1, \ se \ \sigma = 1_G \\ 0, se \ \sigma \neq 1_G. \end{cases}$$

Finalmente, podemos afirmar que para cada elemento σ de G, existem elementos $x_{(1,\sigma)}, x_{(2,\sigma)}, y_{(1,\sigma)}, y_{(2,\sigma)} \in L$ tais que:

$$\sum_{i=1}^{2} x_{(i,\sigma)} \sigma(y_{(i,\sigma)}) = \begin{cases} 1, \ se \ \sigma = 1_G \\ 0, se \ \sigma \neq 1_G. \end{cases}$$

Além disso, como $G = \cup_{\sigma \neq 1_G} \{1_G, \sigma\}$, então conseguimos construir $x_i, y_i \in L$, com $i \in \{1, ..., m\}$, tais que:

$$\sum_{i,j=1}^{m} x_i \sigma(y_i) = \begin{cases} 1, \ se \ \sigma = 1_G \\ 0, se \ \sigma \neq 1_G. \end{cases}$$

(i)⇒(ix)
É imediato porque $K \neq L$.

□

Seja L/K uma extensão de Galois. Os elementos $x_i, y_i \in L$ que satisfazem a afirmação (viii) do Teorema 1.2.1 são chamados de Coordenadas de Galois. Note que, como vimos na demonstração do teorema, estes elementos não são únicos e tampouco o número deles é constante, como ilustrado no exemplo a seguir.

Exemplo 1.2.2. Considere a extensão de corpos $\mathbb{Q}(\sqrt{p}, i)/\mathbb{Q}$, sendo p um número primo. Sabemos que $G = Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt{p}, i)) = \{\sigma_1, \sigma_2, \ \sigma_3, \ \sigma_4\}$, onde:

$$\begin{array}{rl} \sigma_1(\sqrt{p}) = \sqrt{p} & \sigma_1(i) = i \\ \sigma_2(\sqrt{p}) = -\sqrt{p} & \sigma_1(i) = i \\ \sigma_3(\sqrt{p}) = \sqrt{p} & \sigma_1(i) = -i \\ \sigma_4(\sqrt{p}) = -\sqrt{p} & \sigma_1(i) = -i \end{array}$$

Sabemos que tomando as coordenadas abaixo temos o resultado esperado para $\{\sigma_1, \sigma_2\}$:

$$x_1 = \sqrt{p}, \ x_2 = 1 \ e \ y_1 = \frac{\sqrt{p}}{2p}, \ y_2 = \frac{1}{2}.$$

Agora vamos construir estas coordenadas para funcionar para σ_3, e mais tarde para σ_4. Tomaremos, $i \in \mathbb{Q}(\sqrt{p}, i)$ pois $\sigma(i) \neq i$, para algum $\sigma \in G$, que, nesse caso, é σ_3 o automorfismo que conjuga i. Assim obtemos:

$$x_3 = -i,\ x_4 = 1\ e\ y_3 = \frac{i}{2},\ y_4 = \frac{1}{2}.$$

Da mesma forma, tomaremos $\sqrt{p} \in \mathbb{Q}(\sqrt{p}, i)$ pois $\sigma_4(\sqrt{p}) \neq \sqrt{p}$. E assim obtemos:

$$x_5 = \sqrt{p},\ x_6 = 1\ e\ y_5 = \frac{\sqrt{p}}{2p},\ y_6 = \frac{1}{2}.$$

Agora basta tomar as Coordenadas de Galois da extensão $\mathbb{Q}(\sqrt{p}, i)/\mathbb{Q}$ da seguinte forma:

$$\begin{array}{ll} X_1 = x_1x_3x_5 & Y_1 = y_1y_3y_5 \\ X_2 = x_1x_3x_6 & Y_2 = y_1y_3y_6 \\ X_3 = x_1x_4x_5 & Y_3 = y_1y_4y_5 \\ X_4 = x_1x_4x_6 & Y_4 = y_1y_4y_6 \\ X_5 = x_2x_3x_5 & Y_5 = y_2y_3y_5 \\ X_6 = x_2x_3x_6 & Y_6 = y_2y_3y_6 \\ X_7 = x_2x_4x_6 & Y_7 = y_2y_4y_6 \\ X_8 = x_2x_4x_5 & Y_8 = y_2y_4y_5 \end{array}$$

assim obtemos:

$$\begin{array}{rl} X_1 = -pi & Y_1 = \dfrac{i}{8p} \\ X_2 = -\sqrt{p}i & Y_2 = \dfrac{\sqrt{p}i}{8p} \\ X_3 = p & Y_3 = \dfrac{1}{8p} \\ X_4 = \sqrt{p} & Y_4 = \dfrac{\sqrt{p}}{8p} \\ X_5 = -\sqrt{p}i & Y_5 = \dfrac{\sqrt{p}i}{8p} \\ X_6 = -i & Y_6 = \dfrac{i}{8} \\ X_7 = 1 & Y_7 = \dfrac{1}{8} \\ X_8 = \sqrt{p} & Y_8 = \dfrac{\sqrt{p}}{8p}. \end{array}$$

Vamos testar as Coordenadas para σ_1:

$$X_1\sigma_1(Y_1) + X_2\sigma_1(Y_2) + X_3\sigma_1(Y_3) + X_4\sigma_1(Y_4)$$

$$+X_5\sigma_1(Y_5) + X_6\sigma_1(Y_6) + X_7\sigma_1(Y_7) + X_8\sigma_1(Y_8)$$

$$= X_1Y_1 + X_2Y_2 + X_3Y_3 + X_4Y_4 + X_5Y_5 + X_6Y_6 + X_7Y_7 + X_8Y_8$$

$$= (-pi)(\frac{i}{8p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (p)(\frac{1}{8p}) + (\sqrt{p})(\frac{\sqrt{p}}{8p})$$

$$+(-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (-i)(\frac{i}{8}) + (1)(\frac{1}{8}) + (\sqrt{p})(\frac{\sqrt{p}}{8p}) = 1.$$

Testando para σ_2 temos:

$$X_1\sigma_2(Y_1) + X_2\sigma_2(Y_2) + X_3\sigma_2(Y_3) + X_4\sigma_2(Y_4)$$

$$+X_5\sigma_2(Y_5) + X_6\sigma_2(Y_6) + X_7\sigma_2(Y_7) + X_8\sigma_2(Y_8)$$

$$= X_1Y_1 + X_2(-Y_2) + X_3Y_3 + X_4(-Y_4) + X_5(-Y_5) + X_6Y_6 + X_7Y_7 + X_8(-Y_8)$$

$$= (-pi)(\frac{i}{8p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (p)(\frac{1}{8p}) + (\sqrt{p})(-\frac{\sqrt{p}}{8p})$$

$$+(-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (-i)(\frac{i}{8}) + (1)(\frac{1}{8}) + (\sqrt{p})(-\frac{\sqrt{p}}{8p}) = 0.$$

Analogamente para σ_3 obtemos:

$$X_1\sigma_3(Y_1) + X_2\sigma_3(Y_2) + X_3\sigma_3(Y_3) + X_4\sigma_3(Y_4)$$

$$+X_5\sigma_3(Y_5) + X_6\sigma_3(Y_6) + X_7\sigma_3(Y_7) + X_8\sigma_3(Y_8)$$

$$= X_1(-Y_1) + X_2(-Y_2) + X_3Y_3 + X_4Y_4 + X_5(-Y_5) + X_6(-Y_6) + X_7Y_7 + X_8Y_8$$

$$= (-pi)(-\frac{i}{8p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (p)(\frac{1}{8p}) + (\sqrt{p})(\frac{\sqrt{p}}{8p})$$

$$+(-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (-i)(-\frac{i}{8}) + (1)(\frac{1}{8}) + (\sqrt{p})(\frac{\sqrt{p}}{8p}) = 0.$$

Finalmente testando para σ_4 temos:

$$X_1\sigma_4(Y_1) + X_2\sigma_4(Y_2) + X_3\sigma_4(Y_3) + X_4\sigma_4(Y_4)$$

$$+X_5\sigma_4(Y_5) + X_6\sigma_4(Y_6) + X_7\sigma_4(Y_7) + X_8\sigma_4(Y_8)$$

$$= X_1(-Y_1) + X_2Y_2 + X_3Y_3 + X_4(-Y_4) + X_5Y_5 + X_6(-Y_6) + X_7Y_7 + X_8(-Y_8)$$

$$= (-pi)(-\frac{i}{8p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (p)(\frac{1}{8p}) + (\sqrt{p})(-\frac{\sqrt{p}}{8p})$$

$$+(-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (-i)(-\frac{i}{8}) + (1)(\frac{1}{8}) + (\sqrt{p})(-\frac{\sqrt{p}}{8p}) = 0.$$

Note que podemos diminuir o número de Coordenadas de Galois, basta tomar:

$$\begin{aligned} X_1 = -pi \quad & Y_1 = \frac{i}{4p} \\ X_2 = -\sqrt{p}i \quad & Y_2 = \frac{\sqrt{p}i}{4p} \\ X_3 = p \quad & Y_3 = \frac{1}{4p} \\ X_4 = \sqrt{p} \quad & Y_4 = \frac{\sqrt{p}}{4p}. \end{aligned}$$

Vamos testar para σ_1:

$$X_1\sigma_1(Y_1) + X_2\sigma_1(Y_2) + X_3\sigma_1(Y_3) + X_4\sigma_1(Y_4)$$

$$= X_1Y_1 + X_2Y_2 + X_3Y_3 + X_4Y_4$$

$$= (-pi)(\frac{i}{4p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{4p}) + (p)(\frac{1}{4p}) + (\sqrt{p})(\frac{\sqrt{p}}{4p}) = 1.$$

Testando as Coordenadas para σ_2 obtemos:

$$X_1\sigma_2(Y_1) + X_2\sigma_2(Y_2) + X_3\sigma_2(Y_3) + X_4\sigma_2(Y_4)$$

$$= X_1Y_1 + X_2(-Y_2) + X_3Y_3 + X_4(-Y_4)$$

$$= (-pi)(\frac{i}{4p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{4p}) + (p)(\frac{1}{4p}) + (\sqrt{p})(-\frac{\sqrt{p}}{4p}) = 0.$$

Da mesma forma, testando as Coordenadas para σ_3 obtemos:

$$X_1\sigma_3(Y_1) + X_2\sigma_3(Y_2) + X_3\sigma_3(Y_3) + X_4\sigma_3(Y_4)$$

$$= X_1(-Y_1) + X_2(-Y_2) + X_3Y_3 + X_4Y_4$$

$$= (-pi)(-\frac{i}{4p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{4p}) + (p)(\frac{1}{4p}) + (\sqrt{p})(\frac{\sqrt{p}}{4p}) = 0.$$

E, testanto para σ_4 também obtemos o desejado. De fato:

$$X_1\sigma_4(Y_1) + X_2\sigma_4(Y_2) + X_3\sigma_4(Y_3) + X_4\sigma_4(Y_4)$$

$$= X_1(-Y_1) + X_2Y_2 + X_3Y_3 + X_4(-Y_4)$$

$$= (-pi)(-\frac{i}{4p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{4p}) + (p)(\frac{1}{4p}) + (\sqrt{p})(-\frac{\sqrt{p}}{4p}) = 0.$$

Ainda podemos modificar as Coordenas de Galois escolhendo:

$$x_1 = \sqrt{p},\ x_2 = 1\ e\ y_1 = \frac{\sqrt{p}}{2p},\ y_2 = \frac{1}{2},$$

$$x_3 = -i,\ x_4 = 1\ e\ y_3 = \frac{i}{2},\ y_4 = \frac{1}{2}$$

e modificando $x_5,\ x_6,\ y_5,\ y_6$. Fazemos isso, tomando $i \in \mathbb{Q}(\sqrt{p}, i)$, pois sabemos que $\sigma_4(i) \neq i$. Assim obtemos:

$$x_5 = -i,\ x_6 = 1\ e\ y_5 = \frac{i}{2p},\ y_6 = \frac{1}{2}.$$

Agora basta tomar as Coordenadas de Galois da extensão $\mathbb{Q}(\sqrt{p}, i)/\mathbb{Q}$ da mesma forma de antes, obtendo:

$$\begin{aligned} X_1 = -\sqrt{p} \quad & Y_1 = \frac{-\sqrt{p}}{8p} \\ X_2 = -\sqrt{p}i \quad & Y_2 = \frac{\sqrt{p}i}{8p} \\ X_3 = -\sqrt{p}i \quad & Y_3 = \frac{\sqrt{p}i}{8p} \\ X_4 = \sqrt{p} \quad & Y_4 = \frac{\sqrt{p}}{8p} \\ X_5 = -1 \quad & Y_5 = \frac{-1}{8} \\ X_6 = -i \quad & Y_6 = \frac{i}{8} \\ X_7 = 1 \quad & Y_7 = \frac{1}{8} \\ X_8 = -i \quad & Y_8 = \frac{i}{8}. \end{aligned}$$

Vamos testar para σ_1:

$$X_1\sigma_1(Y_1) + X_2\sigma_1(Y_2) + X_3\sigma_1(Y_3) + X_4\sigma_1(Y_4)$$

$$+X_5\sigma_1(Y_5) + X_6\sigma_1(Y_6) + X_7\sigma_1(Y_7) + X_8\sigma_1(Y_8)$$

$$= X_1Y_1 + X_2Y_2 + X_3Y_3 + X_4Y_4 + X_5Y_5 + X_6Y_6 + X_7Y_7 + X_8Y_8$$

$$= (-\sqrt{p})(-\frac{\sqrt{p}}{8p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (\sqrt{p})(\frac{\sqrt{p}}{8p})$$

$$+(-1)(\frac{-1}{8}) + (-i)(\frac{i}{8}) + (1)(\frac{1}{8}) + (-i)(\frac{i}{8}) = 1.$$

Testando para σ_2 temos que:

$$X_1\sigma_2(Y_1) + X_2\sigma_2(Y_2) + X_3\sigma_2(Y_3) + X_4\sigma_2(Y_4)$$

$$+X_5\sigma_2(Y_5) + X_6\sigma_2(Y_6) + X_7\sigma_2(Y_7) + X_8\sigma_2(Y_8)$$

$$= X_1(-Y_1) + X_2(-Y_2) + X_3(-Y_3) + X_4(-Y_4) + X_5Y_5 + X_6Y_6 + X_7Y_7 + X_8Y_8$$

$$= (-\sqrt{p})(\frac{\sqrt{p}}{8p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (\sqrt{p})(-\frac{\sqrt{p}}{8p})$$

$$+(-1)(\frac{-1}{8}) + (-i)(\frac{i}{8}) + (1)(\frac{1}{8}) + (-i)(\frac{i}{8}) = 0.$$

De forma análoga, testando para σ_3 obtemos:

$$X_1\sigma_3(Y_1) + X_2\sigma_3(Y_2) + X_3\sigma_3(Y_3) + X_4\sigma_3(Y_4)$$

$$+X_5\sigma_3(Y_5) + X_6\sigma_3(Y_6) + X_7\sigma_3(Y_7) + X_8\sigma_3(Y_8)$$

$$= X_1Y_1 + X_2(-Y_2) + X_3(-Y_3) + X_4Y_4 + X_5Y_5 + X_6(-Y_6) + X_7Y_7 + X_8(-Y_8)$$

$$= (-\sqrt{p})(-\frac{\sqrt{p}}{8p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (-\sqrt{p}i)(-\frac{\sqrt{p}i}{8p}) + (\sqrt{p})(\frac{\sqrt{p}}{8p})$$

$$+(-1)(\frac{-1}{8}) + (-i)(-\frac{i}{8}) + (1)(\frac{1}{8}) + (-i)(-\frac{i}{8}) = 0.$$

E o desejado também se encontra testando para σ_4:

$$X_1\sigma_4(Y_1) + X_2\sigma_4(Y_2) + X_3\sigma_4(Y_3) + X_4\sigma_4(Y_4)$$

$$+X_5\sigma_4(Y_5) + X_6\sigma_4(Y_6) + X_7\sigma_4(Y_7) + X_8\sigma_4(Y_8)$$

$$= X_1(-Y_1) + X_2Y_2 + X_3Y_3 + X_4(-Y_4) + X_5Y_5 + X_6(-Y_6) + X_7Y_7 + X_8(-Y_8)$$

$$= (-\sqrt{p})(\frac{\sqrt{p}}{8p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (-\sqrt{p}i)(\frac{\sqrt{p}i}{8p}) + (\sqrt{p})(-\frac{\sqrt{p}}{8p})$$

$$+(-1)(\frac{-1}{8}) + (-i)(-\frac{i}{8}) + (1)(\frac{1}{8}) + (-i)(-\frac{i}{8}) = 0.$$

Capítulo 2

Um atalho para a Teoria de Galois

No decorrer deste trabalho lançaremos mão de muitas ferramentas que serão usadas para estudar a assim chamada Correspondência de Galois-Grothendieck segundo a visão de A. Dress que, em [4], a desenvolveu especificamente para apresentá-la através de um atalho construído, tendo como argumento principal o Lema de Dedekind e algumas propriedades básicas da teoria de G-conjuntos. Para que o leitor fique a par desses resultados e definições, apresentaremos aqui um breve resumo de tais propriedades.

2.1 Lema de Dedekind

Considere L/K uma extensão de corpos. Denotaremos por $Hom_K(A, L)$ o K-espaço vetorial de todas as aplicações K-lineares de uma K-álgebra A em L. Além disso, também trabalharemos com $Alg_K(A, L)$, o subconjunto de $Hom_K(A, L)$ dos homomorfismos de K-álgebras de A em L.

O Lema de Dedekind visto no capítulo anterior pode ser estendido para o contexto de álgebras da forma que se segue. No caso específico em que A é um corpo reobtemos o clássico Lema de Dedekind enunciado na Seção 1.1.

Lema 2.1.1 (Lema de Dedekind)**.** *Sejam L/K uma extensão de corpos e A uma K-álgebra. Então $Alg_K(A, L)$ é um subconjunto linearmente independente de $Hom_K(A, L)$.*

Demonstração. Vamos supor, por absurdo, que $\varphi_1, ..., \varphi_n \in Alg_K(A, L)$ sejam linearmente dependentes sobre L. Ou seja, estamos supondo que existem

elementos $x_1, .., x_n \in L$ não todos nulos tais que, $\forall a \in A$:

$$\sum_{i=1}^{n} x_i \varphi_i(a) = 0. \tag{2.1}$$

Desprezando os coeficientes nulos da combinação linear 2.1, podemos supor, sem perda de generalidade, que $x_i \neq 0 \ \forall i \in \{1, .., n\}$.

Se $n = 1$ então temos, em particular, que:

$$0 = x_1 \varphi_1(a), \ \forall a \in A \Rightarrow x_1 = 0$$

o que é um absurdo. Então, consideraremos $n > 1$. Adicionalmente, podemos assumir que n é mínimo tal que 2.1 aconteça, e, além disso, que $x_n = 1$, pois L é corpo.

Assim, $\forall a, b \in A$ tem-se:

$$\sum_{i=1}^{n-1} (x_i \varphi_i(a) - x_i \varphi_n(a)) \varphi_i(b)$$

$$= \sum_{i=1}^{n} (x_i \varphi_i(a) - x_i \varphi_n(a)) \varphi_i(b)$$

$$= \sum_{i=1}^{n} x_i \varphi_i(ab) - \varphi_n(a) \sum_{i=1}^{n} x_i \varphi_i(b) = 0.$$

Donde decorre, devido a minimalidade de n que:

$$x_i \varphi_i(a) = x_i \varphi_n(a), \ \forall a \in A \ e \ i \in \{1, ..., n-1\},$$

então $\varphi_n = \varphi_i$, para algum $i \in \{1, 2, ..., n-1\}$, o que contradiz a minimalidade de n. Logo $\varphi_1, ..., \varphi_n$ são L-independentes. □

Decorre imediatamente do Lema de Dedekind que o número $\#Alg_K(A, L)$ é delimitado por $dim_L Hom_K(A, L)$.

Proposição 2.1.2. *Seja A uma K-álgebra. Se A tem dimensão finita como um K-espaço vetorial então $Hom_K(A, L)$, como um L-espaço vetorial, tem dimensão finita e, além disso,*

$$dim_K A = dim_L Hom_K(A, L).$$

Demonstração. Considere $\{a_1, a_2, ..., a_n\}$ uma base de A como um K-espaço vetorial. Para concluir o que queremos, basta observar que a aplicação α dada a seguir é um isomorfismo:

$$\begin{aligned} \alpha : Hom_K(A, L) &\to L^n \\ \varphi &\mapsto (\varphi(a_1), \varphi(a_2), ..., \varphi(a_n)) \end{aligned}$$

- α está bem definida.
  De fato, como $\varphi : A \to L$, então $\varphi(a_i) \in L,\ \forall\ i \in \{1, 2, ..., n\}$.
- α é K-linear.
  Observe que a K-linearidade de α decorre da K-linearidade de φ.
- α é injetiva.
  $(\varphi(a_1), \varphi(a_2), ..., \varphi(a_n)) = (0, ..., 0) \Rightarrow \varphi(a_i) = 0\ \forall i \in \{1, 2, ..., n\}$. Como $\{a_1, a_2, ..., a_n\}$ é uma base de A então todo $a \in A$ pode ser escrito como $\sum_{i=1}^{n} x_i a_i = a$, e consequentemente temos que:

$$\begin{aligned} \varphi(a) &= \varphi(\sum_{i=1}^{n} x_i a_i) \\ &= \sum_{i=1}^{n} x_i \varphi(a_i) \\ &= 0 \end{aligned}$$

  assim, $\varphi(a) = 0\ \forall a \in A$, isto é: $\varphi = 0$.
- α é sobrejetiva.
  Basta tomar $(x_1, x_2, ..., x_n) \in L^n$, e $\varphi \in Hom_K(A, L)$ tal que $\varphi(a_i) = x_i$. Logo α é sobrejetiva. □

A proposição a seguir, que também pode ser vista como uma consequência do Lema de Dedekind, será de extrema utilidade para o desenvolvimento do próximo capítulo.

Proposição 2.1.3. *Seja L um corpo e G um grupo finito de automorfismos de L. Considere:*

- $K = L^G = \{x \in L \mid \sigma(x) = x,\ \forall \sigma \in G\}$.
- *W um L-espaço vetorial sobre o qual G atua semilinearmente, isto é:* $\sigma(x.w) = \sigma(x)\sigma(w), \forall \sigma \in G, x \in L$ *e* $w \in W$.

Então o K-espaço vetorial $V = W^G = \{w \in W \mid \sigma(w) = w,\ \forall \sigma \in G\}$ gera livremente W como um L-espaço vetorial, isto é, qualquer K-base de V é também uma L-base de W.

Demonstração. Considere $\{v_1, v_2, ..., v_n\}$ uma K-base de $V = W^G$. Mostraremos que esta é também uma base de W sobre L.

Primeiro provaremos que $\{v_1, v_2, ..., v_n\}$ são linearmente independentes sobre L. Para tal, suponha, por absurdo, que existem elementos $x_1, .., x_n \in L$ não todos nulos tais que:

$$\sum_{i=1}^{n} x_i v_i = 0. \tag{2.2}$$

Desprezando os coeficientes nulos da combinação linear 2.2, podemos supor, sem perda de generalidade, que $x_i \neq 0\ \forall i \in \{1, .., n\}$.

Se $n = 1$ então temos que $0 = x_1 v_1$, mas como $\{v_1\}$ é uma K-base de $V = W^G$ temos que $0 = x_1$, o que é um absurdo. Suponha então que $n > 1$. Além disso, podemos assumir que n é mínimo tal que 2.2 acontece. Como L é corpo, podemos assumir que $x_n = 1$. Aplicando-se $\sigma \neq 1_G \in G$ em ambos os lados de 2.2 tem-se:

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(\sum_{i=1}^{n} x_i v_i) \\ &= \sum_{i=1}^{n} \sigma(x_i v_i) \\ &= \sum_{i=1}^{n} \sigma(x_i)\sigma(v_i) \\ &= \sum_{i=1}^{n} \sigma(x_i) v_i, \end{aligned}$$

pois $v_i \in V = W^G, \forall i \in \{1, 2, ..., n\}$.

Agora note que:

- $\sum_{i=1}^{n} \sigma(x_i) v_i - \sum_{i=1}^{n} x_i v_i = 0$, pois ambos são iguais a zero.
- $\sigma(x_n) = \sigma(1) = 1 = x_n$.

Então:

$$\sum_{i=1}^{n}(\sigma(x_i) - x_i)v_i = 0 = \sum_{i=1}^{n-1}(\sigma(x_i) - x_i)v_i.$$

Da minimalidade de n, decorre então que $\sigma(x_i) = x_i, \forall i \in \{1, 2, ..., n\}$. Entretanto, se tal fato ocorresse, teríamos que:

$$x_i \in K = L^G, \forall i \in \{1, 2, ..., n\}$$

o que contradiz o fato de $\{v_1, v_2, ..., v_n\}$ serem K-linearmente independentes.

Para mostrar que W é gerado por $V = W^G$ como um L-espaço vetorial é suficiente mostrar que toda a aplicação L-linear $f : W \to L$ que se anula em todo $v \in V$ deve se anular em W.

Considere, convenientemente, para cada $x \in L$ e $w \in W$, o elemento $\sum_{\sigma \in G} \sigma(xw)$. Note que esse elemento está em W^G. Supondo que f anule todo o elemento de $W^G = V$, temos que:

$$\begin{aligned} 0 &= f(\sum_{\sigma \in G} \sigma(xw)) \\ &= \sum_{\sigma \in G} f(\sigma(xw)) \\ &= \sum_{\sigma \in G} f(\sigma(x))f(\sigma(w)) \\ &= \sum_{\sigma \in G} \sigma(x)f(\sigma(w)). \end{aligned}$$

As duas últimas igualdades decorrem do fato de f ser L-linear e de que $\sigma(x) \in L$.

Analisando agora o último somatório temos que, pelo Lema de Dedekind, $f(\sigma(w)) = 0, \forall \sigma \in G$ e $\forall w \in W$. Em particular, para $\sigma = id_L$ temos:

$$0 = f(w) = f(\sigma(w)), \forall w \in W.$$

□

2.2 G-conjuntos

Nesta seção trataremos com G-conjuntos e veremos alguns resultados básicos que ajudarão a deduzir o Teorema da Correspondência de Galois-Grothendieck segundo o enfoque de A. Dress.

Definição 2.2.1. • Sejam X um conjunto e G um grupo. Dizemos que X é um G-conjunto quando X sofre uma ação de G, isto é, quando existir uma aplicação da forma:

$$\begin{aligned} G \times X &\to X \\ (\sigma, x) &\mapsto \sigma \cdot x \end{aligned}$$

que satisfaz as seguintes condições:

(i) $\forall \sigma, \tau \in G, \forall x \in X$ tem-se: $\tau \cdot (\sigma \cdot x) = \tau\sigma \cdot x$.

(ii) $\forall x \in X$ tem-se: $1_G \cdot x = x$.

- Considere X um G-conjunto. Definimos a parte invariante de X pela ação de G como sendo o subconjunto de X tal que:

$$X^G = \{x \in X \mid \sigma \cdot x \ = x, \ \forall \sigma \in G\}.$$

- Sejam X e Y dois G-conjuntos com as respectivas G-ações $\bullet$ e $*$. Um homomorfismo entre X e Y como G-conjuntos é uma aplicação $T : X \to Y$ tal que:

$$T(g \bullet x) = g * T(x).$$

Nesse caso, dizemos que T é uma G-aplicação.

Exemplo 2.2.2. Sejam L um corpo e $G = Aut(L)$, então L é um G-conjunto. De fato, considere a ação de G em L dada por:

$$\begin{aligned} G \times L &\to L \\ (\sigma, \ell) &\mapsto \sigma \cdot \ell = \sigma(\ell) \end{aligned}$$

Então:

(i) $\forall \sigma_1, \sigma_2 \in G, \forall \ell \in L$ tem-se: $\sigma_2 \cdot (\sigma_1 \cdot \ell) = \sigma_2\sigma_1 \cdot \ell$.
Note que este fato segue diretamente da definição da aplicação, pois:

$$\sigma_2 \cdot (\sigma_1 \cdot \ell) = \sigma_2(\sigma_1(\ell)) = \sigma_2\sigma_1 \cdot \ell.$$

(ii) $\forall \ell \in L$ tem-se: $1_G \cdot \ell = \ell$.

$$1_G \cdot \ell = id_L(\ell) = \ell.$$

Logo L é um G-conjunto segundo a G-ação dada acima.

Exemplo 2.2.3. Se S, T são G-conjuntos então o conjunto $Map(S,T)$ de todas as aplicações de S em T também é um G-conjunto via a ação induzida pelas ações de G sobre S e T respectivamente, da seguinte forma:

$$\begin{aligned} G \times Map(S,T) &\to Map(S,T) \\ (\sigma, f) &\mapsto \sigma \cdot f : S \to T \\ & \qquad s \mapsto \sigma \cdot f(\sigma^{-1} \cdot s) \end{aligned}$$

De fato:

(i) $\forall \sigma, \tau \in G, \forall f \in Map(S,T)$ tem-se: $\tau \cdot (\sigma \cdot f) = \tau\sigma \cdot f$.

$$\begin{aligned} (\tau \cdot (\sigma \cdot f))(s) &= \tau \cdot (\sigma(f(\sigma^{-1} \cdot s))) \\ &= \tau(\sigma(f(\sigma^{-1}(\tau^{-1} \cdot s)))) \\ &= ((\tau\sigma)(f)(\tau\sigma)^{-1})(s) \\ &= (\tau\sigma \cdot f)(s),\ \forall s \in S. \end{aligned}$$

(ii) $\forall f \in Map(S,T)$ tem-se: $1_G \cdot f = f$.

$$\begin{aligned} (1_G \cdot f)(s) &= 1_G(f(1_G^{-1} \cdot s)) \\ &= 1_G(f(s)) \\ &= f(s),\ \forall s \in S. \end{aligned}$$

Além disso, o conjunto $Map(S,T)^G$ coincide com o conjunto $Hom_G(S,T)$, pois:

$$f \in Map(S,T)^G \Leftrightarrow \sigma \cdot f = f, \forall \sigma \in G,$$

e então $(\sigma \cdot f)(s) = \sigma(f(\sigma^{-1}(s))),\ \forall s \in S \Leftrightarrow f = \sigma f \sigma^{-1} \Leftrightarrow f\sigma = \sigma f, \forall \sigma \in G$.

Observação 2.2.4. No exemplo 2.2.3, se T for um corpo e G for um subgrupo de $Aut(T)$, então $Map(S,T)$ é também uma T-álgebra com as operações usuais de adição e multiplicação pontuais e produto por escalar.

Exemplo 2.2.5. (i) Considere G um grupo e H um subgrupo de G. G é um H-conjunto via a ação induzida pela multiplicação de G. Note que, nesse caso:

$$G^H = \begin{cases} \varnothing, \ se\ |H| > 1 \\ G, se\ |H| = 1. \end{cases}$$

(ii) Considere G um grupo e H um subgrupo de G, então o conjunto $\frac{G}{H}$ das classes laterais à esquerda de H em G é um G-conjunto via a ação induzida pela multiplicação de G. De fato, considere a ação de G em $\frac{G}{H}$ dada da seguinte forma:

$$\begin{aligned} G \times \frac{G}{H} &\to \frac{G}{H} \\ (\sigma, \tau H) &\mapsto \sigma \cdot \tau H = \sigma\tau H \end{aligned}$$

Então:

(i) $\forall \sigma_1, \sigma_2 \in G, \forall \tau H \in \frac{G}{H}$ tem-se: $\sigma_2 \cdot (\sigma_1 \cdot \tau H) = \sigma_2\sigma_1 \cdot \tau H$.
Note que isto segue direto da definição da aplicação, pois:

$$\sigma_2 \cdot (\sigma_1 \cdot \tau H) = \sigma_2\sigma_1\tau H = \sigma_2\sigma_1 \cdot \tau H.$$

(ii) $\forall \tau H \in \frac{G}{H}$ tem-se: $1_G \cdot \tau H = \tau H$, pois

$$1_G \cdot \tau H = 1_G\tau H = \tau H.$$

Proposição 2.2.6. *Considere G um grupo, H um subgrupo de G e T um G-conjunto. A seguinte aplicação canônica*

$$\begin{aligned} \theta : Hom_G(\frac{G}{H}, T) &\to T^H \\ f &\mapsto f(H) \end{aligned}$$

é uma bijeção.

Demonstração. • θ está bem definida.

De fato, dado $f \in Hom_G(\frac{G}{H}, T) = Map(\frac{G}{H}, T)^G$ então: $\sigma f = f$, e consequentemente $\sigma f(H) = f(H), \forall \sigma \in G$.

• θ é injetiva.

Sejam $f_1, f_2 \in Hom_G(\frac{G}{H}, T)$ e considere $f_1(H) = f_2(H)$, então:

$$\begin{aligned} f_1(\sigma H) &= \sigma(f_1(H)) \\ &= \sigma(f_2(H)) \\ &= f_2(\sigma H) \end{aligned}$$

$$\begin{aligned} &\Rightarrow f_1(\sigma H) = f_2(\sigma H), \forall \sigma \in G \\ &\Rightarrow f_1 = f_2. \end{aligned}$$

Note que a primeira igualdade e a terceira seguem do fato que $f_1, f_2 \in Hom_G(\frac{G}{H}, T)$.

- θ é sobrejetiva.
  Vamos mostrar que:

$$\forall t \in T^H \ \exists f \in Hom_G(\frac{G}{H}, T) \mid \theta(f) = t.$$

Dado $t \in T^H$, considere $f \in Map(\frac{G}{H}, T)$ dada por $f(\sigma H) = \sigma(t)$, $\forall \sigma \in G$. Note que, em particular, $f(H) = t$. Resta portanto mostrar que $f \in Hom_G(\frac{G}{H}, T)$. De fato, $\forall \sigma, \tau \in G$ temos:

$$(\sigma \cdot f)(\tau H) = \sigma(f(\sigma^{-1}\tau H)) = \sigma(\sigma^{-1}\tau t) = \tau(t) = f(\tau H).$$

Assim provamos que é sobrejetiva, e portanto é uma bijeção entre os conjuntos $Hom_G(\frac{G}{H}, T)$ e T^H. □

2.3 Fatos Decorrentes

Nesta seção veremos alguns fatos que decorrem do Lema de Dedekind e dos resultados apresentados anteriormente a respeito da Teoria de G-conjuntos. Tais consequências terão um papel essencial na compreensão do Teorema da Correspondência que estudaremos no próximo capítulo.

Assuma novamente que L/K é uma extensão de Galois e que $G = Aut_K L$. Além disso, considere S um G-conjunto finito e a L-álgebra $Map(S, L)$.

Proposição 2.3.1. *$Map(S, L)$ tem L-dimensão $\#S$.*

Demonstração. Seja $n = \#S$ e considere a aplicação:

$$\begin{aligned} \varphi : Map(S, L) &\to \overbrace{L \times ... \times L}^{n \ vezes} \\ f &\mapsto (f(s_i))_{1 \leq i \leq n} \end{aligned}$$

- φ é um homomorfismo de L-álgebras. De fato, dados $f, g \in Map(S, L)$ e $\lambda \in L$, temos:

(i) $\varphi(f+g) = \varphi(f) + \varphi(g)$.

$$\begin{aligned}\varphi(f+g) &= ((f+g)(s_i))_{1\leq i\leq n} \\ &= (f(s_i) + g(s_i))_{1\leq i\leq n} \\ &= (f(s_i))_{1\leq i\leq n} + (g(s_i))_{1\leq i\leq n} \\ &= \varphi(f) + \varphi(g).\end{aligned}$$

(ii) $\varphi(\lambda f) = \lambda\varphi(f)$.

$$\begin{aligned}\varphi(\lambda f) &= (\lambda f(s_i))_{1\leq i\leq n} \\ &= \lambda(f(s_i))_{1\leq i\leq n} \\ &= \lambda\varphi(f).\end{aligned}$$

(iii) $\varphi(fg) = \varphi(f)\varphi(g)$.

$$\begin{aligned}\varphi(fg) &= ((fg)(s_i))_{1\leq i\leq n} \\ &= (f(s_i)g(s_i))_{1\leq i\leq n} \\ &= (f(s_i))_{1\leq i\leq n}(g(s_i))_{1\leq i\leq n} \\ &= \varphi(f)\varphi(g).\end{aligned}$$

(iv) $\varphi(1) = 1_{L\times ...\times L}$, com 1 representando a função constante igual a 1 em $Map(S, L)$.
$\varphi(1) = (1(s_i))_{1\leq i\leq n} = (1_L, ..., 1_L)$.

- φ é injetiva.
  De fato, dado $f \in Map(S, L)$ tal que $\varphi(f) = 0$, temos:

$$(f(s)) = 0, \forall s \in S \Rightarrow f \equiv 0.$$

- φ é sobrejetiva.

Considere $\ell = (\ell_1, ..., \ell_n) \in \overbrace{L \times ... \times L}^{n\ vezes}$. Para mostrar que existe $f \in Map(S, L)$ tal que $\varphi(f) = \ell$, basta tomar:

$$\begin{aligned}f : S &\to L \\ s_i &\mapsto \ell_i, \forall i \in \{1, ..., n\}\end{aligned}$$

$$\begin{aligned}\Rightarrow \varphi(f) &= (f(s_i))_{1\leq i\leq n} \\ &= (f(s_1), ..., f(s_n)) \\ &= (\ell_1, ..., \ell_n) \\ &= \ell.\end{aligned}$$

Como $\#S = n = dim_L \overbrace{L \times ... \times L}^{n\ vezes}$ então $dim_L Map(S, L) = n$.

□

Proposição 2.3.2. *A K-álgebra $Hom_G(S, L)$ tem K-dimensão $\#S$.*

Demonstração. Seguiremos a mesma ideia da Proposição 2.1.3. Além disso, as argumentações para se mostrar que toda K-base de $Map(S, L)^G$ também é uma L-base de $Map(S, L)$ são exatamente as mesmas. Assim, basta mostrar que a ação de G em $Map(S, L)$ é K-linear tal que:

$$\sigma(x \cdot f) = \sigma(x) \cdot \sigma(f), \forall \sigma \in G, x \in L \text{ } e \text{ } f \in Map(S, L).$$

Vamos começar provando que a ação de G em $Map(S, L)$ é K-linear. Sejam $r_1, r_2 \in K; h_1, h_2 \in Map(S, L); \sigma \in G, s \in S$, então:

$$\begin{aligned}
\sigma(r_1 \cdot h_1 + r_2 \cdot h_2)(s) &= (\sigma(r_1 h_1 + r_2 h_2))(s) \\
&\overset{(1)}{=} \sigma((r_1 h_1 + r_2 h_2)\sigma^{-1} \cdot s) \\
&= \sigma(r_1 h_1(\sigma^{-1} \cdot s) + r_2 h_2(\sigma^{-1} \cdot s)) \\
&= \sigma(r_1)\sigma(h_1(\sigma^{-1} \cdot s)) + \sigma(r_2)\sigma(h_2(\sigma^{-1} \cdot s)) \\
&\overset{(2)}{=} r_1(\sigma h_1)(s) + r_2(\sigma h_2)(s) \\
&= (r_1 \cdot \sigma h_1 + r_2 \cdot \sigma h_2)(s)
\end{aligned}$$

- A igualdade (1) sai do fato de que $Map(S, L)$ é um G-conjunto segundo a G-ação que satisfaz:
$$\sigma h = \sigma h \sigma^{-1}.$$

- A igualdade (2) sai do fato de:
$$r_1, r_2 \in K = L^G.$$

  Agora precisamos mostrar que $Map(S, L)$ satisfaz:

$$\sigma(x \cdot h) = \sigma(x) \cdot \sigma(h), \forall \sigma \in G, x \in L \text{ } e \text{ } h \in Map(S, L).$$

  Para tanto, note que:

$$\begin{aligned}
\sigma(xh)(s) &= \sigma(xh(\sigma^{-1} \cdot s)) \\
&= \sigma(x)\sigma(h(\sigma^{-1} \cdot s)) \\
&= (\sigma(x)\sigma h)(s), \forall s \in S.
\end{aligned}$$

  Usando o Exemplo 2.2.3, temos que:

$$\begin{aligned}
\#S &= dim_L Map(S, L) \\
&= dim_K Map(S, L)^G \\
&= dim_K Hom_G(S, L).
\end{aligned}$$

□

Corolário 2.3.3. *Se* $S = \dfrac{G}{\{1_G\}}$, *então* $dim_K L = |G|$.

Demonstração. É consequência direta da Proposição 2.2.6.

□

Corolário 2.3.4. *Se* $S = \dfrac{G}{H}$, *com* H *um subgrupo de* G, *então* $dim_K L^H = [G : H]$.

Demonstração. Basta considerar a bijeção vista na Proposição 2.2.6:

$$\begin{aligned} \theta : Hom_G(\frac{G}{H}, L) &\to L^H \\ f &\mapsto f(H) \end{aligned}$$

então:

$$\begin{aligned} dim_K L^H &= dim_K Hom_G(\frac{G}{H}, L) \\ &= \#(\frac{G}{H}) \\ &= [G : H]. \end{aligned}$$

□

Sejam L/K uma extensão de Galois, F um corpo intermediário desta extensão e $G = Aut_K L$. Na Proposição a seguir trabalharemos com o conjunto $G_F := \{\sigma \in G \mid \sigma(x) = x, \forall x \in F\}$ que é um subgrupo de G. De fato:

- $1_G \in G_F$.
  $1_G = id_L \Rightarrow 1_G(x) = id_L(x) = x, \forall x \in L$, em particular, $\forall x \in F \subseteq L$.
- Sejam $\sigma_1, \sigma_2 \in G_F \Rightarrow \sigma_1 \circ \sigma_2^{-1} \in G_F$.

  $$\forall x \in F, \sigma_1(x) = x \text{ e } \sigma_2(x) = x.$$

  E note que:

  $$\begin{aligned} x = \sigma_2^{-1}(\sigma_2(x)) = \sigma_2^{-1}(x) \\ \Rightarrow (\sigma_1 \circ \sigma_2^{-1})(x) = \sigma_1(\sigma_2^{-1}(x)) = \sigma_1(x) = x. \end{aligned}$$

Portanto G_F é um subgrupo de G.

Proposição 2.3.5. *Sejam L/K uma extensão de Galois e $G = Aut_K L$. Considere F um corpo intermediário desta extensão e G_F. Então restringindo a F os elementos de G, existe uma imersão do G-conjunto $\frac{G}{G_F}$ no G-conjunto $Alg_K(F, L)$, isto é, podemos ver $\frac{G}{G_F}$ como um conjunto isomorfo a um subconjunto de $Alg_K(F, L)$.*

Demonstração. Procederemos por etapas.

(i) Como G_F é um subgrupo de G, então $\frac{G}{G_F}$ é um G-conjunto, pelo Exemplo 2.2.5.

(ii) $Alg_K(F, L)$ é um G-conjunto.
Considere a seguinte aplicação:

$$\begin{aligned} G \times Alg_K(F, L) &\to Alg_K(F, L) \\ (\sigma, f) &\mapsto \sigma \cdot f = \sigma \circ f \end{aligned}$$

Vamos mostrar que, de fato, esta aplicação define uma ação de G em $Alg_K(F, L)$.

- $\forall \sigma_1, \sigma_2 \in G, \forall f \in Alg_K(F, L)$ tem-se: $\sigma_2 \cdot (\sigma_1 \cdot f) = \sigma_2\sigma_1 \cdot f$, pois

$$\sigma_2 \cdot (\sigma_1 \cdot f) = \sigma_2 \circ \sigma_1 \circ f = \sigma_2\sigma_1 \circ f = \sigma_2\sigma_1 \cdot f.$$

- $\forall f \in Alg_K(F, L)$ tem-se: $1_G \cdot f = f$, pois

$$1_G \cdot f = 1_G \circ f = f.$$

(iii) $\{\sigma|_F \mid \sigma \in G\}$ é um G-conjunto via a ação $*$ dada por, $\forall \sigma, \tau \in G$, $\tau * \sigma|_F = \tau\sigma|_F$.

- $1_G * \sigma|_F = 1_G\sigma|_F = \sigma|_F$, $\forall \sigma \in G$.
- $\sigma_1 * (\sigma_2 * \sigma|_F) = \sigma_1 * (\sigma_2\sigma|_F) = \sigma_1\sigma_2\sigma|_F = \sigma_1\sigma_2 * \sigma|_F$, $\forall \sigma_1, \sigma_2 \in G$.

(iv) $\frac{G}{G_F} \simeq \{\sigma|_F \mid \sigma \in G\}$ como G-conjuntos.
Considere a seguinte aplicação:

$$\begin{aligned} \phi : \frac{G}{G_F} &\to \{\sigma|_F \mid \sigma \in G\} \\ \sigma G_F &\mapsto \sigma|_F : F \to L \end{aligned}$$

Note que a aplicação ϕ está bem definida e é injetiva, pois, dados $\sigma_1, \sigma_2 \in G$, temos:

$$\sigma_1 G_F = \sigma_2 G_F \Leftrightarrow (\sigma_2)^{-1}\sigma_1 G_F = G_F \Leftrightarrow (\sigma_2)^{-1}\sigma_1(x) = x,\ \forall x \in F$$

$$\Leftrightarrow \sigma_1(x) = \sigma_2(x),\ \forall x \in F \Leftrightarrow \sigma_1|_F = \sigma_2|_F \Leftrightarrow \phi(\sigma_1 G_F) = \phi(\sigma_1 G_F).$$

A sobrejetividade de ϕ decorre do Teorema 1.1.9.

Resta mostrar que ϕ é um homomorfismo entre G-conjuntos. De fato, se $\bullet$ e $*$ denotam as G-ações sobre por $\dfrac{G}{G_F}$ e $\{\sigma|_F \mid \sigma \in G\}$, respectivamente, então, dados $\sigma, \tau \in G$:

$$\phi(\tau \bullet \sigma G_F) = \phi(\tau\sigma G_F) = \tau\sigma|_F = \tau * \sigma|_F = \tau * \phi(\sigma G_F).$$

□

Corolário 2.3.6. *Sejam L/K uma extensão de Galois, F um corpo intermediário entre K e L e $G = Aut_K L$. Então:*

$$dim_K F = \#Alg_K(F, L) = \#(\frac{G}{G_F}) = [G : G_F] = dim_K L^{G_F}.$$

Demonstração. Decorre da seguinte sequência de desigualdades. No que se segue, justificaremos cada uma delas.

$$dim_K F \overset{(1)}{\geq} \#Alg_K(F, L) \overset{(2)}{\geq} \#(\frac{G}{G_F}) = [G : G_F] \overset{(3)}{=} dim_K L^{G_F} \overset{(4)}{\geq} dim_K F.$$

(1) Pelo Lema de Dedekind:

$$\#Alg_K(F, L) \leq dim_L Hom_K(F, L)$$

e pela Proposição 2.1.2 temos que $dim_L Hom_K(F, L) = dim_K F$.

(2) Decorre da Proposição 2.3.5.

(3) Decorre da Proposição 2.3.5 e do Corolário 2.3.4.

(4) É decorrente do fato de que $F \subseteq L^{G_F}$, pois:

$$L^{G_F} := \{\ell \in L \mid \sigma(\ell) = \ell, \forall \sigma \in G_F\}.$$

Em particular, $F = L^{G_F}$, pois, pelo Corolário 2.3.4, sabemos que $dim_K L^{G_F} = dim_K F$.

□

Observe que concluímos que:

$$\frac{G}{G_F} \simeq \{\sigma|_F \mid \sigma \in G\} = Alg_K(F, L).$$

Note que este fato implica que todo homomorfismo de K-álgebras de F em L estende-se a um K-automorfismo de L.

Corolário 2.3.7. *Sejam L/K uma extensão de Galois, $G = Aut_K L$, H um subgrupo de G e $F = L^H$. Então $H = G_F$.*

Demonstração. Note que, pelos Corolários 2.3.4 e 2.3.6, temos $[G : G_F] = [G : H]$ e que claramente $H \subset G_F$, por definição. Além disso, a igualdade dos respectivos índices em G implica $|H| = |G_F|$. Portanto $H = G_F$. □

Capítulo 3

Correspondência de Galois-Grothendieck

A ideia deste capítulo é apresentar ao leitor a teoria de Galois-Grothendieck que estabelece uma correspondência entre a categoria de G-conjuntos finitos e a categoria das K-álgebras L-decomponíveis de dimensão finita, onde L/K é uma extensão de Galois e $G = Aut_K L$. Para tal, começaremos apresentando algumas observações e definições essenciais.

Definição 3.0.8. Uma categoria $\mathfrak{C}$ consiste de uma coleção $Ob\mathfrak{C}$ de objetos e de uma coleção $Mor_{\mathfrak{C}}$ de morfismos entre objetos que verificam as seguintes propriedades:

(i) Para cada par de objetos $X, Y \in Ob\mathfrak{C}$ existe um conjunto $Mor_{\mathfrak{C}}(X, Y)$ de morfismos de X para Y tal que $Mor_{\mathfrak{C}}(X, Y) \cap Mor_{\mathfrak{C}}(X', Y') = \varnothing$ se $(X, Y) \neq (X', Y')$.

(ii) Para cada tripla de objetos $X, Y, Z \in Ob\mathfrak{C}$ existe uma aplicação composição:

$$\begin{aligned} \circ : Mor_{\mathfrak{C}}(Y, Z) \times Mor_{\mathfrak{C}}(X, Y) &\to Mor_{\mathfrak{C}}(X, Z) \\ (g, f) &\mapsto g \circ f \end{aligned}$$

(iii) Para cada objeto $X \in Ob\mathfrak{C}$ existe um morfismo identidade $I_X \in Mor_{\mathfrak{C}}(X, X)$ que satisfaz:

$$I_X \circ f = f \quad e \quad g \circ I_X = g$$

para quaisquer morfismos $f \in Mor_{\mathfrak{C}}(Y, X)$ e $g \in Mor_{\mathfrak{C}}(X, Z)$, com $Y, Z \in Ob\mathfrak{C}$.

Exemplo 3.0.9. (1) A categoria $\mathfrak{Set}$, cujos objetos são conjuntos e os morfismos são funções.

(2) A categoria $\mathfrak{Grp}$, cujos objetos são grupos e os morfismos são homomorfismos de grupos.

(3) A categoria $\mathfrak{GSet}$, cujos objetos são G-conjuntos finitos e os morfismos são G-aplicações.

Definição 3.0.10. (i) Sejam $\mathfrak{C}$ e $\mathfrak{D}$ duas categorias. Um funtor covariante $F : \mathfrak{C} \to \mathfrak{D}$ consiste das correspondências:

• $Ob(\mathfrak{C}) \to Ob(\mathfrak{D})$, $X \mapsto F(X)$

• $Mor(\mathfrak{C}) \to Mor(\mathfrak{D})$, $f : X \to Y \mapsto F(f) : F(X) \to F(Y)$,
tal que:

- $F(I_X) = I_{F(X)}, \forall X \in Ob(\mathfrak{C})$.
- $F(g \circ f) = F(g) \circ F(f), \forall g \in Mor_{\mathfrak{C}}(Y, Z)$ e $f \in Mor_{\mathfrak{C}}(X, Y)$.

(ii) Sejam $\mathfrak{C}$ e $\mathfrak{D}$ duas categorias. Um funtor contravariante $F : \mathfrak{C} \to \mathfrak{D}$ consiste das correspondências:

• $Ob(\mathfrak{C}) \to Ob(\mathfrak{D})$, $X \mapsto F(X)$

• $Mor(\mathfrak{C}) \to Mor(\mathfrak{D})$, $f : X \to Y \mapsto F(f) : F(Y) \to F(X)$,
tal que:

- $F(I_X) = I_{F(X)}, \forall X \in Ob(\mathfrak{C})$.
- $F(g \circ f) = F(f) \circ F(g), \forall g \in Mor_{\mathfrak{C}}(Y, Z)$ e $f \in Mor_{\mathfrak{C}}(X, Y)$.

Definição 3.0.11. (i) Um funtor covariante $F : \mathfrak{C} \to \mathfrak{D}$ é dito uma equivalência de categorias se existe um funtor covariante $G : \mathfrak{D} \to \mathfrak{C}$ tal que:

$$F \circ G = 1_{\mathfrak{D}}$$
$$G \circ F = 1_{\mathfrak{C}}$$

(ii) Um funtor contravariante $F : \mathfrak{C} \to \mathfrak{D}$ é dito uma (anti-)equivalência de categorias se existe um funtor contravariante $G : \mathfrak{D} \to \mathfrak{C}$ tal que:

$$F \circ G = 1_{\mathfrak{C}}$$
$$G \circ F = 1_{\mathfrak{D}}$$

Definição 3.0.12. Seja L um corpo. Uma K-álgebra A L-decomponível é uma K-álgebra que satisfaz:
$\forall a, b \in A, a \neq b$, existe um homomorfismo de K-álgebras $\varphi : A \to L$ tal que $\varphi(a) \neq \varphi(b)$.

Exemplo 3.0.13. Seja L/K uma extensão de corpos. Então K é trivialmente uma K-álgebra L-decomponível. Para tanto basta considerar $\pi : K \to L$ a K-imersão de K em L.

Exemplo 3.0.14. Sejam L/K uma extensão de Galois, $G = Aut_K L$, e S um G-conjunto finito. Vimos na Proposição 2.3.2 que $Hom_G(S, L)$ é uma álgebra de K-dimensão $\#S$. Note que, de fato, $Hom_G(S, L)$ é uma álgebra L-decomponível. Para tal basta considerar, para cada $s \in S$, a aplicação:

$$\begin{aligned} \nu_s : Hom_G(S, L) &\to L \\ f &\mapsto f(s) \end{aligned}$$

e observar que $\forall f, g \in Hom_G(S, L)$, com $f(s) \neq g(s)$ para algum $s \in S$, obtemos:

$$\nu_s(f) = f(s) \neq g(s) = \nu_s(g).$$

Observação 3.0.15. Denotemos por $\mathfrak{Alg}$ a categoria cujos objetos são as álgebras L-decomponíveis e os morfismos são os homomorfismos de K-álgebras.

3.1 O Teorema da Correspondência de Galois-Grothendieck

No que se segue trataremos de construir as ferramentas necessárias para obtermos a (anti-)equivalência entre as categorias $\mathfrak{GSet}$ e $\mathfrak{Alg}$. Procederemos por etapas.

Etapa 1. Sejam L/K uma extensão de Galois e $G = Aut_K L$. Considere, para toda K-álgebra L-decomponível A de dimensão finita, a aplicação:

$$\begin{aligned} \mu : A &\to A* := Hom_G(Alg_K(A, L), L) \\ a &\mapsto \mu_a : Alg_K(A, L) \to L \\ &\qquad\qquad \varphi \mapsto \varphi(a) \end{aligned}$$

Proposição 3.1.1. *A aplicação μ é um isomorfismo de K-álgebras.*

Demonstração. • μ está bem definida.

De fato, $\mu_a \in Hom_G(Alg_K(A,L),L)$, pois $\forall a \in A$, $\forall \varphi \in Alg_K(A,L)$ e $\forall \sigma \in G$ temos:

$$\sigma \cdot \mu_a(\varphi) = \sigma(\mu_a(\sigma^{-1} \circ \varphi)) = \sigma(\sigma^{-1}(\varphi(a))) = \varphi(a) = \mu_a(\varphi).$$

• μ é um homomorfismo de K-álgebras.

Para quaisquer $a, b \in A$, $k \in K$ e $\varphi \in Alg_K(A,L)$ temos que:

$$\begin{aligned} \mu_{ka+b}(\varphi) &= \varphi(ka+b) \\ &= k\varphi(a) + \varphi(b) \\ &= (k\mu_a + \mu_b)(\varphi) \end{aligned}$$

e que

$$\begin{aligned} \mu_{ab}(\varphi) &= \varphi(ab) \\ &\overset{(\circledast)}{=} \varphi(a)\varphi(b) \\ &= (\mu_a\mu_b)(\varphi). \end{aligned}$$

Observe que $\circledast$ segue do fato de $\varphi \in Alg_K(A,L)$, que é uma K-álgebra.

• μ é bijeção.

μ é injetor.

De fato, dados $a, b \in A$ com $a \neq b$, existe $\phi \in Alg_K(A,L)$ tal que $\phi(a) \neq \phi(b)$ (pois A é L-decomponível) e portanto:

$$\mu(a)(\phi) = \mu_a(\phi) = \phi(a) \neq \phi(b) = \mu_b(\phi) = \mu(b)(\phi).$$

Ou seja $\mu(a) \neq \mu(b)$.

μ é sobrejetor.

De fato, decorre das Proposições 2.3.2 e 2.1.2 que:

$$dim_K A* = \#Alg_K(A,L) \leq dim_K A.$$

Como $\mu(A)$ é um K-subespaço vetorial de $A*$, necessariamente devemos ter:

$$dim_K A* \geq dim_K \mu(A) = dim_K A.$$

Logo μ é sobrejetor, e portanto é um isomorfismo de K-álgebras. □

Etapa 2. Sejam L/K uma extensão de Galois e $G = Aut_K L$. Para cada G-conjunto S considere a aplicação:

$$\begin{aligned} \nu : S &\to S* := Alg_K(Hom_G(S, L), L) \\ s &\mapsto \nu_s \end{aligned}$$

com ν_s dado no Exemplo 3.0.14.

Proposição 3.1.2. *ν é um isomorfismo de G-conjuntos.*

Demonstração. • ν está bem definida.

De fato, $\nu_s : Hom_G(S, L) \to L$ é um homomorfismo de K-álgebras, pois, dados $f, g \in Hom_G(S, L)$ e $k \in K$, temos:

$$\nu_s(f + kg) = (f + kg)(s) = f(s) + kg(s)$$

e

$$\nu_s(f \cdot g) = (f \cdot g)(s) = f(s) \cdot g(s).$$

• ν é uma G-aplicação.

De fato, $\forall \sigma \in G, s \in S$ e $\forall f \in Hom_G(S, L)$, temos:

$$\begin{aligned} \nu(\sigma \cdot s)(f) &= \nu_{\sigma \cdot s}(f) \\ &= f(\sigma \cdot s) \\ &= \sigma(f(s)) \\ &= \sigma(\nu_s(f)) \\ &= \sigma \circ \nu_s(f) \\ &= \sigma \circ \nu(s)(f). \end{aligned}$$

• ν é bijetor.

Sabemos, pelas Proposições 2.3.2 e 3.1.1 que:

$$\begin{aligned} \#S* &= \#Alg_K(Hom_G(S, L), L) \\ &= dim_K Hom_G(S, L) \\ &= \#S. \end{aligned}$$

Então, basta mostrar que a aplicação é injetora. Conforme visto na Proposição 2.3.2, $Hom_G(S, L)$ gera $Map(S, L)$ como um L-espaço vetorial. Dados $s, s' \in S$ tais que $s \neq s'$ se $g(s) \neq g(s')$, para todo $g \in Hom_G(S, L)$, então $f(s) \neq f(s')$, para todo $f \in Map(S, L)$. Mas sempre é possível construir $f \in Map(S, L)$ tal que $f(s) \neq f(s')$, por exemplo, $f : S \to L$ dada por:

$$f(x) = \begin{cases} 1, \ se \ x = s \\ 0, se \ x \neq s \end{cases}$$

Portanto, se $s \neq s'$ existe $a \in Hom_G(S, L)$ com $a(s) \neq a(s')$, ou seja:

$$\nu_s(a) = a(s) \neq a(s') = \nu_{s'}(a).$$

Consequentemente $\nu(s) \neq \nu(s')$. □

Etapa 3. Agora estamos em condições de enunciar e demonstrar o principal resultado deste capítulo.

Teorema 3.1.3 (Teorema da Correspondência de Galois-Grothendieck)**.** *Sejam L/K uma extensão de Galois e $G = Aut_K L$. Então a aplicação:*

$$\begin{aligned} \Theta : \mathfrak{GSet} &\to \mathfrak{Alg} \\ S &\mapsto Hom_G(S, L) \end{aligned}$$

é um funtor contravariante que induz uma (anti-)equivalência canônica de categorias, cuja inversa é dada por:

$$\begin{aligned} \Theta' : \mathfrak{Alg} &\to \mathfrak{GSet} \\ A &\mapsto Alg_K(A, L). \end{aligned}$$

Demonstração. • Θ é um funtor contravariante.

De fato, $\forall \varphi \in Mor_{\mathfrak{GSet}}(S, T)$:

$$\begin{aligned} \Theta(\varphi) : \Theta(T) &\to \Theta(S) \\ f &\mapsto f \circ \varphi \end{aligned}$$

Assim,

– $\forall S \in Ob_{\mathfrak{GSet}}$ e $\forall f \in \Theta(S)$ temos $\Theta(I_S) = I_{\Theta(S)}$.
De fato, para qualquer $f \in \Theta(S)$ temos:

$$\Theta(I_S)(f) = f \circ (I_S) = f.$$

– $\forall \gamma \in Mor_{\mathfrak{GSet}}(T, X),\ \forall \delta \in Mor_{\mathfrak{GSet}}(S, T)$ e $\forall f \in \Theta(X)$ temos:

$$\begin{aligned} \Theta(\gamma \circ \delta)(f) &= f \circ \gamma \circ \delta \\ &= \Theta(\delta)(f \circ \gamma) \\ &= \Theta(\delta)(\Theta(\gamma)(f)) \\ &= (\Theta(\delta) \circ \Theta(\gamma))(f). \end{aligned}$$

• De forma análoga, Θ' é um funtor contravariante.

• Θ é uma (anti-)equivalência de categorias.
Já provamos nas Proposições 3.1.2 e 3.1.1 que

$$S \simeq Alg_K(Hom_G(S, L), L)$$

como G-conjuntos e que

$$A \simeq Hom_G(Alg_K(A, L), L)$$

como K-álgebras. Consequentemente, temos:

$$S \simeq Alg_K(Hom_G(S, L), L) = \Theta'(\Theta(S))$$

e

$$A \simeq Hom_G(Alg_K(A, L), L) = \Theta(\Theta'(A)).$$

□

3.2 Uma releitura do Teorema Fundamental da Teoria de Galois

Finalmente podemos apresentar o Teorema Fundamental da Teoria de Galois como um caso particular do Teorema da Correspondência de Galois-Grothendieck.

Para tanto, sejam L/K uma extensão de Galois e $G = Aut_K L$. Conforme vimos no Exemplo 2.2.5, para cada subgrupo H de G o quociente $\frac{G}{H}$ é um G-conjunto finito via a ação induzida pela multiplicação de G. Da mesma forma, vimos no Exemplo 3.0.13 que cada corpo F intermediário da extensão L/K é uma K-álgebra L-decomponível.

Denotemos por *Subg(G)* o conjunto dos subgrupos de G, por *Quoc(G)* o conjunto dos quocientes $\frac{G}{H}$ e por *Subc(L)* o conjunto dos corpos intermediários de L/K. A correspondência de Galois entre subgrupos de G e subcorpos intermediários de L, conforme enunciado abaixo, é uma consequência imediata da Proposição 2.3.5 e da composição das seguintes bijeções:

- a bijeção óbvia entre *Subg(G)* e *Quoc(G)*,
- a restrição a *Quoc(G)* e a *Subc(L)* dos funtores Θ e Θ', respectivamente, conforme descritos no Teorema 3.1.3,
- o isomorfismo θ conforme descrito na Proposição 2.2.6.

A vizualização em diagramas fica da seguinte forma:

$$H \to \frac{G}{H} \overset{\Theta}{\to} Hom_G(\frac{G}{H}, L) \overset{\theta}{\simeq} L^H.$$

$$G_F \leftarrow \frac{G}{G_F} \overset{2,3.5}{\leftarrow} Alg_K(F, L) \overset{\Theta'}{\leftarrow} F.$$

Teorema 3.2.1 (Teorema Fundamental da Teoria de Galois)**.** *Sejam L/K uma extensão de Galois e $G = Aut_K L$. Então a aplicação:*

$$\begin{aligned} Subg(G) &\to Subc(L) \\ H &\mapsto L^H \end{aligned}$$

é uma correspondência bijetora, que inverte a inclusão, cuja inversa é dada por:

$$\begin{aligned} Subc(L) &\quad Subg(G) \\ F &\mapsto G_F. \end{aligned}$$

Referências Bibliográficas

[1] ARTIN, E.; *Galois Theory*. Notre Dame Mathematical Lectures, Notre Dame University (1948).

[2] BRZEZINSKI, T. and WISBAWER R.; *Corings and Comodules*. London Mathematical Society Lecture Note Series 309, United Kingdom (2003).

[3] DEMEYER, F.; *Another Proof of the Fundamental Theorem of Galois Theory*, in: The American Mathematical Monthly, 75, 7, 720-740, Aug - Sep. (1968).

[4] DRESS, A. W. M.; *One more shortcut to Galois Theory*, in: Advances in Mathematics, 110, 129-140, (1995).

[5] GROTHENDIECK, A.; *Revêtements étales et groupe fondamental*. Lecture Notes in Mathematics 224, Springer-Verlag, French, (1971).

[6] MCCARTHY, P.J.; *Algebraic Extension of Fields*. Blaisdell Publishing Company, London (1966).

[7] MORANDI, P.; *Field and Galois Theory*. Graduate Texts in Mathematics, Springer-Verlag, New Mexico, USA (1996).

[8] PAQUES, A.; *Teorias de Galois*, in: Minicurso: Escola de Álgebra (2012).

[9] ROTMAN, J.; *Galois Theory*. Springer-Verlag, Illinois, USA (1990).

[10] STEWART, I.; *Galois Theory*. Champman and Hall/CRC Mathematics, Coventry, United Kingdom (2003).