Universidade Federal do Rio Grande do Sul

Instituto de Matemática e Estatística

Programa de Pós-Graduação em Matemática

Extensões Galoisianas Comutativas

Dissertação de Mestrado

Gustav Beier

Porto Alegre, Maio de 2021.

Dissertação submetida por Gustav Eckard Gorniski Beier[1] como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática e Estatística da Universidade Federal do Rio Grande do Sul.

Professora Orientadora:

Thaísa Raupp Tamusiunas (PPGMat-UFRGS)

Banca Examinadora:

Antonio Paques (PPGMat-UFRGS)

Bárbara Seelig Pogorelsky (PPGMat-UFRGS)

Dirceu Bagio (UFSM)

Data da Apresentação: 25 de Maio de 2021.

[1]Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

Agradecimentos

Este trabalho é, no momento, a conclusão de uma grande jornada enquanto Estudante. Estudante enquanto aluno, monitor, pesquisador e até mesmo professor. Por isso, é também motivo de muita gratidão.

Agradeço a minha família, em especial a minha mãe, Laura Felix Gorniski, que sempre me apoia, e também a meu pai, Horst Hans Beier. Sempre que vejo um objeto do dia a dia e me pergunto qual seu volume, me lembro do meu pai e todo o estímulo que recebi na infância para aprender sempre mais. Sei que estaria bastante orgulhoso, embora nunca houvesse esperado diferente. Agradeço a meus irmãos, meu padrinho, minha madrinha, e todos aqueles que acompanharam meu crescimento e minhas conquistas.

Este é um trabalho bastante especial, e não poderia ter contado com pessoas mais especiais neste período que me dediquei à Álgebra: agradeço de coração à minha orientadora, Thaísa, que esteve sempre disposta a resolver as dúvidas - aquelas que eu tinha, e principalmente as que eu mesmo criava. Ao meu amigo e colega de pesquisa Wesley, que não auxiliou apenas nos pré-requisitos, mas também na revisão e ao longo de todo o trabalho. Sendo meu primeiro contato com a pesquisa em Matemática, vejo o quanto ambos se dedicam e gostam de seu trabalho, e desejo tudo de melhor nas suas carreiras.

Ao longo da Licenciatura e do Mestrado, a Matemática me trouxe muitos amigos, e por isso sou muito grato a uma lista enorme de pessoas: Cristian, Tomás, Eduarda, Alessandra, Vinícius, Izabella, além de diversos outros colegas e professores. Dentre estes, destaco o professor Antonio Paques. Apesar de não haver sido seu aluno, vejo o reflexo de seu trabalho e seu estudo sobre

Extensões Galoisianas Comutativas, que iluminou este trabalho.

Agradeço ao CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico, pelo apoio financeiro - sei que a oportunidade que tive não é acessível a todos, e parte do meu trabalho é lutar para que isso se torne realidade.

Agradeço ao Instituto de Matemática e Estatística, que se tornou um novo lar. Que o Instituto, que completa 62 anos em 2021, possa formar professores, matemáticos e estatísticos por mais 62 anos.

Resumo

Neste trabalho estendemos a teoria de Galois desenvolvida sobre corpos para extensões de anéis comutativos. Os principais resultados são relacionados à separabilidade de extensões de anéis comutativos, bem como a definição das estruturas e objetos necessários. Seguindo [7], definimos extensões galoisianas, exploramos a correspondência de Galois e os homomorfismos de extensões galoisianas. Por fim, apresentamos um resultado da cohomologia galoisiana, principal resultado de [7], a partir do isomorfismo entre $H^n(S/R, F)$, o n-ésimo grupo de cohomologia de Amitsur de T/R com valores em F, e $H^n(G, F(S))$, o n-ésimo grupo de cohomologia de G sobre $F(S)$.

Palavras-chave: extensões comutativas, cohomologia galoisiana, teoria de Galois.

Abstract

In this essay we will extend the Galois theory over fields to commutative ring extensions. The main results relate to the separability of commutative ring extensions, along with the definition of the required structures and objects. In addition to that, we will define the Galois extensions, explore the Galois correspondence and homomorphisms of Galois extensions. Concluding it, we present a result of the Galois cohomology, which is the main result of [7], consequence of the isomorphism between $H^n(S/R, F)$, the n-th Amitsur cohomology group of T/R with values in F, and $H^n(G, F(S))$, the n-th cohomology group of G over $F(S)$.

Keywords: commutative extensions, Galois cohomology, Galois theory.

Sumário

Introdução

Para compreender a importância do nome Galois na Matemática, iremos buscar um pouco da história por trás dele. Évariste Galois, com o objetivo de resolver equações polinomiais de quinto grau, desenvolveu o início do estudo hoje conhecido como teoria de Galois, origem histórica da teoria de grupos. Galois, voltado às equações polinomiais, permitiu determinarmos quando polinômios são solúveis por radicais - isto é, quando podemos determinar suas raízes a partir de seus coeficientes, de forma semelhante a como resolvemos polinômios de segundo grau. As extensões de corpos estudadas por Galois eram subcorpos dos números complexos, e a teoria posteriormente foi generalizada para corpos abstratos.

A teoria de Galois é fundamentada sobre uma correspondência entre extensões de corpos e grupos de automorfismos (destes corpos). As características destes grupos podem ser fonte de informações sobre estas extensões de corpos. Podemos dar mais um passo: desenvolver a teoria de Galois sobre anéis comutativos. Auslander e Goldman foram os primeiros a introduzir a noção de extensão de Galois para anéis comutativos, no artigo *The Brauer group of a Commutative Ring* em 1960. Este artigo desenvolve o princípio da teoria geral de álgebras separáveis sobre anéis comutativos.

Em 1965, Chase, Harrison, e Rosenberg desenvolvem uma nova caracterização de extensões galoisianas de anéis comutativos. Estes resultados serão apresentados nesta dissertação, e são mais próximos ao desenvolvimento original (para corpos). No artigo *Galois theory and Galois cohomology of Commutative Rings*, Chase, Harrison, e Rosenberg desenvolvem também a

cohomologia de Amitsur sobre extensões galoisianas, generalizando resultados obtidos por Auslander e Goldman, assim como do Teorema 90 de Hilbert.

Nesta dissertação, iremos explorar os resultados obtidos por Chase, Harrison, e Rosenberg em [7], além da construção do grupo de Brauer apresentada em [4] por Auslander e Goldman. No capítulo 1, serão desenvolvidos os pré-requisitos para que possamos compreender a teoria de Galois sobre anéis comutativos, a partir da construção inicial desta teoria. No capítulo 2, iremos estudar a teoria de Galois sobre extensões de anéis comutativos. No capítulo 3, iremos abordar o grupo de Brauer e a cohomologia galoisiana.

Capítulo 1

Preliminares

A proposta desta dissertação é desenvolver uma teoria de Galois sobre anéis comutativos como uma generalização natural da teoria sobre corpos. Assim, iremos utilizar os resultados da teoria de Galois e resultados da álgebra comutativa.

Na primeira seção, como introdução e motivação para o estudo que segue, estão enunciados definições e resultados da teoria de Galois sobre corpos abstratos. O principal conceito observado ao longo desta seção é o de separabilidade [20]. A separabilidade será estendida para anéis comutativos no próximo capítulo.

Na segunda seção, temos definições da álgebra comutativa e o estudo de módulos, em particular de módulos projetivos.

1.1 Teoria de Galois Clássica

Para iniciar o estudo da teoria de Galois, necessitamos do principal objeto do estudo – as extensões galoisianas. Para isso, precisamos averiguar sob quais condições a correspondência de Galois é bijetiva. Ao longo desta seção, trabalharemos com resultados da teoria clássica, que adiante serão generalizados para o contexto de extensões comutativas.

Definição 1.1.1. (i) Sejam K e L dois corpos quaisquer. Se existir um monomorfismo $i : K \to L$, dizemos que L é uma extensão de K. Por simplicidade, identificaremos K com sua imagem $i(K) \subset L$. Denotaremos esta extensão por $L \mid_K$.

(ii) Definimos o grau da extensão $L \mid_K$ como sendo a dimensão de L visto como um K-espaço vetorial. Denotaremos o grau por $[L : K] = \dim_K L$.

(iii) Dado um conjunto $X \subset L$, denotamos por $K(X)$ o corpo gerado por $K \cup X$. Caso seja finito, isto é, $X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, denotamos $K(X) = K(\alpha_1, \ldots, \alpha_n)$, e dizemos que é o corpo obtido a partir de K pela *adjunção* de $\alpha_1, \ldots, \alpha_n$.

(iv) Uma extensão $L \mid_K$ é dita simples se $L = K(\alpha)$ para algum $\alpha \in L$.

(v) Se X for um conjunto finito, dizemos que $K(X)$ é finitamente gerada.

(vi) Dizemos que uma extensão $L \mid_K$ é finita se $[L : K] < \infty$.

Assim, temos que $\mathbb{R}(i) = \mathbb{C}$ é um exemplo de extensão simples de $\mathbb{R}$, gerada a partir da adjunção da unidade imaginária i. Note que esse elemento não é único. Por exemplo, $\mathbb{R}(-i) = \mathbb{R}(i) = \mathbb{C}$. Mais ainda, temos que i é a raiz do polinômio $p(x) = x^2 + 1$, o qual é irredutível sobre $\mathbb{R}$. Assim, dizemos que i é algébrico sobre $\mathbb{R}$.

Definição 1.1.2. (i) Seja $L \mid_K$ uma extensão de corpos. Um elemento $\alpha \in L$ é dito algébrico sobre K se α é raiz de algum polinômio $p \in K[x]$. Caso contrário, α é dito transcendente.

(ii) A extensão $L \mid_K$ é dita algébrica se todos elementos de L são algébricos sobre K.

(iii) Se α é algébrico sobre K, então denotamos por $m_\alpha \in K[x]$ seu polinômio minimal: o polinômio mônico de menor grau em $K[x]$ tal que $m_\alpha(\alpha) = 0$.

Observe que um polinômio minimal $m \in K[x]$ é um polinômio irredutível em $K[x]$. De fato, suponhamos que m seja redutível sobre K, isto é, $m = fg$, onde f, g tem grau menor do que m. Vamos assumir f e g mônicos. Então, como $m(\alpha) = 0$, temos que $f(\alpha)g(\alpha) = 0$, isto é, $f(\alpha) = 0$ ou $g(\alpha) = 0$, o que contradiz a definição de m.

Suponhamos agora $p \in K[x]$ tal que $p(\alpha) = 0$. Pelo algoritmo da divisão, existem $q, r \in K[x]$ tais que $p(x) = m(x)q(x) + r(x)$, com grau de r menor do que o grau de m. Logo, $p(\alpha) = 0 = r(\alpha)$. Pela minimalidade do grau de m, temos que $r = 0$. Assim, m divide todos os polinômios que possuem α como raiz.

Note que se uma extensão é finita, então ela é algébrica e finitamente gerada [20; Lemma 6.11.].

Teorema 1.1.3. *Seja $K(\alpha) \mid_K$ uma extensão algébrica simples, e seja $m \in K[x]$ o polinômio minimal de α sobre K. Então $K(\alpha) \mid_K$ é isomorfa a $K[x]/\langle m \rangle \mid_K$, onde $\langle m \rangle$ denota o ideal gerado por m em $K[x]$.*

Demonstração. O isomorfismo $\phi : K[x]/\langle m \rangle \to K(\alpha)$ é definido por $\bar{p} \mapsto p(\alpha)$, onde $\bar{p}$ é a classe de equivalência de $p \mod m$. Caso $\bar{p} = \bar{q}$, então $p - q = mn$, para algum $n \in K[x]$. Assim, $p(\alpha) - q(\alpha) = m(\alpha)n(\alpha) = 0$. Além disso, ϕ é claramente sobrejetivo.

Como $p(\alpha) = 0$ se e somente se m divide p, temos que a aplicação é um monomorfismo entre corpos. Logo, as extensões são isomorfas. □

Um resultado que pode ser obtido a partir deste teorema é que se $K(\alpha) \mid_K$ e $K(\beta) \mid_K$ são extensões algébricas tais que $m_\alpha = m_\beta \in K[x]$, então são extensões isomorfas. Assim, a caracterização das extensões pode ser feita a partir do polinômio minimal.

A ideia da teoria de Galois é estudar uma extensão de corpos $L \mid_K$ a partir do grupo de K-automorfismos de L, os automorfismos $\sigma : L \to L$ tais que $\sigma(k) = k$, para todo $k \in K$, isto é, $\sigma \mid_K = \mathrm{id}_K$.

Observe que $\sigma(kx) = \sigma(k)\sigma(x) = k\sigma(x)$, para quaisquer $k \in K$, $x \in L$. Assim, os K-automorfismos de L são isomorfismos de anéis e também morfis-

mos de K-espaços vetoriais. Além disso, formam um grupo com a operação de composição: sabemos que a composição de K-automorfismos será também um K-automorfismo de L. Além disso, id_L é um K-automorfismo. Basta verificarmos se, dado um K-automorfismo σ, seu inverso σ^{-1} também é um K-automorfismo de L. De fato é, pois $\sigma^{-1}(k) = \sigma^{-1}(\sigma(k)) = k$, para todo $k \in K$.

Se α é algébrico sobre K, e $\sigma : K(\alpha) \to K(\alpha)$ é um K-automorfismo, então $0 = \sigma(0) = \sigma(m_\alpha(\alpha)) = m_\alpha(\sigma(\alpha))$. Assim, $\sigma(\alpha)$ é uma raiz de m_α. Logo a ação de σ em $K(\alpha)$ apenas permuta as raízes do polinômio minimal m_α.

1.1.1 A Correspondência de Galois

Para ilustrar a correspondência de Galois, tomemos a extensão $L\,|_K$, com $L = \mathbb{Q}(\sqrt{2}, i)$ e $K = \mathbb{Q}$. Como os K-automorfismos de L permutam as raízes do polinômio minimal, observando os polinômios minimais podemos determinar o grupo dos K-automorfismos de L – o grupo de Galois da extensão, denotado por $\mathrm{Gal}\,(L\,|_K)$.

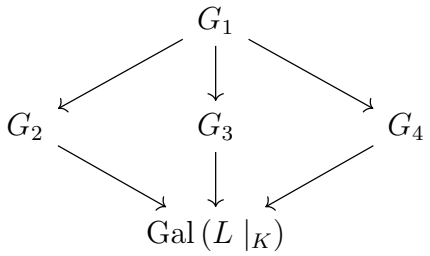
Os polinômios minimais são $m_{\sqrt{2}}(x) = x^2 - 2$ e $m_i(x) = x^2 + 1$. Portanto, um automorfismo $\sigma \in \mathrm{Gal}\,(L\,|_K)$ é tal que $\sigma(i) = \pm i$ e $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Portanto, o grupo é formado pelos automorfismos $\{\sigma_i, \sigma_2, \sigma_{2,i}, 1\}$ (denotamos $1 = \mathrm{id}_L$ o automorfismo identidade), tais que

$$\begin{array}{rcr} \sigma_i(i) = -i & & \sigma_i(\sqrt{2}) = \sqrt{2} \\ \sigma_2(i) = i & \text{e} & \sigma_2(\sqrt{2}) = -\sqrt{2} \\ \sigma_{2,i}(i) = -i & & \sigma_{2,i}(\sqrt{2}) = -\sqrt{2} \end{array}$$

Assim, podemos observar que $\mathrm{Gal}\,(L\,|_K) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, e que os subgrupos de $\mathrm{Gal}\,(L\,|_K)$ são os seguintes:

$$G_1 = \{1\} \qquad G_2 = \{1, \sigma_i\} \qquad G_3 = \{1, \sigma_2\} \qquad G_4 = \{1, \sigma_{2,i}\}$$

Estes subgrupos dão origem ao diagrama a seguir.

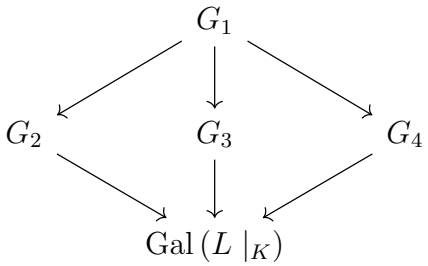


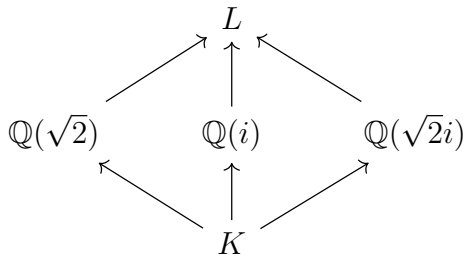
A cada subgrupo, corresponde um *corpo fixo* pela ação desse subgrupo. Por exemplo, seja $z = a + bi + c\sqrt{2} + di\sqrt{2} \in L$. Se z permanece fixo pela ação de G_2, temos que

$$\begin{aligned} \sigma_i(z) &= z \\ a - bi + c\sqrt{2} - di\sqrt{2} &= a + bi + c\sqrt{2} + di\sqrt{2} \\ &\Rightarrow b = d = 0 \end{aligned}$$

Assim, o corpo fixo associado ao subgrupo G_2 é $\mathbb{Q}(\sqrt{2})$. Da mesma forma, podemos determinar os corpos fixos a partir da ação dos outros subgrupos de $\mathrm{Gal}\,(L\mid_K)$, obtendo o diagrama abaixo.

Note que o corpo que permanece fixo por todos os elementos de $\mathrm{Gal}\,(L\mid_K)$ é exatamente K. Além disso, para cada subcorpo intermediário, temos um subgrupo associado a ele, uma relação biunívoca.





Por outro lado, tomando a extensão $L\mid_K = \mathbb{Q}(\alpha)\mid_{\mathbb{Q}}$, onde $\alpha = \sqrt[3]{2}$, temos que $\mathrm{Gal}\,(L\mid_K) = \{1\}$, pois as raízes do polinômio minimal $m_\alpha = t^3 - 2$ não estão todas em $\mathbb{Q}(\alpha)$. Assim, o corpo fixo pela ação de $\mathrm{Gal}\,(L\mid_K) = \{1\}$ é L, e não K. Assim, vamos buscar quais condições são necessárias para que a correspondência de Galois seja biunívoca.

Fixemos uma extensão $L\mid_K$ qualquer. Temos a classe dos corpos intermediários de $L\mid_K$ e também a classe dos subgrupos de $\mathrm{Gal}\,(L\mid_K)$. Seja H um subgrupo de $\mathrm{Gal}\,(L\mid_K)$ e M um corpo intermediário da extensão $L\mid_K$, isto é, $K \subset M \subset L$. Denotamos por L^H o subcorpo de L fixo pela ação do subgrupo H, e M^* o grupo dos M-automorfismos de L.

Se H é subgrupo de $\mathrm{Gal}\,(L\mid_K)$, então L^H é subcorpo de L e contém K. Tomando $x, y \in L^H$ e $\sigma \in H$, temos $\sigma(x+y) = \sigma(x) + \sigma(y) = x + y$. Da mesma forma, $\sigma(xy) = \sigma(x)\sigma(y) = xy$ e, supondo $x \neq 0$, $\sigma(xx^{-1}) = \sigma(1) = 1$ implica que $x^{-1} = x^{-1}\sigma(xx^{-1}) = x^{-1}\sigma(x)\sigma(x^{-1}) = \sigma(x^{-1})$. Assim, L^H é de fato um subcorpo de L.

As propriedades necessárias são a *normalidade* e a *separabilidade*. Considerando o exemplo anterior, onde a correspondência entre os subcorpos de L e os subgrupos de $\mathrm{Gal}\,(L\mid_K)$ não era biunívoca, isso foi um efeito colateral da raízes de m_α que não pertenciam a L. Como $K \subset L \subset \mathbb{C}$, sabemos que o polinômio possui raízes em $\mathbb{C}$, e portanto em alguma extensão de K contendo L. Assim, por exemplo, $f(x) = x^2 + 1$ não possui raízes em $\mathbb{Q}$, mas sim em $\mathbb{Q}(i)$. Dizemos que um polinômio $f \in K[x]$ se fatora completamente sobre K se ele pode ser expresso da forma

$$f(x) = k \cdot (x - \alpha_1) \cdots (x - \alpha_n)$$

com $k, \alpha_1, \ldots, \alpha_n \in K$. Por exemplo, o polinômio $f(x) = 3x^2 + 12 \in \mathbb{Q}[x]$ se fatora sobre $\mathbb{Q}(i)$, pois pode ser escrito como $f(x) = 3(x + 2i)(x - 2i)$.

Definição 1.1.4. Dizemos que uma extensão de corpos $L\mid_K$ é normal se qualquer polinômio irredutível $f \in K[x]$ que possui uma raiz em L se fatora completamente sobre L.

Dizemos que uma extensão $\Sigma\mid_K$ é corpo de decomposição para $f \in K[x]$ se Σ é gerada a partir da adjunção das raízes de f, isto é, $\Sigma = K(\alpha_1, \ldots, \alpha_n)$, onde α_i, $i = \{1, \ldots, n\}$, são todas as raízes de f.

Se uma extensão $L\mid_K$ é normal e finita, então sabemos que L é algébrica e finitamente gerada, isto é, $L = K(\alpha_1, \ldots, \alpha_n)$. Tomemos então m_i o polinômio minimal de α_i, para cada $i \in \{1, \ldots, n\}$. Seja $f = m_1 \cdots m_n$. Como

$m_i(\alpha_i) = 0$, temos que f tem raízes em L, e portanto, como L é normal, f se fatora completamente em L, ou seja, todas suas raízes pertencem a L e L é gerado a partir da adjunção das raízes de f. Logo, é um corpo de decomposição para f. Reciprocamente, podemos mostrar que uma extensão $L\ |_K$ é normal e finita somente se é corpo de decomposição para algum polinômio $f \in K[x]$ [20; Theorem 9.9.].

Vamos agora abordar a separabilidade.

Definição 1.1.5. (i) Seja $L\ |_K$ extensão de corpos e seja $f \in K[x]$ polinômio irredutível com $\partial f \geq 1$. Dizemos que f é separável sobre K se admite somente raízes simples em seu corpo de decomposição Σ (que é único a menos de isomorfismos [20]), ou seja, $f(x) = k \cdot (x - \alpha_1) \dots (x - \alpha_n) \in \Sigma[x]$. Um polinômio que não é separável é dito inseparável.

(ii) Um elemento $\alpha \in L$ algébrico sobre K é dito separável sobre K se seu polinômio minimal $m_\alpha \in K[t]$ é separável sobre K.

(iii) Uma extensão $L\ |_K$ é dita separável se todo elemento de L for separável sobre K.

A propriedade da separabilidade pode se trivializar se tratando de corpos de característica 0, no sentido de que *todo* polinômio irredutível é separável neste caso. Segue na proposição a seguir uma caracterização de separabilidade para corpos abstratos:

Proposição 1.1.6. *Se K é um corpo de característica 0, todo polinômio irredutível sobre K é separável sobre K.*

Se K tem característica $p > 0$, então um polinômio irredutível é inseparável se e somente se $f(x) = k_0 + k_1 x^p + \dots + k_r t^{rp} = g(x^p)$, para algum $g \in K[x]$.

Para demonstrar a proposição acima, iremos utilizar a derivada formal: dado um polinômio $f(x) \in K[x]$,

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

a derivada formal de f é o polinômio

$$Df(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

em $K[x]$. A derivada formal herda várias propriedades da derivada usual em $\mathbb{R}$, por exemplo $D(f+g) = Df + Dg$ e $D(fg) = (Df)g + f(Dg)$.

Claramente D é linear. Além disso,

$$\begin{aligned} D(x^k f) &= D(a_0x^k + \cdots + a_nx^{n+k}) \\ &= ka_0x^{k-1} + (k+1)a_1x^k + \cdots + (n+k)a_nx^{n+k-1} \\ &= kx^{k-1}\left[a_0 + a_1x + \cdots + a_nx^n\right] \\ &\quad + x^k\left[a_1 + 2a_2x + \cdots + na_nx^{n-1}\right] \\ &= (Dx^k)f + x^k(Df) \end{aligned}$$

Assim, a partir da linearidade, temos $D(fg) = (Df)g + f(Dg)$.

Afirmamos que uma raiz α de f é múltipla no seu corpo de decomposição se e somente se f e Df têm fator comum não constante em $K[x]$. De fato, seja Σ o corpo de decomposição para f e suponha $f(x) = (x-\alpha)^2g(x) \in \Sigma[x]$. Então $Df = 2(x-\alpha)g(x) + (x-\alpha)^2Dg = (x-\alpha)\left[2g(x) + (x-a\alpha)Dg\right] \in \Sigma[x]$. Seja m_α o polinômio minimal de α sobre K. Logo m_α é um fator comum entre f e Df em $K[x]$.

Por outro lado, se f não tem raízes múltiplas, suponha que f e Df têm um fator comum (não constante) em $K[x]$ e seja α raiz deste fator. Então $f = (x-\alpha)g$ em $\Sigma[x]$ e $Df = (x-\alpha)h$ em $\Sigma[x]$. Assim, $Df = (x-\alpha)Dg + g = (x-\alpha)h$. Portanto $(x-\alpha)$ divide g, e $(x-\alpha)^2$ divide f, mostrando que α é raiz múltipla em Σ. Vamos agora para a demonstração da Proposição 1.1.6:

Demonstração. Para $f \in K[x]$ ser irredutível e inseparável, então f e Df têm fator comum não constante. Como f é irredutível e Df tem grau menor do que f, temos $Df = 0$. Assim, se

$$f(x) = a_0 + \cdots + a_nx^n$$

temos que $ma_m = 0$, para todo $m > 0$.

Em característica 0, isso implica $a_m = 0$, para todo m. Em característica $p > 0$, temos que $a_m = 0$ se p não divide m. Tomemos $k_i = a_i p$, e segue o resultado. □

O teorema a seguir nos permite relacionar qualquer extensão separável e finita com uma extensão algébrica simples. Assim, pelo Teorema 1.1.3, temos que $L \simeq K[x]/\langle m \rangle$, para algum polinômio irredutível m sobre K. O resultado foi extraído de [9; Teorema 1.2.6, p.15].

Teorema 1.1.7 (Teorema do Elemento Primitivo)**.** *Seja $L\,|_K$ uma extensão de corpos finita e separável. Então $L = K(\alpha)$ para algum $\alpha \in L$.*

Demonstração. Seja $L = K(\alpha_1, \ldots, \alpha_n)$. Para demonstrar que L é uma extensão simples de K, vamos utilizar indução em n. Se $n = 1$, não há nada a demonstrar, pois $L = K(\alpha_1)$. Suponha que $M = F(\alpha_1, \ldots, \alpha_{n-1})$ é uma extensão simples de K, isto é, $M = K(\beta)$, para algum $\beta \in M$. Então $L = M(\alpha_n) = K(\beta, \alpha_n)$. Assim, temos nossa demonstração reduzida ao caso $n = 2$.

Digamos que L é gerado por dois elementos α e β. Sejam $f(x)$ e $g(x)$ os polinômios minimais de α e β sobre K, e seja Σ o corpo de decomposição destes polinômios. Sejam $\alpha_1 = \alpha, \alpha_2 \ldots, \alpha_r$ e $\beta_1 = \beta, \beta_2, \ldots, \beta_s$ as raízes de f e g, respectivamente. Como f e g são separáveis, temos que as raízes são todas distintas. Consideremos agora as seguintes equações em x:

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

com $1 \leq i \leq r$ e $2 \leq j \leq n$. Estas equações têm exatamente uma solução no fecho normal $\bar{K}$,

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

Seja k um elemento de K que não seja solução destas equações, e tomemos $\gamma = \beta + k\alpha$.

Vamos mostrar que a extensão L é gerada pela adjunção de γ, isto é, $K(\alpha, \beta) = K(\gamma)$. Como $\gamma \in K(\alpha, \beta)$, temos que $K(\gamma) \subset K(\alpha, \beta)$. Agora, basta mostrarmos que α e β pertencem a $K(\gamma)$.

Para mostrar que $\beta \in K(\gamma)$, vamos mostrar que α é raiz de um polinômio de grau 1 sobre $K(\gamma)$. Consideremos os polinômios f e g como anteriormente. Temos que $f(x)$ e $h(x) = g(\gamma - kx)$ são polinômios sobre $K(\gamma)$. Dada a forma como $h(x)$ foram escolhido, α é raiz de ambos os polinômios, pois $h(\alpha) = g(\gamma - k\alpha) = g(\beta) = 0$. Assim, o máximo divisor comum destes polinômios é divisível por $x - \alpha$ em $\bar{K}[x]$, admitindo portanto a raiz α. Como f não tem raízes múltiplas, seu máximo divisor comum também não as tem, ou seja, α é uma raiz simples. Mas, pela escolha de k, os polinômios $f(x)$ e $h(x)$ não têm outra raíz em comum, dado que as raízes de $f(x)$ são α_i, com $i \in \{1, \ldots, r\}$, e $\gamma - k\alpha_i \neq \beta_j$, para todo $j \in \{2, \ldots, s\}$. Portanto, o máximo divisor comum é um polinômio sobre $K(\gamma)$, o corpo dos coeficientes de $f(x)$ e $h(x)$. Portanto, α é a raiz de um polinômio de grau 1 sobre $K(\gamma)$, ou seja, $\alpha \in K(\gamma)$. Assim, $\gamma - k\alpha = \beta \in K(\gamma)$. □

Uma vez que os conceitos de normalidade e separabilidade foram esclarecidos, definimos uma extensão galoisiana e finalizamos a seção enunciando o Teorema de Correspondência de Galois no caso clássico [20; Theorem 17.23, p.202].

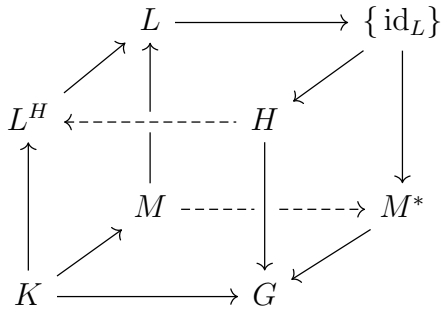
Definição 1.1.8. Se $L \mid_K$ é uma extensão de corpos finita, normal e separável, então L é dita *extensão de Galois* de K com grupo de Galois $G = \mathrm{Aut}_K(L)$.

Teorema 1.1.9. *Se $L \mid_K$ é uma extensão de Galois com grupo de Galois G, então:*

1. *O grupo de Galois G tem ordem $[L : K]$;*
2. *Existe uma correspondência biunívoca, que inverte ordem, entre os subgrupos de G e os subcorpos de L que contém K;*
3. *Se M é um corpo intermediário e M^* é o subgrupo dos M-automorfismos de L, então $[L : M] = |M^*|$ e $[M : K] = |G| \,/\, |M^*|$;*
4. *Um corpo intermediário M é uma extensão normal de K se e somente se M^* é um subgrupo normal de G;*

5. *Se um corpo intermediário M é uma extensão normal de K, então o grupo de Galois de $M\,|_K$ é isomorfo ao grupo quociente G/M^*.*

A correspondência entre os subgrupos de G e os subcorpos de L que contém K pode ser observada no diagrama a seguir.



Note que os conceitos de normalidade e separabilidade se apoiam nos resultados sobre polinômios. Para generalizar estes resultados para extensões de anéis comutativos, vamos utilizar as equivalências a seguir, apresentadas em [15].

Teorema 1.1.10. *Seja $L\,|_K$ uma extensão de corpos e G um grupo finito de K-automorfismos de L.*

Seja $L \rtimes G$ o L-espaço vetorial com base $\{\delta_\sigma \mid \sigma \in G\}$, com multiplicação definida por $a_\sigma \delta_\sigma b_\tau \delta_\tau = a_\sigma \sigma(b_\tau)\delta_{\sigma\tau}$ para os elementos geradores e estendida linearmente para os demais elementos.

Então, são equivalentes:

1. *$L^G = K$;*
2. *L é uma extensão de Galois de K e G é o grupo de todos os K-automorfismos de L;*
3. *O grupo G tem ordem $[L : K]$;*
4. *L é uma extensão finita de K e $\varphi : L \rtimes G \to Hom_K(L, L)$ é um isomorfismo de K-álgebras.*

1.2 Módulos Projetivos

Diversos dos resultados apresentados para corpos são provenientes da estrutura de K-espaço vetorial da extensão L. Para estudarmos a generalização sobre anéis comutativos, precisamos de resultados acerca de módulos. Importante ressaltar que, ao longo desta dissertação, os anéis serão anéis comutativos com unidade, exceto quando o contrário estiver explicitamente mencionado.

Definição 1.2.1. Seja R um anel comutativo com unidade. Um grupo abeliano M é dito *R-módulo* se existe uma ação linear $R \times M \to M$ compatível com a multiplicação de R. Ou seja, dados $r, r_1, r_2 \in R$ e $m, m_1, m_2 \in M$

$$\begin{aligned}(r_1 + r_2)m &= r_1m + r_2m \\ r(m_1 + m_2) &= rm_1 + rm_2 \\ r_1(r_2m) &= (r_1r_2)m \\ 1_Rm &= m\end{aligned}$$

Um *R-submódulo de M* é um subgrupo M' de M fechado sobre a ação de R. Além disso, o grupo quociente M/M' herda a estrutura de R-módulo pela ação $r(m + M') = rm + M'$.

Alguns exemplos de R-módulos são os ideais de R – inclusive o próprio anel R – e os polinômios com coeficientes em R. Além disso, se existe um homomorfismo de anéis $f : S \to R$, então um R-módulo M também é um S-módulo, pela ação definida por $(s, m) \mapsto f(s)m$.

Se x é um elemento de M, os múltiplos de x formam um submódulo de M, denotado por Rx. Se $M = \sum_{i \in I} Rx_i$, os elementos x_i's são chamados de *geradores* de M. Se existe um conjunto finito de geradores de M, então M é dito *finitamente gerado*. Por exemplo, o anel $R[x]$ dos polinômios sobre R não é finitamente gerado, mas seu submódulo formado pelos polinômios de grau menor ou igual a n é.

Se M e N são R-módulos, a *soma direta* $M \oplus N$ é o conjunto de todos os pares $x + y$, com $x \in M$ e $y \in N$, e definimos as operações de adição e

multiplicação por escalar da forma usual. De forma mais geral, se $(M_i)_{i\in I}$ é uma família de R-módulos, podemos definir a soma direta $\bigoplus_{i\in I} M_i$; seus elementos são famílias $\sum_{i\in I} x_i$ tais que $x_i \in M_i$, para cada $i \in I$, e quase todos os x_i são 0 – isto é, $x_i \neq 0$ apenas para um número finito de índices $i \in I$.

Dizemos que um R-módulo M é *livre* se é isomorfo a um R-módulo da forma $\bigoplus_{i\in I} M_i$, com cada $M_i \simeq R$. Assim, um R-módulo livre finitamente gerado é isomorfo a $R^n = R \oplus \cdots \oplus R$.

Além disso, se M é um R-módulo finitamente gerado, então sejam $x_1, \ldots,$ x_n geradores de M, e defina $\phi : R^n \to M$ por $\phi(r_1, \ldots, r_n) = \sum_{i=1}^{n} r_i x_i$. Então ϕ é um homomorfismo de R-módulos sobrejetivo, e portanto $M \simeq R^n/\ker\phi$.

Por outro lado, se temos um epimorfismo $\phi : R^n \to M$, e

$$e_i = (0, \ldots, 1, \ldots, 0)$$

então os e_i's $(1 \leq i \leq n)$ geram R^n e o conjunto formado pelas suas respectivas imagens $\phi(e_i)$ gera M. Logo, M é finitamente gerado. Assim, temos a seguinte proposição, que nos permite caracterizar os módulos finitamente gerados.

Proposição 1.2.2. *[3; II,Propositon 2.3] M é um R-módulo finitamente gerado se e somente se M é isomorfo a um quociente de R^n, para algum $n > 0$.*

Seja

$$\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

uma sequência de R-módulos e R-homomorfismos. Dizemos que essa é uma sequência *exata em* M_i se $\mathrm{Im}(f_i) = \ker f_{i+1}$; se a sequência é exata em cada M_i, dizemos apenas que a sequência é exata. Note que $0 \to M' \xrightarrow{f} M$ é exata se e somente se f é um monomorfismo, e $M \xrightarrow{g} M' \to 0$ é exata se e somente se g é um epimorfismo. Além disso, a sequência

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

é exata se e somente se f é injetivo, g é sobrejetivo e g induz um isomorfismo

$$\mathrm{Coker}(f) = M/f(M') = M/\ker g \simeq M'' = \mathrm{Im}(g)$$

A Proposição a seguir, extraída de [19; 1.3.6], traz um resultado semelhante ao Teorema do Núcleo-Imagem, de espaços vetoriais, para o caso de módulos.

Proposição 1.2.3. *Seja R um anel e consideremos a sequência exata curta de R-módulos*

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0.$$

Então, as seguintes afirmações são equivalentes:

1. *$M \simeq N \oplus P$;*
2. *Existe um R-homomorfismo $\psi : M \to N$, tal que $\psi \circ f = id_N$;*
3. *Existe um R-homomorfismo $\varphi : P \to M$ tal que $g \circ \varphi = id_P$.*

Demonstração. A seguir, segue a demonstração da equivalência $(1 \Leftrightarrow 2)$. A equivalência $(1 \Leftrightarrow 3)$ pode ser demonstrada com uma argumentação semelhante.

Como f é injetivo, segue que $N \simeq f(N)$ e assim, $M \simeq N \oplus P \simeq f(N) \oplus P$. Desta forma, dado $m \in M$, temos $m = m_1 + m_2$, com $m_1 \in f(N)$ e $m_2 \in P$. Novamente pela injetividade de f, segue que existe um único $n \in N$ tal que $f(n) = m_1$. Definimos então $\psi : M \to N$ por $\psi(m) = n$. Segue da escrita única e da injetividade de f que ψ está bem definida é um R-homomorfismo. Mais ainda, para todo $n \in N$, $f(n)$ se escreve de forma única como $f(n) + 0 \in f(N) \oplus P$, e onde segue $\psi \circ f = \mathrm{id}_N$.

Suponhamos que exista $\psi : M \to N$ tal que $\psi \circ f = \mathrm{id}_N$. Neste caso, $M = f(N) \oplus \ker \psi$, pois se $m \in M$, tomamos $x = f(\psi(m)) \in M$ e consideramos $y = m - x \in M$. Segue então que

$$\psi(y) = \psi(m - x)\psi(m) - \psi(f(\psi(m))) = \psi(m) - \psi(m) = 0$$

isto é, $y \in \ker \psi$. Logo, $m = x + y \in f(N) + \ker \psi$. Além disso, se $z \in f(N) \cap \ker \psi$, segue que existe $n \in N$ tal que $f(n) = z$, o que implica $n = \psi \circ f(n) = \psi(z) = 0$, de onde decorre $z = 0$. Portanto, $M = f(N) \oplus \ker \psi$.

Resta mostrar que $P \simeq \ker \psi$. Basta observar que

$$P \simeq \frac{M}{\ker g} = \frac{f(N) \oplus \ker \psi}{f(N)} \simeq \ker \psi.$$

□

Agora, vamos descrever algumas propriedades do produto tensorial sobre sequências exatas. Em [3; II, p.28], Atiyah e Macdonald desenvolvem um isomorfismo canônico

$$\mathrm{Hom}\,(M \otimes N, P) \simeq \mathrm{Hom}\,(M, \mathrm{Hom}\,(N, P))$$

a partir do qual demonstramos que o produto tensorial é exato – isto é, leva sequência exatas em sequências exatas – sob certas condições. Por exemplo, seja

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

uma sequência exata de R-módulos e N um R-módulo qualquer. Então a sequência

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0$$

é exata [3; II, Proposition 2.18.]. Porém, isso não é verdade para qualquer R-módulo N e qualquer sequência. De fato, considere $R = \mathbb{Z}$ e a sequência exata

$$0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

onde $f(x) = 2x$. Se $N = \mathbb{Z}_2$, a sequência não é exata, pois para qualquer $x \otimes y \in \mathbb{Z} \otimes \mathbb{Z}_2$, temos $(f \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = 0$, e $\mathbb{Z} \otimes N \neq 0$.

Assim, a aplicação $M \mapsto M \otimes_R N$ nem sempre preserva a exatidão da sequência. Se esta aplicação preservar exatidão, isto é, se tensorizar uma sequência com N transforma qualquer sequência exata em outra sequência exata, então N é dito um R-módulo *plano*.

Proposição 1.2.4. *Seja N um R-módulo. São equivalentes:*

1. *N é plano;*
2. *Se $0 \to M' \to M \to M'' \to 0$ é uma sequência exata de R-módulos, a sequência tensorizada $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ também é exata;*
3. *Se $f : M' \to M$ é injetiva, então $f \otimes 1 : M' \otimes N \to M \otimes N$ é injetiva;*
4. *Se $f : M' \to M$ é injetiva e M, M' são finitamente gerados, então $f \otimes 1 : M' \otimes N \to M \otimes N$ é injetiva.*

Demonstração. $(1 \Leftrightarrow 2)$ é direta da definição, quebrando sequências exatas longas em sequências exatas curtas.

$(2 \Leftrightarrow 3)$ é consequência de [3; II, Proposition 2.18.].

$(3 \Rightarrow 4)$ é direta.

$(4 \Rightarrow 3)$ Seja $f : M' \to M$ injetiva e $u = \sum_{i \in I} x_i \otimes y_i \in \ker(f \otimes 1)$, ou seja, $\sum_{i \in I} f(x_i) \otimes y_i = 0$. Seja M'_0 o submódulo de M' gerado por x_i e seja $u_0 = \sum_{i \in I} x_i \otimes y_i$ como um elemento de $M'_0 \otimes N$. Então existe um submódulo finitamente gerado M_0 de M que contém $f(M'_0)$ e tal que $(f \otimes 1)(u_0) = 0$ como elemento de $M_0 \otimes N$. Se $f_0 : M'_0 \to M_0$ é a restrição de f, isso significa que $(f_0 \otimes 1)(u_0) = 0$. Como M_0 e M'_0 são finitamente gerados, $f_0 \otimes 1$ é injetiva e portanto $u_0 = 0$, logo $u = 0$; assim, $f \otimes 1$ é injetiva. □

Se L_0 e L_1 são R-módulos livres, dizemos que a sequência exata de R-módulos $L_1 \to L_0 \to M \to 0$ é uma *apresentação* de um R-módulo M. Essa apresentação é dita finita se L_0 e L_1 são finitamente gerados, e M é dito um R-módulo de apresentação finita. Em [5; I, §2.8, p.20], Bourbaki apresenta o resultado a seguir.

Proposição 1.2.5.
1. *Todo módulo finitamente apresentado é finitamente gerado;*
2. *Todo módulo finitamente gerado projetivo admite apresentação finita.*

Claramente, a primeira afirmação decorre diretamente das definições.

Um R-módulo P é projetivo se é somando direto de um R-módulo livre, isto é, se existem um R-módulo livre L e um submódulo $Q \subset L$ tais que $L = P \oplus Q$. Assim, suponha M um R-módulo projetivo finitamente gerado; então é somando direto de um R-módulo livre L_0, e o núcleo N do epimorfismo $L_0 \to M$ é isomorfo a um quociente de L_0, e portanto finitamente gerado. Assim, dada a sequência $N \to L_0 \to M \to 0$, temos que M admite apresentação finita.

O teorema a seguir traz equivalências para a definição de módulo projetivo, e nos permite uma melhor compreensão sobre estes módulos.

Teorema 1.2.6. *[15; Teorema 2.1.] Seja P um R-módulo. As seguintes proposições são equivalentes:*

1. *P é projetivo;*

2. *Dado o diagrama*

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \sigma} & & \\ M & \xrightarrow{\theta} & N & \longrightarrow & 0 \end{array}$$

   de R-módulos, onde θ é sobrejetivo, existe um homomorfismo $\sigma' : P \to M$ tal que $\sigma'\theta = \sigma$.

3. *Se $0 \to M' \xrightarrow{\beta} M \xrightarrow{\alpha} N \to 0$ é uma sequência exata de R-módulos, então a sequência*

$$0 \to Hom_R(P, M') \xrightarrow{\beta^*} Hom_R(P, M) \xrightarrow{\alpha^*} Hom_R(P, N) \to 0$$

   é exata, onde β^* e α^* são dadas por $\beta^*(f) = \beta \circ f$ e $\alpha^*(g) = \alpha \circ g$.

4. *Toda sequência exata de R-módulos $M \xrightarrow{\phi} P \to 0$ cinde, isto é, existe um homomorfismo de R-módulos $\psi : P \to M$ tal que $\phi\psi = id_P$.*

5. *Existem conjuntos* $\{p_i \mid i \in I\}$ *em* P *e* $\{f_i \mid i \in I\}$ *em* $P^* = Hom_R(P, R)$ *tais que para todo* $p \in P$, $p = \sum_{i \in I} f_i(p)p_i$, *onde* $f_i(p) = 0$ *exceto para um número finito de índices.*

Demonstração. $(1 \Rightarrow 2)$ Consideremos o diagrama acima, onde θ é sobrejetivo. Como P é somando direto de um R-módulo livre L, existe um submódulo Q de L tal que $L = P \oplus Q$. Seja $\pi : L \to P$ a projeção canônica, e consideremos uma base $\{e_i \mid i \in I\}$ de L, e seja $n_i = \sigma(\pi(e_i)) \in N$, para cada $i \in I$, e seja $m_i \in M$ tal que $\theta(m_i) = n_i$, para cada $i \in I$. Definimos $\tau : L \to M$ por $\tau\left(\sum_{i \in I} r_i e_i\right) = \sum_{i \in I} r_i m_i$. Note que $r_i = 0$ para quase todo $i \in I$. Evidentemente τ é R-linear e $\theta \circ \tau = \sigma \circ \pi$, logo basta tomarmos $\sigma' = \tau \mid_P$.

$(2 \Rightarrow 3)$ Consideremos a sequência exata de R-módulos

$$0 \to M' \xrightarrow{\beta} M \xrightarrow{\alpha} N \to 0$$

Sejam β^*, α^* como na hipótese. Se $\beta^*(f) = 0$ para algum $f \in \mathrm{Hom}_R(P, M')$, então $\beta(f(p)) = 0$ para todo $p \in P$. Assim, $f(p) \in \ker \beta = 0$, logo $f = 0$, e β^* é injetiva.

Seja $g \in \mathrm{Hom}_R(P, M)$. Se $g = \beta \circ f$ para algum $f \in \mathrm{Hom}_R(P, M')$, então $\alpha^*(g) = \alpha \circ \beta \circ f = 0$, logo $g \in \ker \alpha^*$. Assim, $\beta^*(\mathrm{Hom}_R(P, M')) \subset \ker \alpha^*$.

Por outro lado, suponha $g \in \ker \alpha^*$. Então $\alpha \circ g = \alpha^*(g) = 0$, o que implica $\alpha \circ g(p) = 0$ para todo $p \in P$. Logo $g(p) \in \ker \alpha = \beta(M')$, para qualquer $p \in P$. Portanto, existe $x_p \in M'$ tal que $\beta(x_p) = g(p)$, para todo $p \in P$ e definimos $f : P \to M'$ por $f(p) = x_p \in M'$. f é um homomorfismo de R-módulos e temos que $\beta^*(f)(p) = (\beta \circ f)(p) = \beta(x_p) = g(p)$ para todo $p \in P$, ou seja, $g = \beta^*(f)$ pertence a $\beta^*(\mathrm{Hom}_R(P, M'))$. Assim, $\beta^*(\mathrm{Hom}_R(P, M')) = \ker \alpha^*$.

Por fim, seja $\gamma \in \mathrm{Hom}_R(P, N)$. Então temos que existe um homomorfismo γ^* em $\mathrm{Hom}_R(P, M)$ tal que $\alpha \circ \gamma^* = \gamma$, ou seja $\alpha^*(\gamma^*) = \gamma$. Assim, a sequência

$$0 \to \mathrm{Hom}_R(P, M') \xrightarrow{\beta^*} \mathrm{Hom}_R(P, M) \xrightarrow{\alpha^*} \mathrm{Hom}_R(P, N) \to 0$$

é exata.

(3 $\Rightarrow$ 4) Suponhamos que a sequência de R-módulos $M \xrightarrow{\phi} P \to 0$ é exata. Podemos estendê-la para a sequência exata

$$0 \to \ker \phi \to M \xrightarrow{\phi} P \to 0$$

Por (3) sabemos que a sequência

$$0 \to \mathrm{Hom}_R(P, \ker \phi) \to \mathrm{Hom}_R(P, M) \xrightarrow{\phi^*} \mathrm{Hom}_R(P, P) \to 0$$

é exata. Logo, dado $\mathrm{id}_P \in \mathrm{Hom}_R(P, P)$, existe $\psi \in \mathrm{Hom}_R(P, M)$ tal que $\phi^*(\psi) = \mathrm{id}_P$, isto é, $\phi \circ \psi = \mathrm{id}_P$. Portanto, a sequência $M \xrightarrow{\phi} P \to 0$ cinde.

(4 $\Rightarrow$ 5) Sejam $\{p_i \mid i \in I\}$ geradores de P como R-módulo. Seja L um R-módulo livre com base $\{e_i \mid i \in I\}$. Definimos o homomorfismo de R-módulos $\rho : L \to P$ dado por $\rho(e_i) = p_i$, para todo $i \in I$. Obviamente $L \xrightarrow{\rho} P \to 0$ é exata e cinde. Então existe um homomorfismo $\delta : P \to L$ tal que $\rho \circ \delta = \mathrm{id}_P$.

Seja $\pi_i : L \to R$ dada por $\pi_i(\sum_{j \in I} r_j e_j) = r_i$ e defina $f_i : P \to R$ por $f_i = \pi_i \circ \delta$, para todo $i \in I$. Evidentemente $f_i \in P^*$, para todo $i \in I$.

Seja $p \in P$. Então, temos

$$\delta(p) = \sum_{i \in I} f_i(p) e_i$$

com $f_i(p) = r_i$, nulos exceto por um número finito de índices i, e

$$\begin{aligned} p = \rho \circ \delta(p) &= \rho\left(\sum_{i \in I} f_i(p) e_i\right) \\ &= \sum_{i \in I} f_i(p) \rho(e_i) = \sum_{i \in I} f_i(p) p_i \end{aligned}$$

(5 $\Rightarrow$ 1) Sejam P um R-módulo e $\{p_i \mid i \in I\} \subset P$ e $\{f_i \mid i \in I\} \subset P^*$ famílias de elementos como em (5).

Seja L um R-módulo livre com base $\{e_i \mid i \in I\}$.

Seja $\rho : L \to P$ o homomorfismo dado por $\rho(e_i) = p_i$, para todo $i \in I$. Como $p = \sum_{i \in I} f_i(p) p_i$, para todo $p \in P$, a família $\{p_i \mid i \in I\}$ gera P.

Portanto, ρ é sobrejetivo. Seja $\delta : P \to L$ o homomorfismo dado por $\delta(p) = \sum_{i\in I} f_i(p)e_i$. Logo, $\rho \circ \delta = \mathrm{id}_P$, pois

$$\begin{aligned}\rho \circ \delta(p) &= \rho\left(\sum_{i\in I} f_i(p)e_i\right) = \sum_{i\in I} f_i(p)\rho(e_i)\\ &= \sum_{i\in I} f_i(p)p_i = p\end{aligned}$$

Assim, concluímos que $P \simeq \delta(P)$ e $L \simeq \delta(P) \oplus \ker\rho$. □

O teorema a seguir é um resultado apresentado por Bourbaki e fornece condições para que um módulo à esquerda sobre um anel não necessariamente comutativos seja livre, e o Corolário 1.2.9 apresenta uma caracterização deste tipo de módulo, mediante determinadas hipóteses.

Definição 1.2.7. Seja A um anel. O *radical de Jacobson* de A, denotado por $J(A)$, é a intersecção de todos os ideais maximais de A.

Teorema 1.2.8. *[5; II, §3.2, p.83, Proposition 5] Seja A um anel (não necessariamente comutativo), $I \subset J(A)$ um ideal de A e M um A-módulo (à esquerda). Suponha que M tem apresentação finita ou I é nilpotente.*

Se $(A/I) \otimes_A M \simeq M/IM$ é um A/I-módulo livre (à esquerda) e o homomorfismo canônico $I \otimes_A M \to M$ é injetivo, então M é um A-módulo livre.

Corolário 1.2.9. *[5; II, §3.2, p.84, Corollary 2] Seja A um anel (não necessariamente comutativo), $J(A)$ o radical de Jacobson de A e M um A-módulo (à esquerda). Suponha que $A/J(A)$ é um corpo, e que uma das condições a seguir é satisfeita:*

- *M tem apresentação finita;*
- *$J(A)$ é nilpotente.*

Então as sequintes propriedades são equivalentes:

1. *M é livre;*

2. *M é projetivo;*

3. *M é plano;*

4. *o homomorfismo canônico $J(A) \otimes_A M \to M$ é injetivo.*

Demonstração. As implicações $(1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4)$ são diretas. Como $A/J(A)$ é um corpo $(A/J(A)) \otimes_A M$ é um $(A/J(A))$-módulo livre e o Teorema 1.2.8 mostra que $(4 \Rightarrow 1)$. □

Agora vamos observar a construção de anéis de frações e o processo de localização. Sejam R um anel comutativo com unidade e S um subconjunto multiplicativamente fechado de R tal que $1 \in S$. Vamos definir uma relação em R por

$$(a, s) \equiv (b, t) \Leftrightarrow (at - bs)u = 0,$$

para algum $u \in S$. Podemos ver que esta é uma relação reflexiva e simétrica com facilidade. Sejam $(a, r) \equiv (b, s)$ e $(b, s) \equiv (c, t)$. Então, existem $u, v \in S$ tais que $(as - br)u = 0$ e $(bt - cs)v = 0$. Assim, temos que $asu = bru$ e $btv = csv$; multiplicando a primeira equação por tv, e a segunda por ru, obtemos a igualdade $brutv = asutv = csvru$. Assim, $(at - cr)suv = 0$. Como S é multiplicativamente fechado, temos que $suv \in S$ e portanto $(a, r) \equiv (c, t)$. Logo a relação é transitiva e, consequentemente, de equivalência.

Como $\equiv$ é uma relação de equivalência, podemos observar as classes de equivalência determinadas por $\equiv$ em R. Assim, seja $S^{-1}R$ o conjunto das classes de equivalência de R, onde a classe de (r, s) é denotada por $\frac{r}{s}$. Definimos as operações usuais de frações em $S^{-1}R$, o que garante uma estrutura de anel [3; p.36].

Seja $\mathcal{P}$ um ideal primo de R. Então $R \setminus \mathcal{P}$ é um conjunto multiplicativamente fechado. De fato, como $\mathcal{P}$ é primo, se $xy \in \mathcal{P}$, então $x \in \mathcal{P}$ ou $y \in \mathcal{P}$. Assim, se $x, y \in R \setminus \mathcal{P}$, então $xy \in R \setminus \mathcal{P}$, caso contrário x ou y seriam elementos de $\mathcal{P}$, e isto é uma contradição. Além disso, $1 \in R \setminus \mathcal{P}$, pois se

$1 \in \mathcal{P}$, então $\mathcal{P} = R$. Seja $\mathcal{P}$ um ideal primo de R, e M um R-módulo. Denotamos por $M_{\mathcal{P}} = S^{-1}M$, onde $S = R \setminus \mathcal{P}$, a localização de M com respeito a $\mathcal{P}$. Então $R_{\mathcal{P}}$ é uma R-álgebra, $M_{\mathcal{P}}$ é um $R_{\mathcal{P}}$-módulo e $M_{\mathcal{P}} \simeq R_{\mathcal{P}} \otimes M$ são $R_{\mathcal{P}}$-módulos isomorfos [3]. De fato, a aplicação

$$\begin{aligned} R_{\mathcal{P}} \times M &\longrightarrow M_{\mathcal{P}} \\ (r/s, m) &\longmapsto rm/s \end{aligned}$$

é R-bilinear, e a propriedade universal do produto tensorial induz um R-homomorfismo

$$\begin{aligned} f : R_{\mathcal{P}} \otimes M &\longrightarrow M_{\mathcal{P}} \\ \frac{r}{s} \otimes m &\longmapsto \frac{rm}{s} \end{aligned}$$

Além disso, temos que qualquer elemento de $R_{\mathcal{P}} \otimes M$ é da forma $\frac{1}{s} \otimes m$. Seja $\sum_{i=1}^{n} (r_i/s_i) \otimes m_i$ qualquer elemento de $R_{\mathcal{P}} \otimes M$. Sejam $s = \prod_{i=1}^{n} s_i$ e $t_i = \prod_{j=1, j\neq i}^{n} s_j$. Então

$$\sum_{i=1}^{n} \frac{r_i}{s_i} = \sum_{i=1}^{n} \frac{t_i r_i}{s} = \frac{1}{s} \sum_{i=1}^{n} t_i r_i$$

$$\Rightarrow \sum_{i=1}^{n} \frac{r_i}{s_i} \otimes m_i = \frac{1}{s} \sum_{i=1}^{n} t_i r_i \otimes m_i = \frac{1}{s} \otimes \sum_{i=1}^{n} t_i r_i m_i$$

Suponha $f((1/s) \otimes m) = 0$. Então, $m/s = 0$, logo existe $k \in A \setminus \mathcal{P}$ tal que $km = 0$. Assim, temos que

$$\frac{1}{s} \otimes m = \frac{k}{sk} \otimes m = \frac{1}{sk} \otimes km = \frac{1}{sk} \otimes 0 = 0$$

e portanto f é um isomorfismo.

Capítulo 2

Extensões Galoisianas Comutativas

Tendo em mãos as ferramentas necessárias, inicia agora a caminhada para os resultados da teoria de Galois sobre anéis comutativos. Iniciaremos nos distanciando das propriedades decorrentes de polinômios – e isso impacta, principalmente, em nosso conceito de separabilidade. Vamos buscar uma nova definição de separabilidade, que seja adequada tanto para corpos quanto para as extensões de anéis, como uma generalização da definição usada para corpos.

Nesta primeira seção, iremos abordar resultados desenvolvidos por Paques em [15], que serão de grande importância para justificar a definição de álgebra separável.

Nas seções seguintes, abordaremos extensões galoisianas comutativas – sua definição, o Teorema Fundamental da Teoria de Galois, homomorfismos de extensões galoisianas comutativas e por fim, localização e bases normais. Estes resultados foram desenvolvidos por Chase, Harrison, e Rosenberg em [7].

2.1 Álgebras Separáveis

Normalidade e separabilidade são as condições que garantem que a correspondência entre subcorpos intermediários e subgrupos do grupo de Galois $\mathrm{Gal}\,(L\,|_K)$ seja biunívoca. A normalidade se refere a presença de todas as raízes do polinômio minimal de um elemento em L, e a separabilidade da multiplicidade das raízes de polinômios irredutíveis. A partir destas informações, ambas as propriedades se referem às raízes e como os automorfismos do grupo de Galois permutam estas raízes.

Iremos tratar agora de extensões algébricas simples. Os seguintes resultados nos auxiliam a, em determinado sentido, afastar a separabilidade da extensão da separabilidade de polinômios. Em particular, o Teorema do Elemento Primitivo tem papel essencial para a caracterização de extensões separáveis.

Os resultados a seguir buscam caracterizar as extensões de corpos separáveis, para então tratarmos de álgebras sobre anéis.

Devido ao isomorfismo

$$K(\alpha)|_K \simeq \left.\frac{K[x]}{\langle m_\alpha\rangle}\right|_K,$$

apresentado no Teorema 1.1.3, onde m_α é o polinômio minimal de α sobre K, e ao Teorema do Elemento Primitivo (Teorema 1.1.7), a caracterização de extensões algébricas, finitas e separáveis pode ser realizada a partir do polinômio minimal, que satisfaz as hipóteses da proposição a seguir.

Proposição 2.1.1. *Sejam K um corpo e $f \in K[x]$ um polinômio mônico irredutível. Então f é separável sobre K se e somente se $\dfrac{K[x]}{\langle f\rangle} \otimes_K L$ não tem elementos nilpotentes não nulos, para qualquer extensão L de K.*

Demonstração. Suponha que $\dfrac{K[x]}{\langle f\rangle} \otimes_K L$ não possui elementos nilpotentes não nulos, para toda extensão L de K. Seja Σ o corpo de decomposição para f. Então Σ contém todas as raízes de f, digamos $\alpha_1, \ldots, \alpha_r$, e podemos

escrever

$$f = (x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r} \in \Sigma[x],$$

com $n_1, \ldots, n_r \geq 1$, e

$$\frac{K[x]}{\langle f \rangle} \otimes_K \Sigma \simeq \frac{\Sigma[x]}{\langle f \rangle} \simeq \frac{\Sigma[x]}{\langle x - \alpha_1 \rangle^{n_1}} \oplus \cdots \oplus \frac{\Sigma[x]}{\langle x - \alpha_r \rangle^{n_r}}.$$

Como $\dfrac{K[x]}{\langle f \rangle} \otimes_K \Sigma$ não tem elementos nilpotentes não nulos, temos que $n_i = 1$ para todo $i \in \{1, \ldots, r\}$, e portanto f é separável.

Por outro lado, seja $f \in K[x]$ polinômio minimal de $\alpha \in L$ tal que $L \simeq K(\alpha)$ e sejam $p_1, p_2, \ldots, p_r \in L[x]$ os r fatores irredutíveis distintos de f, isto é, temos

$$f = \prod_{i=1}^{r} p_i^{n_i}$$

com inteiros $n_i \geq 1$. Assim, temos

$$\frac{K[x]}{\langle f \rangle} \otimes_K L \simeq \frac{L[x]}{\langle f \rangle} \simeq \frac{L[x]}{\langle p_1 \rangle^{n_1}} \oplus \cdots \oplus \frac{L[x]}{\langle f_r \rangle^{n_r}}.$$

Se f é separável, temos $n_i = 1$ para todo $i \in \{1, \ldots, r\}$; como os polinômios p_i são irredutíveis, temos que $\dfrac{L[x]}{\langle p_i \rangle}$ é corpo para todo i. Desta forma, segue que

$$\frac{K[x]}{\langle f \rangle} \otimes_K L \simeq \frac{L[x]}{\langle p_1 \rangle} \oplus \cdots \oplus \frac{L[x]}{\langle p_r \rangle}$$

não possui elementos nilpotentes não nulos. □

Teorema 2.1.2. *Seja $L\ |_K$ uma extensão finita de corpos. Então $L\ |_K$ é separável se e somente se $L \simeq \dfrac{K[x]}{\langle f \rangle}$ para algum polinômio mônico, irredutível e separável f.*

Demonstração. Como $L\ |_K$ é finita, então é finitamente gerada e algébrica. Assim, se L é separável sobre K, $L = K(\alpha)$ pelo Teorema 1.1.7. Desta forma, o polinômio minimal m_α satisfaz as condições do enunciado e temos $L \simeq \dfrac{K[x]}{\langle m_\alpha \rangle}$. Para a recíproca, suponha $L \simeq \dfrac{K[x]}{\langle f \rangle}$. Então f é o polinômio minimal de algum $\alpha \in L$ e $L \simeq K(\alpha)$ e portanto, L é separável. □

Como consequência da Proposição 2.1.1 e do Teorema 2.1.2, temos o seguinte corolário:

Corolário 2.1.3. *Seja L uma extensão finita de um corpo K. Então, L é uma extensão separável de K se e somente se $L \otimes_K F$ não tem elementos nilpotentes não nulos, para qualquer extensão de corpos F de K.*

Definição 2.1.4. Seja R um anel comutativo. Uma R-álgebra é um anel S que também é um R-módulo tal que as operações de multiplicação de S e a ação de R sobre S são compatíveis, isto é,

$$r(st) = (rs)t = s(rt),$$

para quaisquer $s, t \in S$, $r \in R$.

A partir de agora, iremos denotar por A uma K-álgebra comutativa com elemento identidade e de dimensão finita sobre K (como K-espaço vetorial). Diremos que A é separável sobre K, se $A \otimes_K L$ não tem elementos nilpotentes não nulos, para qualquer extensão L de K.

O teorema de Wedderburn a seguir nos auxilia a caracterizar álgebras separáveis sobre corpos, a partir dos elementos nilpotentes não nulos. Esta é uma versão simplificada para o caso comutativo. Na página 69, está enunciada a versão geral do Teorema.

Teorema 2.1.5 (Wedderburn - Caso Comutativo)**.** *Seja A uma K-álgebra comutativa de dimensão finita com unidade. Então A é separável sobre o corpo K se e somente se $A \simeq F_1 \oplus \cdots \oplus F_n$, onde F_i são corpos que são extensões finitas e separáveis de K.*

Demonstração. Suponha $A \simeq F_1 \oplus \cdots \oplus F_r$. Então $A \otimes_K L \simeq (F_1 \otimes_K L) \oplus \cdots \oplus (F_r \otimes_K L)$. Como cada somando não tem elementos nilpotentes não nulos, segue que $A \otimes_K L$ também não os possui. Portanto, A é separável sobre K.

Suponhamos A separável sobre K; então $A \otimes_K K \simeq A$ não tem elementos nilpotentes não nulos.

Pelos Lemas 1.5,...,1.9 de [15], temos que $A = F_1 \oplus \cdots \oplus F_n$, onde cada F_i é uma extensão finita de K. Se algum F_i não é separável sobre K, então existe uma extensão L de K tal que $F_i \otimes_K L$ tem pelo menos um elemento nilpotente $x \neq 0$. Então, $(0, \ldots, x, \ldots, 0) \in F_1 \otimes_K L \oplus \cdots \oplus F_n \otimes_K L = A \otimes_K L$ é um elemento nilpotente não nulo, o que contradiz a hipótese de A ser separável. Portanto, todos os F_i são separáveis sobre K. □

Seja A uma K-álgebra, não necessariamente comutativa. Definimos a álgebra oposta de A, denotada por A^o como o anel definido sobre o próprio conjunto A, com multiplicação dada por $x * y = yx$, para quaisquer $x, y \in A$. Podemos ver que A^o é de fato um anel. A multiplicação é associativa:

$$(x * y) * z = yx * z = zyx = x * (zy) = x * (y * z).$$

Além disso, distribui sobre a adição:

$$x * (y + z) = (y + z)x = yx + zx = x * y + x * z$$

De forma semelhante, decorrem as propriedades de K-módulo de A^o. Se A é uma álgebra comutativa, então $A = A^o$.

Consideremos o produto tensorial $A^e = A \otimes_K A^o$, chamado álgebra envolvente de A. Como A e A^o são R-álgebras, temos que A^e também é uma R-álgebra, com multiplicação $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 * b_2 = a_1 a_2 \otimes b_2 b_1$, para quaisquer $a_1, a_2 \in A, b_1, b_2 \in A^o$. A álgebra A possui uma estrutura de A^e-módulo à esquerda, com a ação definida por $(a \otimes c_o)b = abc_o$.

Seja $\mu : A^e \to A$ definida por $x \otimes y = xy$, aplicação chamada de contração. O teorema a seguir nos auxiliará a estender a definição de separabilidade de uma álgebra A. Sua demonstração será omitida.

Teorema 2.1.6. *Seja A uma K-álgebra de dimensão finita com elemento identidade 1. Então A é separável sobre K se e somente se a sequência exata de A^e-módulos (à esquerda)*

$$0 \to \ker \mu \to A^e \xrightarrow{\mu} A \to 0$$

cinde.

Seja agora R um anel comutativo com unidade e S uma R-álgebra.

Teorema 2.1.7. *São equivalentes as seguintes afirmações:*

1. *S é um S^e-módulo projetivo;*

2. *A sequência exata de S^e-módulos*

$$0 \to \ker \mu \to S^e \xrightarrow{\mu} S \to 0$$

   onde $\mu(x \otimes y) = xy$, cinde;

3. *Existe $e \in S^e$ tal que $\mu(e) = 1$ e $\ker \mu\, e = 0$. O elemento e é chamado* idempotente de separabilidade.

Demonstração. A equivalência entre as afirmações (1) e (2) é consequência do Lema 1.2.6. Assim, veremos a equivalência entre as afirmações (2) e (3).

(2 $\Rightarrow$ 3) Seja $\nu : S \to S^e$ um homomorfismo de S^e-módulos tal que $\mu \circ \nu = \mathrm{id}_S$. Seja $e = \nu(1)$. Então, $\mu(e) = 1$; além disso, para qualquer $s \in S$, $(s \otimes 1)e = (s \otimes 1)\nu(1) = \nu(s \otimes 1 \cdot 1) = \nu(s \cdot 1 \cdot 1) = \nu(1 \cdot 1 \cdot s) = \nu(1 \otimes s \cdot 1) = 1 \otimes s \cdot \nu(1) = 1 \otimes s \cdot e$, logo $(s \otimes 1 - 1 \otimes s)e = 0$. Portanto $\ker \mu e = 0$.

(3 $\Rightarrow$ 2) Seja $e \in S^e$ tal que $\mu(e) = 1$ e $\ker \mu e = 0$. Definimos $\nu : S \to S^e$ por $\nu(s) = (s \otimes 1)e = (1 \otimes s)e$. Temos $\nu(s+r) = (s+r \otimes 1)e = (s \otimes 1)e + (r \otimes 1)e = \nu(s) + \nu(r)$ e $\mu \circ \nu(s) = \mu(s \otimes 1 \cdot e) = \mu(s \otimes 1)\mu(e) = s \Rightarrow \mu \circ \nu = \mathrm{id}_S$. Além disso, $\nu(s \otimes r \cdot t) = \nu(str) = (str \otimes 1)e = (st \otimes 1)(r \otimes 1)e = (st \otimes 1)(1 \otimes r)e = (s \otimes r)(t \otimes 1)e = (s \otimes r)\nu(t)$. Portanto, ν é um homomorfismo de S^e-módulos que $\mu \circ \nu = \mathrm{id}_S$. □

Note que os elementos da forma $(s \otimes 1 - 1 \otimes s)$ pertencem a $\ker \mu$. Além disso, se $\sum s_i \otimes t_i \in \ker \mu$, então $\sum s_i t_i = 0$. Assim, temos que $\sum s_i t_i \otimes 1 = 0$ e, portanto, $\sum s_i \otimes t_i = \sum s_i \otimes t_i - \sum s_i t_i \otimes 1 = \sum (s_i \otimes 1)(1 \otimes t_i - t_i \otimes 1)$. Logo, o $\ker \mu$ é um ideal de S^e gerado pelos elementos da forma $(s \otimes 1 - 1 \otimes s)$.

Encerramos esta seção com a definição de uma álgebra separável, motivada pelo Teorema 2.1.6, além de dois exemplos.

Definição 2.1.8. Uma R-álgebra S é dita separável se S é um S^e-módulo projetivo.

Exemplo. Tomemos $R = \mathbb{Z}$ e $S = \mathbb{Z}_n$ o anel dos inteiros módulo n. Se $\mu\left(\sum \overline{m_i} \otimes \overline{n_i}\right) = \overline{0}$, temos $\sum \overline{m_i n_i} = 0$. Logo $\sum \overline{m_i} \otimes \overline{n_i} = \sum \overline{m_i} \otimes n_i\overline{1} = \sum \overline{m_i n_i} \otimes 1 = 0$. Assim, temos que μ é injetivo. Como μ é claramente sobrejetivo, segue que $\mathbb{Z}_n$ é uma $\mathbb{Z}$-álgebra separável.

Note que se S é um anel comutativo, o idempotente de separabilidade $e \in S^e$ é único: sejam $e_1, e_2 \in S^e$ tais que $\mu(e_i) = 1$ e $\ker\mu\ e_i = 0$, para $i = 1, 2$. Então $0 = \mu(e_1) - \mu(e_2) = \mu(e_1 - e_2)$ e portanto $e_1 - e_2 \in \ker\mu$. Logo, $(e_1 - e_2)e_i = 0$, de onde segue que $e_1 - e_2e_1 = e_2 - e_1e_2 = 0 \Rightarrow e_1 = e_2$.

Desta forma, $e = 1 \otimes 1$ é o único idempotente de separabilidade de $(Z_n)^e$.

Para o próximo exemplo, relembramos que S^e tem multiplicação definida por

$$(s_1 \otimes s_2)(t_1 \otimes t_2) = s_1t_1 \otimes t_2s_2,$$

para quaisquer $s_1, s_2 \in S$, $t_1, t_2 \in S^o$.

Exemplo. Sejam $R = \mathbb{R}$ o corpo dos números reais e $S = \mathbb{H}$ a $\mathbb{R}$-álgebra dos quatérnios. Então $\mathbb{H}$ é uma $\mathbb{R}$-álgebra separável. De fato, tomemos

$$e = \frac{1}{4}\left(1 \otimes 1 - i \otimes i - j \otimes j - k \otimes k\right) \in \mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^o.$$

Primeiramente, temos

$$\mu(e) = \frac{1}{4}\left[(1)(1) - (i)(i) - (j)(j) - (k)(k)\right] = 1.$$

Como $\ker\mu$ é gerado pelos elementos da forma $s \otimes 1 - 1 \otimes s$, temos

$$4(s\otimes 1 - 1\otimes s)e = (s\otimes 1 - si\otimes i - sj\otimes j - sk\otimes k) - (1\otimes s - i\otimes is - j\otimes js - k\otimes ks).$$

Por questão de organização, vamos escrever o segundo termo desta equação como

$$(s \otimes 1 - 1 \otimes s) + (i \otimes is - si \otimes i) + (j \otimes js - sj \otimes j) + (k \otimes ks - sk \otimes k).$$

Expandindo $s \in \mathbb{H}$ como $a + bi + cj + dk$ e efetuando os produtos si, is, sj, js, sk, ks, temos

$$\begin{aligned} si &= -b + ai + dj - ck & \qquad is &= -b + ai - dj + ck \\ sj &= -c - di + aj + bk & \qquad js &= -c + di + aj - bk \\ sk &= -d + ci - bj + ak & \qquad ks &= -d - ci + bj + ak \end{aligned}$$

Assim, expandindo cada parcela da soma separadamente, segue

$$\begin{aligned} s \otimes 1 - 1 \otimes s &= b(i \otimes 1 - 1 \otimes i) + c(j \otimes 1 - 1 \otimes j) + d(k \otimes 1 - 1 \otimes k) \\ i \otimes is - si \otimes i &= b(1 \otimes i - i \otimes 1) + c(i \otimes k + k \otimes i) - d(i \otimes j + j \otimes i) \\ j \otimes js - sj \otimes j &= -b(j \otimes k + k \otimes j) + c(1 \otimes j - j \otimes 1) + d(j \otimes i + i \otimes j) \\ k \otimes ks - sk \otimes k &= b(j \otimes k + k \otimes j) - c(i \otimes k + k \otimes i) + d(1 \otimes k + k \otimes 1) \end{aligned}$$

Observando as expressões acima, podemos ver que os termos se anulam e portanto, $e = \dfrac{1}{4}[1 \otimes 1 - i \otimes i - j \otimes j - k \otimes k]$ é idempotente de separabilidade para $\mathbb{H}$ enquanto $\mathbb{R}$-álgebra.

Note que este elemento é de fato idempotente:

$$\begin{aligned} e^2 =& \frac{1}{16}\left(1 \otimes 1 - i \otimes i - j \otimes j - k \otimes k\right)^2 \\ =& \frac{1}{16}\left[(1 \otimes 1 - i \otimes i - j \otimes j - k \otimes k)\right. \\ & - (i \otimes i - (-1) \otimes (-1) - k \otimes (-k) - (-j) \otimes j) \\ & - (j \otimes j - (-k) \otimes k - (-1) \otimes (-1) - i \otimes (-1)) \\ & \left. - \ (k \otimes k - j \otimes (-j) - (-i) \otimes i - (-1) \otimes (-1))\right] \\ =& \frac{4}{16}\left[1 \otimes 1 - i \otimes i - j \otimes j - k \otimes k\right] = e. \end{aligned}$$

Porém, se um elemento $e \in S^e$ satisfaz $\mu(e) = 1$ e $\ker \mu \ e = 0$, e é necessariamente idempotente, pois $e^2 - e = (e - 1 \otimes 1)e \in \ker \mu \ e = 0$, logo $e^2 = e$. Assim, a verificação de $e^2 = e$ não se faz necessária, nem a adição desta hipótese no Teorema 2.1.7.

Exemplo. Seja R um anel comutativo com unidade e $S = M_n(R)$ a R-álgebra de matrizes de ordem n com entradas em R. Denotemos por e_{ij} as matrizes com todas as entradas nulas, exceto a entrada i, j, que tem valor 1.

Para cada $1 \leq j \leq n$, temos que $e = \sum_{i=1}^{n} e_{ij} \otimes e_{ji}$ satisfaz

$$\mu(e) = \sum_{i=1}^{n} e_{ij}e_{ji} = \sum_{i=1}^{n} e_{ii} = I_n = 1,$$

onde I_n denota a matriz identidade de ordem n, isto é, a unidade de $M_n(R)$. Além disso, como $\ker \mu$ é gerado por elementos da forma $s \otimes 1 - 1 \otimes s$, seja $s \in M_n(R)$ uma matriz de ordem n. Então

$$(s \otimes 1 - 1 \otimes s)e = \sum_{i=1}^{n} se_{ij} \otimes e_{ji} - e_{ij} \otimes e_{ji}s$$

e, escrevendo

$$s = \sum_{k=1}^{n} \sum_{l=1}^{n} s_{kl}e_{kl},$$

onde $s_{kl} \in R$, para todos $1 \leq k, l \leq n$, temos então

$$se_{ij} = \sum_{k=1}^{n} s_{ki}e_{kj} \quad \text{e} \quad e_{ji}s = \sum_{l=1}^{n} s_{il}e_{jl}.$$

Realizando a substituição, obtemos

$$\begin{aligned}
(s \otimes 1 - 1 \otimes s)e &= \sum_{i=1}^{n} \sum_{k=1}^{n} s_{ki}e_{kj} \otimes e_{ji} - \sum_{i=1}^{n} \sum_{l=1}^{n} s_{il}e_{ij} \otimes e_{jl} \\
&= \sum_{i=1}^{n} \sum_{k=1}^{n} s_{ki}e_{kj} \otimes e_{ji} - \sum_{l=1}^{n} \sum_{i=1}^{n} s_{il}e_{ij} \otimes e_{jl} \\
&= \sum_{i=1}^{n} \sum_{k=1}^{n} s_{ki}e_{kj} \otimes e_{ji} - \sum_{i=1}^{n} \sum_{k=1}^{n} s_{ki}e_{kj} \otimes e_{ji} = 0.
\end{aligned}$$

Portanto e é idempotente de separabilidade para $M_n(R)$ sobre R, e $M_n(R)$ é uma R-álgebra separável.

2.2 Extensões Galoisianas

Deixando as extensões de corpos, a partir da definição de extensão separável, podemos dar início ao estudo das extensões galoisianas de anéis comutativos. O estudo se torna mais rico ao abordarmos extensões que não contenham idempotentes além de 0 e 1, mas os resultados serão desenvolvidos sobre extensões quaisquer. Para isso, precisamos dos resultados a seguir. Os produtos tensoriais nas seções a seguir serão denotados apenas por $\otimes$, por simplicidade, e serão sobre R exceto onde explicitado.

Definição 2.2.1. Sejam $f, g : S \to T$ homomorfismos de anéis comutativos. Dizemos que f e g são fortemente distintos se, para qualquer idempotente não nulo $e \in T$, existe $s \in S$ tal que $f(s) \cdot e \neq g(s) \cdot e$.

Lema 2.2.2. *Sejam S uma R-álgebra comutativa separável, e $f : S \to R$ um homomorfismo de R-álgebras. Então existe um único idempotente $e \in S$ tal que $f(e) = 1$ e se $= f(s)e$ para qualquer $s \in S$. Além disso, se $f_1, \ldots, f_n : S \to R$ são homomorfismos de R-álgebras dois a dois fortemente distintos, então os idempotentes correspondentes $e_1, \ldots, e_n$ são dois a dois ortogonais, e $f_i(e_j) = \delta_{i,j}$.*

Demonstração. Como S é separável, pelo Teorema 2.1.7, existe um homomorfismo de S^e-módulos $g : S \to S^e$ tal que $\mu \circ g = \mathrm{id}_S$.

$$\begin{array}{ccccc} & & S & & \\ & \overset{g}{\swarrow} & \downarrow{\scriptstyle \mathrm{id}_S} & & \\ S \otimes S & \xrightarrow[\mu]{} & S & \longrightarrow & 0 \end{array}$$

Seja então $g(1) = \sum_{i=1}^{m} x_i \otimes y_i \in S \otimes S$. Assim, tomando μ, temos $\sum_{i=1}^{m} x_i y_i = 1$. Como definido na página 29, S é um S^e-módulo com ação definida por $(s \otimes t)a = sat$. Assim, segue

$$\begin{array}{rrl} & g(s) = g(s \cdot 1 \cdot 1) & = g(1 \cdot 1 \cdot s) \\ \Rightarrow & g\left((s \otimes 1) \cdot 1\right) & = g\left(1 \cdot (1 \otimes s)\right) \\ \Rightarrow & (s \otimes 1) \cdot g(1) & = (1 \otimes s) \cdot g(1) \\ \Rightarrow & (s \otimes 1) \cdot \sum_{i=1}^{m} x_i \otimes y_i & = (1 \otimes s) \cdot \sum_{i=1}^{m} x_i \otimes y_i \\ \Rightarrow & \sum_{i=1}^{m} sx_i \otimes y_i & = \sum_{i=1}^{m} x_i \otimes sy_i, \end{array}$$

para qualquer $s \in S$.

Tomando $e = \sum_{i=1}^{m} f(x_i)y_i$, temos:

$$\begin{array}{rll} f(e) & = f\left(\sum_{i=1}^{m} f(x_i)y_i\right) & = \sum_{i=1}^{m} f\left(f(x_i)y_i\right) \\ & = \sum_{i=1}^{m} f(x_i)f(y_i) & = \sum_{i=1}^{m} f(x_i y_i) \\ & = f\left(\sum_{i=1}^{m} x_i y_i\right) & = f(1) = 1 \end{array}$$

Aplicando $f \otimes 1$ na igualdade

$$\sum_{i=1}^{m} sx_i \otimes y_i = \sum_{i=1}^{m} x_i \otimes sy_i$$

obtemos o seguinte:

$$\begin{array}{rrl} & \sum_{i=1}^{m} f(sx_i) \otimes y_i & = \sum_{i=1}^{m} f(x_i) \otimes sy_i \\ \Rightarrow & \sum_{i=1}^{m} f(s)f(x_i) \otimes y_i & = \sum_{i=1}^{m} f(x_i) \otimes sy_i \end{array}$$

Aplicando μ, segue:

$$\begin{array}{rrl} & \sum_{i=1}^{m} f(s)f(x_i)y_i & = \sum_{i=1}^{m} f(x_i)sy_i \\ \Rightarrow & f(s)\sum_{i=1}^{m} f(x_i)y_i & = s\sum_{i=1}^{m} f(x_i)y_i \\ \Rightarrow & f(s)e & = se, \forall s \in S \end{array}$$

Em particular, tomando $s = e$, temos $e = e^2$, isto é, $e \in S$ é realmente um idempotente. Tomando e' outro idempotente de S satisfazendo as mesmas condições, então $e' = 1 \cdot e' = f(e)e' = e \cdot e' = f(e')e = e$.

Para a segunda afirmação, basta mostrarmos que $f_i(e_j) = \delta_{i,j}$ e que os idempotentes e_i são ortogonais, isto é, $e_i e_j = \delta_{i,j} e_i$. Note que $(f_i(e_j))^2 = f_i(e_j)f_i(e_j) = f_i(e_j^2) = f_i(e_j)$ é um idempotente de R, e que $f_i(s)f_i(e_j) = f_i(se_j) = f_i(f_j(s)e_j) = f_j(s)f_i(e_j)$. Como f_i e f_j são fortemente distintos

para $i \neq j$, temos que a igualdade se verifica apenas com $f_i(e_j) = 0$ se $i \neq j$, e portanto temos que $f_i(e_j) = \delta_{i,j}$. Finalmente, $e_i e_j = f_j(e_i)e_j = \delta_{i,j}e_j$, logo $e_1, \ldots, e_n$ são realmente ortogonais dois a dois. □

Ao longo do texto, estaremos focados na seguinte situação: sejam S um anel comutativo, G um grupo finito de automorfismos de S e $R = S^G$ o subanel dos elementos que permanecem fixos pela ação de G.

Para o desenvolvimento do capítulo, vamos definir duas álgebras auxiliares. A primeira, denotada por $D = S \rtimes G$, é o produto cruzado destes conjuntos. D é um S-módulo livre com geradores δ_σ, com $\sigma \in G$, e também uma R-álgebra, com a multiplicação definida por

$$s\delta_\sigma t\delta_\tau = s\sigma(t)\delta_{\sigma\tau}$$

para os geradores e estendida linearmente para a álgebra. A identidade de D é $1\delta_{\mathrm{id}_G}$ e será denotada por 1. Além disso, a aplicação $j : D \to \mathrm{Hom}_R(S, S)$ dada por $j(s\delta_\sigma) = s\sigma$ é um homomorfismo de R-álgebras. De fato:

- $\begin{aligned} j(1)(x) &= j(1\delta_{\mathrm{id}_S})(x) \\ &= 1\,\mathrm{id}_S(x) = x \end{aligned}$

- $\begin{aligned} j(s\delta_\sigma + t\delta_\tau)(x) &= (s\sigma + t\tau)(x) \\ &= s\sigma(x) + t\tau(x) \\ &= j(s\delta_\sigma)(x) + j(t\delta_\tau)(x) \end{aligned}$

- $\begin{aligned} j(rs\delta_\sigma) &= rs\sigma(x) \\ &= rj(s\delta_\sigma)(x) \end{aligned}$

- $\begin{aligned} j(s\delta_\sigma t\delta_\tau)(x) &= j(s\sigma(t)\delta_{\sigma\tau})(x) \\ &= s\sigma(t)\sigma(\tau(x)) \\ &= s\sigma(t\tau(x)) \\ &= j(s\delta(\sigma))(t\tau(x)) = j(s\delta_\sigma)j(t\delta_\tau)(x) \end{aligned}$

Além disso, também é um homomorfismo de S-módulos.

Seja E a álgebra de todas as funções de G em S, com a adição e multiplicação ponto a ponto. Se v_σ é a função definida por $v_\sigma(\tau) = \delta_{\sigma,\tau}$, então

$E = \bigoplus_{\sigma \in G} Sv_\sigma$. Podemos escrever qualquer função $f \in E$ como

$$f(\tau) = \sum_{\sigma \in G} f(\sigma) v_\sigma(\tau)$$

para qualquer $\tau \in G$. Além disso, como $v_\sigma(\tau) = \delta_{\sigma,\tau}$, temos que cada v_σ é idempotente e os elementos do conjunto $\{v_\sigma\}_{\sigma \in G}$ são ortogonais dois a dois e sua soma é 1. De fato,

$$(v_\sigma \cdot v_\tau)(x) = v_\sigma(x) v_\tau(x) = \delta_{\sigma,x}\delta_{\tau,x} = \begin{cases} 0 & \text{se } \sigma \neq \tau \\ v_\sigma(x) & \text{se } \sigma = \tau \end{cases}$$

Tomando $S \otimes S$ como uma S-álgebra no primeiro fator, temos um homomorfismo de S-álgebras $h : S \otimes S \to E$ definido por $h(s \otimes t)(\sigma) = s\sigma(t)$. Com efeito,

- $h(1 \otimes 1)(\sigma) \ = 1\sigma(1) = 1$
- $\begin{aligned} h(s \otimes t + p \otimes q)(\sigma) \ &= s\sigma(t) + p\sigma(q) \\ &= h(s \otimes t)(\sigma) + h(p \otimes q)(\sigma) \end{aligned}$
- $\begin{aligned} h(sr \otimes t)(\sigma) \ &= h((sr) \otimes t)(\sigma) \\ &= sr\sigma(t) \\ &= sh(r \otimes t)(\sigma) \end{aligned}$
- $\begin{aligned} h(s \otimes r \cdot t \otimes u)(\sigma) \ &= h(st \otimes ru)(\sigma) \\ &= st\sigma(ru) \\ &= st\sigma(r)\sigma(u) \\ &= s\sigma(r)t\sigma(u) = h(s \otimes r)(\sigma) \cdot h(t \otimes u)(\sigma) \end{aligned}$

O objetivo desta seção é demonstrar o teorema a seguir. Para isso, vamos definir o que é um G-módulo:

Definição 2.2.3. Seja G um grupo. Um G-módulo é um grupo abeliano A com uma ação de $\mathbb{Z}G$ sobre A, isto é, A é um $\mathbb{Z}G$-módulo.

Teorema 2.2.4. *Sejam S um anel comutativo, G um grupo finito de automorfismos de S e $R = S^G$. Então, são equivalentes:*

1. *S é uma R-álgebra separável, e os elementos de G são dois a dois fortemente distintos;*

2. *Existem elementos $x_1, \ldots, x_n; y_1, \ldots, y_n$ de S tais que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$ para todo $\sigma \in G$. Estes elementos são chamados* sistema de coordenadas de Galois*;*

3. *S é um R-módulo projetivo finitamente gerado e $j : D \to Hom_R(S, S)$ é um isomorfismo;*

4. *Seja M um D-módulo à esquerda, que pode ser visto como um G-módulo com $\sigma(m) = \delta_\sigma(m)$. Então a aplicação $\omega : S \otimes M^G \to M$ definida por $\omega(s \otimes m) = sm$ é um isomorfismo de S-módulos;*

5. *$h : S \otimes S \to E$ é um isomorfismo de S-álgebras;*

6. *Dado $\sigma \neq 1$ em G e um ideal maximal I de S, existe $s = s(I, \sigma)$ tal que $s - \sigma(s) \notin I$.*

Demonstração. $(1 \Rightarrow 2)$ Seja $e = \sum_{i=1}^{m} x_i \otimes y_i \in S \otimes S$ o idempotente de separabilidade de S sobre R, isto é, $\mu(e) = 1$ e $(1 \otimes a - a \otimes 1)\, e = 0$, para qualquer $a \in S$. Seja $e_\sigma = \mu\left((1 \otimes \sigma)e\right)$, para qualquer $\sigma \in G$. Como $R = S^G$, temos que σ é um R-automorfismo de S e, portanto, $1 \otimes \sigma$ é um S-automorfismo de $S \otimes S$. Além disso, como S é comutativo, μ é um homomorfismo de anéis. Assim, para qualquer $\sigma \in G$, temos:

$$\begin{aligned} e_\sigma^2 &= \mu\left((1 \otimes \sigma)(e)\right) \cdot \mu\left((1 \otimes \sigma)(e)\right) \\ &= \mu\left((1 \otimes \sigma)(e) \cdot (1 \otimes \sigma)(e)\right) \\ &= \mu\left((1 \otimes \sigma)(e^2)\right) \\ &= \mu\left((1 \otimes \sigma)(e)\right) \\ &= e_\sigma. \end{aligned}$$

Ou seja, e_σ é um idempotente de S. Por outro lado, para qualquer $x \in S$, temos:

$$\begin{aligned}
xe_\sigma &= x\mu\left((1 \otimes \sigma)(e)\right) \\
&= x \otimes 1 \cdot \mu\left((1 \otimes \sigma)(e)\right) \\
&= \mu\left((x \otimes 1) \cdot (1 \otimes \sigma)(e)\right) \\
&= \mu\left((1 \otimes \sigma)(x \otimes 1) \cdot (1 \otimes \sigma)(e)\right) \\
&= \mu\left((1 \otimes \sigma)(x \otimes 1 \cdot e)\right) \\
&= \mu\left((1 \otimes \sigma)(1 \otimes x \cdot e)\right) \\
&= \mu\left((1 \otimes \sigma)(1 \otimes x) \cdot (1 \otimes \sigma)(e)\right) \\
&= \mu\left((1 \otimes \sigma(x)) \cdot (1 \otimes \sigma)(e)\right) \\
&= (1 \otimes \sigma(x)) \cdot \mu\left((1 \otimes \sigma)(e)\right) \\
&= (1 \otimes \sigma(x)) \cdot e_\sigma \\
&= 1 \cdot e_\sigma \cdot \sigma(x) \\
&= \sigma(x)e_\sigma.
\end{aligned}$$

Assim, $xe_\sigma = \sigma(x)e_\sigma$. Como $\sigma \in G$ são R-automorfismos de S fortemente distintos, temos que $e_\sigma = 0$ ou $\sigma = 1$. Assim, para qualquer $\sigma \in G$, temos $\delta_{1,\sigma} = e_\sigma = \sum_{i=1}^{m} (x_i\sigma(y_i))$.

(2 $\Rightarrow$ 3) Tomemos os elementos $x_i, y_i \in S$, $i \in \{1, \ldots, m\}$ tais que $\sum_{i=1}^{m} x_i\sigma(y_i) = \delta_{1,\sigma}$, para qualquer $\sigma \in G$. Defina $f_j \in \mathrm{Hom}_R(S, R)$ por $f_j(x) = \sum_{\sigma \in G} \sigma(xy_i)$, para todo $x \in S$. De fato, f_j é um homomorfismo:

$$\begin{aligned}
f_j(a + rb) &= \sum_{\sigma \in G} \sigma((a + rb)y_j) \\
&= \sum_{\sigma \in G} \sigma(ay_j + rby_j) \\
&= \sum_{\sigma \in G} \sigma(ay_j) + \sigma(rby_j) \\
&= \sum_{\sigma \in G} \sigma(ay_j) + \sum_{\sigma \in G} r\sigma(by_j) = f_j(a) + rf_j(b).
\end{aligned}$$

Assim, para qualquer $x \in S$, temos:

$$\begin{aligned}\sum_{j=1}^{m} f_j(x)x_j &= \sum_{j=1}^{m}\sum_{\sigma\in G}\sigma(xy_j)x_j \\ &= \sum_{\sigma\in G}\sigma(x)\sum_{j=1}^{m}\sigma(y_j)x_j \\ &= \sum_{\sigma\in G}\sigma(x)\delta_{1,\sigma} \\ &= x,\end{aligned}$$

o que mostra que S é um R-módulo projetivo finitamente gerado pelos elementos x_i, $i \in \{1, \ldots, n\}$. Basta mostrarmos que $j : D \to \mathrm{Hom}_R(S, S)$ é um isomorfismo.

Para mostrarmos que j é sobrejetivo, dado um homomorfismo p em $\mathrm{Hom}_R(S, S)$, seja

$$q = \sum_{\sigma\in G}\sum_{i=1}^{m} h(x_i)\sigma(y_i)\delta_\sigma$$

Dessa forma,

$$\begin{aligned}j(q)(x) &= \sum_{\sigma\in G}\sum_{i=1}^{m} p(x_i)\sigma(y_i)\sigma(x) = \sum_{i=1}^{m} p(x_i)\sum_{\sigma\in G}\sigma(xy_i) \\ &= p\left(\sum_{i=1}^{m} x_i\sum_{\sigma\in G}\sigma(xy_i)\right) = p\left(\sum_{i=1}^{m}\left(\sum_{\sigma\in G} x_i\sigma(y_i)\right)\sigma(x)\right) \\ &= p\left(\sum_{i=1}^{m}\delta_{\sigma,1}\sigma(x)\right) = p(x).\end{aligned}$$

Ou seja, existe $q \in D$ tal que $j(q)(x) = p(x)$, para qualquer $p \in \mathrm{Hom}_R(S, S)$.

Para mostrarmos a injetividade de j, tomemos $w = \sum_{\sigma\in G} a_\sigma\delta_\sigma \in D$ tal que $j(w) = 0$. Então, $j(w)(x) = 0$, para qualquer $x \in S$. Portanto,

$$
\begin{aligned}
0 &= \sum_{\tau\in G}\sum_{i=1}^{n} j(w)(x_i)\cdot\tau(y_i)\delta_\tau = \sum_{\tau\in G}\sum_{i=1}^{n}\sum_{\sigma\in G} a_\sigma\sigma(x_i)\tau(y_i)\delta_\tau \\
&= \sum_{\tau\in G}\sum_{\sigma\in G} a_\sigma\sigma\left(\sum_{i=1}^{n} x_i\sigma^{-1}\tau(y_i)\right)\delta_\tau = \sum_{\tau\in G}\sum_{\sigma\in G} a_\sigma\sigma\left(\delta_{\sigma^{-1}\tau,1}\right)\delta_\tau \\
&= \sum_{\tau\in G}\sum_{\sigma\in G} a_\sigma\delta_{\sigma^{-1}\tau,1}\delta_\tau = \sum_{\sigma\in G} a_\sigma\delta_\sigma = w.
\end{aligned}
$$

Logo, $\ker j = 0$ e j é injetiva, o que implica que j é um isomorfismo.

$(3 \Rightarrow 4)$ Como S é um R-módulo projetivo finitamente gerado, segue do Teorema 1.2.6 que existem elementos $x_i \in S$ e $\phi_i \in \mathrm{Hom}_R(S,S)$, $i \in \{1,\ldots,n\}$ tais que

$$
s = \sum_{i=1}^{n} \phi_i(s)x_i
$$

Como j é um isomorfismo, existem elementos $d_i \in D$ tais que $j(d_i) = \phi_i$. Ainda,

$$
j\left(\sum_{i=1}^{n} x_i d_i\right)(s) = \sum_{i=1}^{n} x_i\phi_i(s) = s
$$

e, sendo j um isomorfismo, segue que $\sum_{i=1}^{n} x_i d_i = \delta_1 = 1_D$.

Além disso, temos $j(\delta_\sigma d_i)(s) = \sigma(\phi_i(s)) = \phi_i(s) = j(d_i)(s)$, o que implica $d_i = \delta_\sigma d_i$, para qualquer $\sigma \in G$. Portanto, $d_i m \in M^G$, para qualquer $m \in M$.

Como $S \subset D$, podemos ver M como um S-módulo, e

$$
\begin{aligned}
d(sm_o) &= \left(\sum_{\sigma\in G} a_\sigma\delta_\sigma\right)(s\delta_1 m_o) = \sum_{\sigma\in G} a_\sigma\delta_\sigma s\delta_1 s m_o \\
&= \sum_{\sigma\in G} a_\sigma\sigma(s)\delta_\sigma m_o = \sum_{\sigma\in G} a_\sigma\sigma(s)\sigma(m_o) \\
&= \left(\sum_{\sigma\in G} a_\sigma j(\delta_\sigma)(s)\right) m_o = j(d)(s)m_o
\end{aligned}
$$

para $d \in D, s \in S$ e $m_o \in M^G$. Agora defina uma aplicação $\gamma : M \to S\otimes M^G$

como $\gamma(m) = \sum_{i=1}^{n} x_i \otimes d_i m$. Temos $\omega\gamma = \mathrm{id}_M$, pois

$$\omega\gamma(m) = \omega\left(\sum_{i=1}^{n} x_i \otimes d_i m\right) = \sum_{i=1}^{n} x_i d_i m = \left(\sum_{i=1}^{n} x_i d_i\right) m = m$$

Por outro lado, se s e m_0 estão em S e M^G, respectivamente, temos

$$\gamma\omega(s \otimes m_o) = \sum_{i=1}^{n} x_i \otimes d_i(sm_o) = \sum_{i=1}^{n} x_i \otimes \phi_i(s)m_o = \sum_{i=1}^{n} \phi_i(s)x_i \otimes m_o = m_o$$

e $\gamma\omega = \mathrm{id}_{S\otimes M^G}$. Assim, podemos concluir que ω é um isomorfismo.

(4 $\Rightarrow$ 5) Determine a ação de G em $E = F(G, S)$ como $\sigma \cdot f(x) = \sigma(f(\sigma^{-1}x))$, para $\sigma, x \in G$ e $f \in E$. Assim, temos $\sigma(sf)(x) = \sigma(sf(\sigma^{-1}x)) = \sigma(s)\sigma(f(\sigma^{-1}x)) = \sigma(s)\sigma(f)(x)$, e E pode ser visto como um D-módulo à esquerda, pela ação $s\delta_\sigma(f) = s\sigma(f)$.

Agora, E^G é o conjunto dos G-homomorfismos de G e S, e a aplicação $\theta : S \to E^G$ definida por $\theta(s)(\sigma) = \sigma(s)$ é um isomorfismo de R-módulos. Com isso, a composição $\omega(1\otimes\theta) : S\otimes S \to E$ é um isomorfismo de S-módulos, e é simplesmente h.

(5 $\Rightarrow$ 1) O E-módulo $Ev_1 = Sv_1$ é E-projetivo. Através do isomorfismo $h : S \otimes S \to E$, podemos ver E como um $S \otimes S$-módulo, e temos que Sv_1 é $S \otimes S$-projetivo. Mais ainda, a equação $h(s \otimes 1)v_1 = h(1 \otimes s)v_1$ mostra que $Sv_1 \simeq S$ como $S \otimes S$-módulos, e portanto S é $S \otimes S$-projetivo, logo é uma R-álgebra separável.

Tomando $h^{-1}(v_1) = \sum_{i=1}^{n} x_i \otimes y_i$, temos que os elementos x_i, y_i, $i \in \{1, \ldots, n\}$ satisfazem $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{\sigma,1}$.

Suponha agora e um idempotente de S tal que $\sigma(s)e = \tau(s)e$, para $\sigma \neq \tau$ em G e qualquer $s \in S$; então $e = \sum_{i=1}^{n} x_i y_i e = \sum_{i=1}^{n} x_i\tau^{-1}\sigma(y_i)e = 0$. Logo, os elementos de G são dois a dois fortemente distintos.

(2 $\Rightarrow$ 6) Suponha que exista $\sigma \neq 1$ em G e um ideal maximal $I \subset S$ tal que $\sigma(x) - x \in I$, para qualquer $x \in S$. Então, $\sum_{i=1}^{m} x_i(y_i - \sigma(y_i)) = 1 \in I$, o que implica que $I = S$, uma contradição. Assim, $\exists\, x \in S$ tal que $\sigma(x) - x \notin I$.

(6 $\Rightarrow$ 2) Seja $\sigma \neq 1$ em G e $I \subset S$ o ideal gerado por $\{x - \sigma(x) \mid x \in S\}$. Pelo argumento acima, temos que $I = S$. Portanto, existem elementos

$x_i, y_i \in S$, $i \in \{1, \ldots, n\}$ tais que $1 = \sum_{i=1}^{n} x_i(y_i - \sigma(y_i))$, ou seja, $\sum_{i=1}^{n} x_i y_i = 1 + \sum_{i=1}^{n} x_i\sigma(y_i)$. Sejam $x_{n+1} = -\sum_{i=1}^{n} x_i\sigma(y_i)$ e $y_{n+1} = 1$. Então, temos

$$\sum_{i=1}^{n+1} x_i y_i = \sum_{i=1}^{n} x_i y_i + x_{n+1}y_{n+1} = 1 + \sum_{i=1}^{n} x_i\sigma(y_i) - \sum_{i=1}^{n} x_i\sigma(y_i) = 1$$

e

$$\sum_{i=1}^{n+1} x_i\sigma(y_i) = \sum_{i=1}^{n} x_i\sigma(y_i) + x_{n+1}\sigma(y_{n+1}) = \sum_{i=1}^{n} x_i\sigma(y_i) - \sum_{i=1}^{n} x_i\sigma(y_i) = 0,$$

isto é, $\sum_{i=1}^{n+1} x_i y_i = \delta_{\sigma,1}$. Tomemos agora dois subconjuntos $H, H' \supset \{1\}$ de G, para os quais existem elementos x_i, y_i, x'_j, y'_j de S, $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$, tais que para todo $\sigma \in H$ e todo $\sigma' \in H'$, $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{1,\sigma}$ e $\sum_{j=1}^{m} x'_i\sigma'(y'_i) = \delta_{1,\sigma'}$. Então, para qualquer $\tau \in H \cup H'$, temos

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_i x'_j \tau(y_i y'_j) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} x'_j \tau(y'_j) \right) x_i\tau(y_i) = \delta_{1,\tau}$$

Como $G = \bigcup_{\sigma \neq 1}\{1, \sigma\}$, temos que a condição é satisfeita para todo $\sigma \in G$. □

A partir deste teorema, podemos definir o que é uma extensão galoisiana de anéis comutativos.

Definição 2.2.5. Se G é um grupo finito de automorfismos de um anel comutativo S e $R = S^G$, então S é dita extensão de Galois de R com grupo de Galois G se uma (e portanto, todas) das condições do Teorema 2.2.4 é satisfeita.

Observação. 1. Se S é um corpo, então a condição (6) do Teorema 2.2.4 claramente é válida, e portanto nossa definição coincide com a definição usual. Além disso, (1) e (3) mostram que uma extensão de corpos galoisiana é uma extensão finita e separável do corpo fixo, com dimensão igual a ordem do grupo de Galois.

2. O item (4) do Teorema 1.1.10 é a motivação para o isomorfismo apresentado no item (3) do Teorema 2.2.4; esta também foi a primeira definição de extensão galoisiana de anéis comutativos, apresentadas em [4] por Auslander e Goldman.

Para dar continuidade, definiremos a aplicação *traço*. Seja S uma extensão galoisiana de R com grupo de Galois G. A aplicação traço é a aplicação definida por

$$\begin{aligned} tr_G : S &\to S \\ x &\mapsto \sum_{\sigma \in G} \sigma(x) \end{aligned}$$

Observe que $tr_G(x) \in S^G = R$:

$$\begin{aligned} \sigma(tr_G(x)) = \sigma \sum_{\rho \in G} \rho(x) &= \sum_{\rho \in G} \sigma\rho(x) \\ &= \sum_{\tau \in G} \tau(x) = tr_G(x). \end{aligned}$$

Ao longo do texto, por simplicidade, usaremos a notação tr.

O próximo Lema, encontrado em [21], nos permitirá mostrar que a aplicação traço é sobrejetiva.

Lema 2.2.6. *Seja R um anel com unidade e I e J dois ideais de R, tal que I gerado por $x_1, \ldots, x_n$ e $I = IJ$. Então existe um elemento $z \in J$ tal que $(1 - z)I = 0$.*

Demonstração. Denote por $I_i = (x_i, \ldots, x_n)$. Assim, $I_1 = I$ e seja $I_{n+1} = 0$. Vamos mostrar, por indução em i, a existência de um elemento z_i em J tal que $(1 - z_i)I \subset I_i$; então z_{n+1} será o elemento z que buscamos.

Para $i = 1$, basta tomarmos $z_1 = 0$. A partir de $(1 - z_i)I \subset I_i$ e $I \subset IJ$, deduzimos $(1 - z_i)I \subset J(1 - z_i)I \subset JI_i$; em particular, temos $(1 - z_i)x_i = \sum_{j=1}^{n} z_{ij}x_j$ com $z_{ij} \in J$. Assim, $(1 - z_i - z_{ii})x_i \in I_{i+1}$, e podemos tomar $1 - z_{i+1} = (1 - z_i)(1 - z_i - z_{ii})$. □

Lema 2.2.7. *Seja S uma extensão galoisiana de R com grupo de Galois G. Então existe $c \in S$ tal que $tr(c) = \sum_{\sigma \in G} \sigma(c) = 1$, e R é um R-módulo somando direto de S.*

Demonstração. Temos que $tr \in \mathrm{Hom}_R(S, R)$. Logo $tr(S)$ é um ideal de R. De fato, dados $x, y \in S$, $r \in R$, temos:

$$tr(x + ry) = \sum_{\sigma \in G} \sigma(x + ry) = \sum_{\sigma \in G} \sigma(x) + r\sigma(y) = tr(x) + r \cdot tr(y)$$

Assim, $0 = tr(0)$, $tr(x)+tr(y) = tr(x+y) \in tr(S)$ e $r \cdot tr(x) = tr(rx) \in tr(S)$. Tomando os elementos x_i, y_i, $i \in \{1, \ldots, m\}$ como no Teorema 2.2.4, temos $\sum_{\sigma \in G} \sum_{i=1}^{m} x_i \sigma(y_i) = \sum_{\sigma \in G} \delta_{1,\sigma} = \sum_{i=1}^{m} x_i tr(y_i) = 1$. Assim, o ideal de S gerado por $tr(S)$ é igual a S. Como S é um R-módulo finitamente gerado, pelo Lema 2.2.6, obtemos r em $tr(S)$ com $(1 - r)S = 0$. Portanto, $r = 1$ e $tr(S) = R$, estabelecendo a existência de $c \in S$ com $tr(c) = 1$. Logo, a sequência de R-módulos $S \xrightarrow{tr} R \to 0$ é exata. Definimos $\theta : R \to S$ por $\theta(r) = rc$, para qualquer $r \in R$. θ é um homomorfismo tal que $tr \circ \theta = \mathrm{id}_R$:

$$\begin{aligned} tr \circ \theta(r) &= tr(rc) = r \cdot tr(c) \\ &= r \cdot 1 = r \\ \theta(x + ry) &= (x + ry)c \\ &= xc + ryc = \theta(x) + r\theta(y). \end{aligned}$$

Portanto, R é somando direto de S como R-módulos. □

O Lema a seguir, adaptado de [16; 2.2], traz mais resultados acerca da aplicação traço.

Lema 2.2.8. *Seja S extensão galoisiana de $R = S^G$ com grupo de Galois G. Então são verdadeiras as afirmações a seguir:*

1. *$tr(S) = R$;*
2. *existe $c \in S$ tal que $tr(c) = 1$;*

3. $tr : S \to R$ é um epimorfismo de R-módulos que cinde;

4. R é somando direto de S como R-módulos;

5. $S \simeq R \oplus \ker tr$ como R-módulo;

Demonstração. A partir da demonstração do Lema 2.2.7, obtemos as primeiras quatro afirmações. Assim, basta mostrarmos (5).

A sequência

$$0 \to \ker tr \to S \xrightarrow{tr} R \to 0$$

é exata e cinde. Portanto, pela Proposição 1.2.3, temos $R \oplus \ker tr = S$. □

Lema 2.2.9. *Seja S uma extensão de Galois de R com grupo de Galois G, e A uma R-álgebra comutativa. Defina a ação de G em $A \otimes S$ por $\sigma(a \otimes s) = a \otimes \sigma(s)$, para $s \in S$, $\sigma \in G$ e $a \in A$. Então $A \otimes S$ é uma extensão de Galois de A com grupo de Galois G.*

Demonstração. Pelo Lema 2.2.7, temos que R é um somando direto de S, então $A \otimes S = A \otimes R \oplus A \otimes N$ e $A \otimes R$ e A são R-álgebras isomorfas, e identificaremos $A \otimes R$ e A em $A \otimes S$ por meio deste isomorfismo.

Se $x_1, \ldots, x_n, y_1, \ldots, y_n$ satisfazem $\sum_{i=1}^n x_i \sigma(y_i) = \delta_{\sigma,1}$, então $1 \otimes x_i, 1 \otimes y_i$, $i \in \{1, \ldots, n\}$ satisfazem a mesma condição para $A \otimes S$:

$$\begin{aligned}\sum_{i=1}^n (1 \otimes x_i)\sigma(1 \otimes y_i) &= \sum_{i=1}^n (1 \otimes x_i)\,(1 \otimes \sigma(y_i)) \\ &= \sum_{i=1}^n (1 \otimes x_i\sigma(y_i)) = \sum_{i=1}^n (1 \otimes \delta_{1,\sigma}) = \delta_{1,\sigma}\end{aligned}$$

Assim, basta mostrar que $(A \otimes S)^G = A$. Para qualquer $a \in A$, temos $(1 \otimes \sigma)(a \otimes 1) = a \otimes \sigma(1) = a \otimes 1$, para qualquer $\sigma \in G$, portanto $A \subset (A \otimes S)^G$. Tomemos então w em $(A \otimes S)^G$. Pelo Lema 2.2.7, existe $c \in S$ tal que $tr(c) = 1$. Então $\sum_{i=1}^n (1 \otimes \sigma)(1 \otimes c) = 1 \otimes 1$. Seja então $w \cdot 1 \otimes c = \sum_{i=1}^m a_i \otimes s_i \in A \otimes S$. Logo:

$$w = w \cdot 1 \otimes 1 = w \sum_{\sigma \in G} (1 \otimes \sigma)(1 \otimes c)$$

e como $w \in (A \otimes S)^G$, segue

$$\begin{aligned} w &= \sum_{\sigma \in G} (1 \otimes \sigma)(w \cdot 1 \otimes c) \\ &= \sum_{\sigma \in G} (1 \otimes \sigma)(w \cdot 1 \otimes c) \\ &= \sum_{\sigma \in G} (1 \otimes \sigma) \left(\sum_{i=1}^{m} a_i \otimes s_i \right) \\ &= \sum_{i=1}^{m} a_i \otimes \sum_{\sigma \in G} \sigma(s_i) \\ &= \sum_{i=1}^{m} a_i \otimes tr(s_i) \in A \otimes R = A \end{aligned}$$

Assim, temos $(A \otimes S)^G = A$ □

2.3 Teorema Fundamental da Teoria de Galois

Tratando de extensões de corpos, o teorema fundamental da teoria de Galois determina que, em uma extensão galoisiana $L \mid_K$, para cada corpo intermediário M, $K \subset M \subset L$, existe um subgrupo $H \subset \mathrm{Gal}(L \mid K)$ tal que M permanece fixo pela ação de H. Reciprocamente, a cada subgrupo de $\mathrm{Gal}(L \mid_K)$, corresponde um corpo intermediário, chamado corpo fixo, pois é o subcorpo que permanece fixo pela ação de H.

Tratando de extensões de anéis comutativos, isso não é sempre verdade. Assim, necessitamos de mais informações sobre as álgebras intermediárias, em especial, as álgebras G-fortes.

Definição 2.3.1. Seja S uma extensão galoisiana de R com grupo de Galois G e $T \subset S$ um subanel. Se diz que T é G-forte se para quaisquer $\sigma, \tau \in G$, $\sigma|_T = \tau|_T$ ou $\sigma|_T$ e $\tau|_T$ são fortemente distintos.

Note que se S não possui idempotentes além de 0 e 1 – em particular, se S é corpo – então todo subanel é G-forte. Assim, neste caso, temos uma correspondência biunívoca entre os subgrupos e os subanéis.

Se S é uma extensão galoisiana de R com grupo de Galois G, $H \subset G$ é um subgrupo de G e $T \subset S$ é uma R-subálgebra de S, denotamos

$$S^H = \{s \in S \mid \tau(s) = s, \forall \tau \in H\}$$

e

$$H_T = \{\sigma \in G \mid \sigma(x) = x, \forall x \in T\}.$$

Verificaremos que S^H é uma R-subálgebra de S. De fato, tomemos $\sigma \in H$ $s, t \in S^H$ e $r \in R$. Então $\sigma(rs + t) = \sigma(rs) + \sigma(t) = r\sigma(s) + \sigma(t) = rs + t$, logo $rs + t \in S^H$. Além disso, $\sigma(st) = \sigma(s)\sigma(t) = st \in S^H$. Logo, S^H é uma R-subálgebra de S.

Vejamos agora que H_T é um subgrupo de G. Claramente, $1 \in H_T$. Sejam então $\sigma, \tau \in H_T$, $t \in T$. Temos que $\sigma(t) = t \Rightarrow \sigma^{-1}\sigma(t) = \sigma^{-1}(t) = t$, ou seja, $\sigma^{-1} \in H_T$. Além disso, $\sigma\tau(t) = \sigma(t) = t$, então $\sigma, \tau \in G_T \Rightarrow \sigma\tau \in H_T$. Portanto, H_T é um subgrupo de G.

Seguimos agora com o teorema fundamental da teoria de Galois.

Teorema 2.3.2. *Seja S uma extensão galoisiana de R com grupo de Galois G.*

1. *Seja H um subgrupo de G e $T = S^H$. Então, T é uma R-álgebra separável e G-forte como subálgebra de S, e S é uma extensão galoisiana de T com grupo de Galois $H = H_T$.*

2. *Seja T uma R-subálgebra separável e G-forte de S e $H = H_T$. Então $T = S^H$.*

3. *Para cada $\sigma \in G$ e para cada R-subálgebra separável e G-forte T de S, $H_{\sigma(T)} = \sigma H_T \sigma^{-1}$. Como consequência, um subgrupo H de G é normal se e somente se $\sigma(S^H) = S^H$, para todo $\sigma \in G$. Mais ainda, neste caso S^H é uma extensão galoisiana de R com grupo de Galois G/H.*

Demonstração. 1. Sejam $x_i, y_i \in S$, $i \in \{1, \ldots, n\}$ que satisfazem

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{\sigma,1}$$

para todo $\sigma \in G$. Claramente $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{\sigma,1}$ para todo $\sigma \in H$, e portanto S é uma extensão galoisiana de $T = S^H$ com grupo de Galois H.

Desta forma, S satisfaz todas as condições do Teorema 2.2.4, sendo um T-módulo projetivo; logo, $S \otimes S$ é um $T \otimes T$-módulo projetivo. Por outro lado, S é uma R-álgebra separável e portanto, um $S \otimes S$-módulo projetivo. Assim, S é um $T \otimes T$-módulo projetivo. Como S é uma extensão galoisiana de T, então T é um somando direto de S como T-módulo e, em consequência, T é também um somando direto de S como $T \otimes T$-módulo. Desta forma, T é um $T \otimes T$-módulo projetivo, e portanto, uma R-álgebra separável.

Seja agora $H' = H_T$. Trivialmente, $H \subset H'$ e $S^{H'} = S^H = T$. Por um raciocínio análogo ao usado no início da demonstração, podemos ver que S é também uma extensão galoisiana de T com grupo de Galois H'. Logo, pelo Teorema 2.2.4, temos que $E_H \simeq S \otimes_T S \simeq E_{H'}$, $|H'| = \dim_S S \otimes_T S = |H|$. Logo $H' = H = H^T$.

Finalmente mostraremos que T é G-forte como subálgebra de S. Como S é extensão galoisiana de T com grupo de Galois H, existe $c \in S$ tal que $\sum_{\rho\in H} \rho(c) = 1$.

Consideremos novamente os elementos $x_i, y_i \in S$ $(i \in \{1, \ldots, n\})$ tais que $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{\sigma,1}$, para qualquer $\sigma \in G$, e sejam $x'_i = \sum_{\rho\in H} \rho(x_ic)$ e $y'_i = \sum_{\rho\in H} \rho(y_i)$, para $i = 1, \ldots, n$. Como $x'_i = tr_H(x_ic)$ e $y'_i = tr_H(y_i)$, estes x'_i, y'_i pertencem a $S^H = T$, como mostrado na página 44.

Além disto, temos:

$$\begin{aligned}
\sum_{i=1}^{n} x'_i\sigma(y'_i) &= \sum_{i=1}^{n} \left(\sum_{\rho\in H} \rho(x_ic)\right) \sigma\left(\sum_{\tau\in H} \tau(y_i)\right) = \sum_{\rho,\tau\in H} \rho(c) \sum_{i=1}^{n} \rho(x_i)\sigma\tau(y_i) \\
&= \sum_{\rho,\tau\in H} \rho(c)\rho\left(\sum_{i=1}^{n} x_i\rho^{-1}\sigma\tau(y_i)\right) = \sum_{\rho,\tau\in H} \rho(c)\delta_{1,\rho^{-1}\sigma\tau} \\
&= \sum_{\rho\in H} \rho(c) \sum_{\tau\in H} \delta_{1,\rho^{-1}\sigma\tau} = \begin{cases} 1, \text{ se } \sigma \in H \\ 0, \text{ se } \sigma \notin H \end{cases}
\end{aligned}$$

para qualquer $\sigma \in G$.

Sejam $\sigma, \tau \in G$ tais que $\sigma|_T \neq \tau|_T$. Então $\tau\sigma^{-1} \notin H$. Se agora $e \in S$ é um idempotente não nulo tal que $\sigma(t)e = \tau(t)e$, para todo $t \in T$, então $te = \tau\sigma^{-1}(t)e$ para todo $t \in T$ e

$$e = \left(\sum_{i=1}^{n} x_i' y_i'\right) = \sum_{i=1}^{n} x_i'(y_i' e) = \sum_{i=1}^{n} x_i' \tau\sigma^{-1}(y_i)e = 0e = 0$$

e, portanto, T é G-forte.

2. Seja T uma R-subálgebra separável e G-forte de S e seja $H = H_T$. $T \subset S^H$, pois S^H são os elementos fixos pela ação de $H = H_T$, que é o subgrupo que mantém T fixo. Basta mostrar que $S^H \subset T$.

Temos que $S \otimes S$ é uma extensão de Galois de $S \otimes R = S$ com grupo de Galois G, onde S opera no primeiro fator e G no segundo. Então o isomorfismo $h : S \otimes S \to E$, dado por $h(s \otimes t)(\sigma) = s\sigma(t)$, induz uma ação de G em E por $\sigma v(\tau) = v(\tau\sigma)$ e portanto, E é uma extensão de Galois de S com grupo G.

Ainda, como S é R-projetivo, identificaremos $S \otimes T$ com sua imagem em $S \otimes S$. Vamos mostrar que $E^H \subset h(S \otimes T)$.

Seja $G = \bigcup_{i=1}^{r} \sigma_i H$. Então E^H é o conjunto das funções de G em S que são constantes nas classes $\sigma_i H$.

Seja $f_i : E \to S$ o homomorfismo de S-álgebras definido por $f_i(v) = v(\sigma_i)$. Vamos mostrar que $f_1, \ldots, f_r$ são dois a dois fortemente distintos.

Pela definição de $H = H_T$, temos que $i \neq j \Rightarrow \sigma_i \mid_T \neq \sigma_j \mid_T$. Dado $e \in S$ idempotente não nulo, como T é G-forte, existe $t \in T$ tal que $f_i(h(1 \otimes t))e = \sigma_i(t)e \neq \sigma_j(t)e = f_j(h(1 \otimes t))e$. Logo, $f_1, \ldots, f_r$ são fortemente distintos.

Como T é R-separável, $S \otimes T$ é S-separável. Podemos verificar isso observando que

$$(S \otimes T) \otimes_S (S \otimes T) = S \otimes (T \otimes T)$$

e que se $e_T \in T \otimes T$ é o idempotente de separabilidade de T sobre R, então $1 \otimes e_T$ é o idempotente de separabilidade de $S \otimes T$ sobre S. Além disso, como h é um isomorfismo de S-álgebras, temos que $h(S \otimes T)$ também é uma

S-álgebra separável. Portanto, existem idempotentes $w_1, \ldots, w_r$, dois a dois ortogonais, com $f_i(x)w_i = xw_i$ e $w_i(\sigma_j) = f_j(w_i) = \delta_{i,j}$.

Notemos que $w_i \in E^H$, para qualquer $i \in \{1, \ldots, r\}$, pois $h(S \otimes T) \subset E^H$. Logo, precisamos mostrar que $w_1, \ldots, w_r$ gera E^H como S-módulo.

Observamos que se $z = \sum_{\sigma \in G} a_\sigma v_\sigma \in E^H$, então $\rho(z) = z$, para qualquer $\rho \in H$, e portanto

$$\sum_{\sigma \in G} a_\sigma v_{\sigma\rho^{-1}} = \sum_{\sigma \in G} a_\sigma v_\sigma \quad \text{ou} \quad \sum_{\sigma \in G} a_{\sigma\rho} v_\sigma = \sum_{\sigma \in G} a_\sigma v_\sigma$$

de onde seque que $a_{\sigma\rho} = a_\sigma$, para todo $\sigma \in G, \rho \in H$. Em particular, $a_{\sigma_i} = a_{\sigma_i \rho}$, para todo $\rho \in H$, $i \in \{1, \ldots, n\}$. Então, como $G = \bigcup_{i=1}^r \sigma_i H$, para qualquer $z \in E^H$, temos:

$$z = \sum_{\sigma \in G} a_\sigma v_\sigma = \sum_{i=1}^r \sum_{\rho \in H} a_{\sigma_i \rho^{-1}} v_{\sigma_i \rho^{-1}} = \sum_{i=1}^r a_{\sigma_i} \left(\sum_{\rho \in H} \rho(v_{\sigma_i}) \right)$$

Como $f_i(w_j) = \delta_{i,j}$ e $w_i \in E^H$, para quaisquer $i, j \in \{1, \ldots, r\}$, obtemos $w_i = \sum_{\rho \in H} \rho(v_{\sigma_i})$ e $z = \sum_{i=1}^r a_{\sigma_i} w_i$, para todo $z \in E^H$. Logo, $E^H \subset h(S \otimes T) \Rightarrow E^H = h(S \otimes T)$.

Como $E^H \subset h(S \otimes T)$, aplicando h^{-1} obtemos $S \otimes S^H \subset (S \otimes S)^H \subset S \otimes T$, e agora aplicamos $tr \otimes 1$ para obter $S^H \subset T$. Logo, $T = S^H$.

3. Sejam $\rho \in H_T$ e $t \in T$. Temos que $\sigma(t) \in \sigma(T)$ e portanto, $\sigma\rho\sigma^{-1}(\sigma(t)) = \sigma\rho(t) = \sigma(t)$, para qualquer $\sigma \in G$. Portanto, $\sigma H \sigma^{-1} \subset H_{\sigma(T)}$. Por outro lado, seja $\rho \in H_{\sigma(T)}$, isto é, $\rho \in G$ tal que $\rho\sigma(t) = \sigma(t)$, para qualquer $t \in T$. Devemos mostrar que $\rho \in \sigma H_T \sigma^{-1}$, ou seja, que existe $\tau \in H$ tal que $\rho = \sigma\tau\sigma^{-1}$. Temos que, dado $t \in T$, $\rho\sigma(t) = \sigma(t)$, pois $\rho \in H_{\sigma(T)}$, então $\sigma^{-1}\rho\sigma(t) = t$, para qualquer $t \in T$. Assim, $\sigma^{-1}\rho\sigma \in H_T$. Então, existe $\tau \in H_T$ tal que $\tau = \sigma^{-1}\rho\sigma$, isto é, $\rho = \sigma\tau\sigma^{-1} \in \sigma H_T \sigma^{-1}$. Portanto, $\sigma H_T \sigma^{-1} = H_{\sigma(T)}$.

Por outro lado, suponha H normal, isto é, $H = \sigma H \sigma^{-1}$, para qualquer $\sigma \in G$. Vamos mostrar que $\sigma(S^H) = S^H$. Sejam quaisquer $s \in S^H$ e $\rho \in H$; então existe $\tau \in H$ tal que $\sigma\tau = \rho\sigma$.

Se $s \in S^H$, então $s = \rho(s) = \sigma\tau\sigma^{-1}(s)$, e $\sigma\tau\sigma^{-1}(s) \in \sigma(S^H)$ se $\tau\sigma^{-1}(s) \in S^H$. Tomemos agora qualquer $\psi \in H$; então existe $\phi \in H$ tal que $\phi\sigma = \sigma\psi$. Segue, então

$$\begin{aligned}\psi(\tau\sigma^{-1}(s)) &= \psi(\sigma^{-1}\rho(s)) = \psi\sigma^{-1}(s) \\ &= \sigma^{-1}\phi(s) = \sigma^{-1}(s) = \sigma^{-1}\rho(s) = \tau\sigma^{-1}(s).\end{aligned}$$

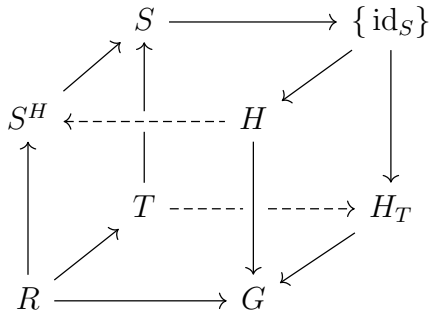
Logo, $\tau\sigma^{-1}(s) \in S^H$ e, desta maneira, $S^H \subset \sigma(S^H)$. Por outro lado, tomemos $\sigma(s) = t \in \sigma(S^H)$. Para qualquer $\rho \in H$, temos

$$\rho(t) = \rho\sigma(s) = \sigma\tau(s) = \sigma(s) = t$$

Portanto, $\sigma(s) = t \in S^H$, para qualquer $s \in S^H$.

Por fim, seja H subgrupo normal de G e $T = S^H$. Então $\sigma(T) = T$, para qualquer $\sigma \in G$. Seja $G/H = \{\bar{\sigma}_i = \sigma_i H \mid 1 \leq i \leq r\}$. Definimos $\bar{\sigma}_i : T \to T$ por $\bar{\sigma}_i(x) = \sigma_i(x)$, para todo $x \in T$, $i \in \{1, \ldots, r\}$. Podemos ver que a ação de σ_i sobre T não depende do representante de $\bar{\sigma}_i$ escolhido, pois $T = S^H$. Além disso, $T^{G/H} = S^G = R$ e os elementos $x_i', y_i' \in T$, $i \in \{1, \ldots, n\}$, construídos na demonstração do item (1) mostram que T é uma extensão galoisiana de R com grupo de Galois G/H, pois satisfazem o Teorema 2.2.4. □

Com o resultado acima, podemos estabelecer a correspondência entre as R-subálgebras G-fortes de S e os subgrupos de G, de forma análoga às extensões galoisianas de corpos. Assim, obtemos o diagrama a seguir:



Exemplo. Sejam R um anel comutativo com unidade e $S = Re_1 \oplus Re_2 \oplus Re_3 \oplus Re_4$, onde e_1, e_2, e_3, e_4 são idempotentes dois a dois ortogonais de S com $e_1+e_2+e_3+e_4 = 1_S$. Seja G o grupo cíclico de ordem 4, gerado a partir de σ, agindo em S via $\sigma(e_i) = e_{i+1}$.

Vamos verificar que S é extensão galoisiana de $R = S^G$ com sistema de coordenadas de Galois $x_i = y_i = e_i$, com $1 \leq i \leq 4$:

$$\sum_{i=1}^{4} x_i \rho(y_i) = \sum_{i=1}^{4} e_i \rho(e_i),$$

caso $\rho = id_S$, temos $\sum_{i=1}^{4} e_i^2 = 1$; caso $\rho \neq id_S$, como $e_i e_j = 0$, para $i \neq j$, temos $\sum_{i=1}^{4} e_i \rho(e_i) = 0$.

Seja $T = R(e_1 + e_2) \oplus R(e_3 + e_4)$ e tomemos $t = r_1(e_1 + e_2) + r_2(e_3 + e_4)$, com $r_1, r_2 \in R$. Observe no quadro abaixo os automorfismos de G restritos a T:

$\mathrm{id}_S(t)$	$r_1(e_1 + e_2) + r_2(e_3 + e_4)$
$\sigma(t)$	$r_1(e_2 + e_3) + r_2(e_4 + e_1)$
$\sigma^2(t)$	$r_1(e_3 + e_4) + r_2(e_1 + e_2)$
$\sigma^3(t)$	$r_1(e_4 + e_1) + r_2(e_2 + e_3)$
$\sigma^4(t) = \mathrm{id}_S(t)$	$r_1(e_1 + e_2) + r_2(e_3 + e_4)$

Podemos observar que $\sigma^i \mid_T \neq \sigma^j \mid_T$, se $i \neq j$, $0 \leq i, j \leq 3$. Assim, temos que σ^i e σ^j devem ser fortemente distintos para que T seja uma R-subálgebra G-forte de S: dois automorfismos distintos $\sigma^i, \sigma^j \in G$ devem satisfazer $\sigma^i(t)e \neq \sigma^j(t)e$, para qualquer $t \in T$ e e idempotente não nulo de T. Temos que

$$\begin{aligned} \sigma(t)e_1 &= (r_1(e_2 + e_3) + r_2(e_4 + e_1))\, e_1 = r_2 e_1, \text{ e} \\ \sigma^2(t)e_1 &= (r_1(e_3 + e_4) + r_2(e_1 + e_2))\, e_1 = r_2 e_1 \\ \Rightarrow \quad \sigma(t)e_1 &= \sigma^2(t)e_1. \end{aligned}$$

Portanto, T não é G-forte. Observemos agora

$$H_T = \{g \in G \mid g(t) = t,\ \forall t \in T\}.$$

Temos que $H_T = \{\mathrm{id}_S\}$, porém $S^{H_T} = S \neq T$. Na página 7, vimos um exemplo semelhante para o caso de corpos, onde a correspondência não era satisfeita, pois a extensão $\mathbb{Q}(\sqrt[3]{2})\ |_{\mathbb{Q}}$ não é normal. Agora, em extensões de anéis, este exemplo deixa clara a importância da hipótese de T ser G-forte para garantir a bijetividade da correspondência de Galois.

Tomemos agora um subgrupo de G. Como G é o grupo cíclico de ordem 4, temos que $H = \{\mathrm{id}_S, \sigma^2\} \simeq \mathbb{Z}_2$ é único subgrupo próprio de G. Pelo Teorema 2.3.2, temos que S^H é uma R-álgebra separável e G-forte, e que $S = Re_1 \oplus Re_1 \oplus Re_3 \oplus Re_4$ é extensão de S^H e, se $\tau(S^H) = S^H$ para todo $\tau \in G$, onde segue que S^H é extensão galoisiana de R com grupo de Galois G/H.

Primeiro, vamos identificar quem é $T = S^H$. Temos

$$\sigma^2(r_1e_1 + r_2e_2 + r_3e_3 + r_4e_4) = r_1e_3 + r_2e_4 + r_3e_1 + r_4e_2,$$

logo se $\sigma^2(t) = t$, temos $t \in R(e_1 + e_3) \oplus R(e_2 + e_4) = T$.

Agora, como

$$\sigma(r_1(e_1 + e_3) + r_2(e_2 + e_4)) = r_1(e_2 + e_4) + r_2(e_1 + e_3)$$

temos que $\sigma(T) = T$, para todo $\sigma \in G$. Logo H é normal e T é extensão galoisiana de R com grupo de Galois $G/H = \left\{\bar{\mathrm{id}}_S, \bar{\sigma}\right\}$.

Exemplo. Seja $G = S_3 \times C_2$, onde S_3 é o grupo de permutações de 3 elementos e C_2 é o grupo cíclico de ordem 2. Seja R um anel comutativo com unidade e considere

$$S = \bigoplus_{g \in G} Re_g.$$

S_3 possui 4 subgrupos próprios: um subgrupo cíclico de ordem 3, formado pelas permutações $\{1, (1\ 2\ 3), (1\ 3\ 2)\}$, e 3 subgrupos cíclicos de ordem 2, a saber $\{1, (1\ 2)\}, \{1, (1\ 3)\}, \{1, (2\ 3)\}$; combinados com os subgrupos de C_2, temos 12 subgrupos do grupo de Galois G:

$$
\begin{array}{cc}
H_1 = \{1\} \times \{1\} & H_2 = \{1\} \times S_2 \\
H_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\} \times \{1\} & H_4 = \{1, (1\ 2\ 3), (1\ 3\ 2)\} \times S_2 \\
H_5 = \{1, (1\ 2)\} \times \{1\} & H_6 = \{1, (1\ 2)\} \times S_2 \\
H_7 = \{1, (1\ 3)\} \times \{1\} & H_8 = \{1, (1\ 3)\} \times S_2 \\
H_9 = \{1, (2\ 3)\} \times \{1\} & H_{10} = \{1, (2\ 3)\} \times S_2 \\
H_{11} = S_3 \times \{1\} & H_{12} = S_3 \times S_2
\end{array}
$$

Para determinar as subálgebras que permanecem fixas pela ação de cada subgrupo H_i, sejam $T_i = S^{H_i}$ e $s \in S$ dado por

$$s = \sum_{(\sigma,\tau)\in G} r_{(\sigma,\tau)} e_{(\sigma,\tau)}.$$

A partir deste momento, vamos denotar os elementos de S_3 e C_2 de forma a facilitar a indexação dos idempotentes. As transposições $(m\ n) \in S_3$ serão denotadas por σ_{mn}, e $(1\ 2\ 3) = \rho$. Além disso, $C_2 = \{1, \varphi\}$.

Vejamos a tábua de operação de S_3.

$(S_3, \circ)$	1	σ_{12}	σ_{23}	σ_{13}	ρ	ρ^2
1	1	σ_{12}	σ_{23}	σ_{13}	ρ	ρ^2
σ_{12}	σ_{12}	1	ρ	ρ^2	σ_{23}	σ_{13}
σ_{23}	σ_{23}	ρ^2	1	ρ	σ_{13}	σ_{12}
σ_{13}	σ_{13}	ρ	ρ^2	1	σ_{12}	σ_{23}
ρ	ρ	σ_{13}	σ_{12}	σ_{23}	ρ^2	1
ρ^2	ρ^2	σ_{23}	σ_{13}	σ_{12}	1	ρ

De onde segue

$$T_1 = S$$

$$T_2 = \bigoplus_{\sigma\in S_3} R\left(e_{(\sigma,1)} + e_{(\sigma,\varphi)}\right)$$

$$\begin{aligned}
T_3 =& R\left(e_{(1,1)} + e_{(\rho,1)} + e_{(\rho^2,1)}\right) \oplus R\left(e_{(\sigma_{12},1)} + e_{(\sigma_{13},1)} + e_{(\sigma_{23},1)}\right) \\
& \oplus R\left(e_{(1,\varphi)} + e_{(\rho,\varphi)} + e_{(\rho^2,\varphi)}\right) \oplus R\left(e_{(\sigma_{12},\varphi)} + e_{(\sigma_{13},\varphi)} + e_{(\sigma_{23},\varphi)}\right)
\end{aligned}$$

Observe agora que $(\rho,\varphi)^2 = (\rho^2, 1)$ e $(\rho,\varphi)^3 = (1,\varphi)$. Como ρ é um elemento de ordem 3 em S_3, e φ é de ordem 2, temos que (ρ,φ) é de ordem 6. Desta forma, associamos os idempotentes em duas somas, com seis parcelas cada.

$$\begin{aligned} T_4 =& R\left(e_{(1,1)} + e_{(\rho,\varphi)} + e_{(\rho^2,1)} + e_{(1,\varphi)} + e_{(\rho,1)} + e_{(\rho^2,\varphi)}\right) \\ & \oplus R\left(e_{(\sigma_{12},1)} + e_{(\sigma_{13},\varphi)} + e_{(\sigma_{23},1)} + e_{(\sigma_{12},\varphi)} + e_{(\sigma_{13},1)} + e_{(\sigma_{23},\varphi)}\right) \end{aligned}$$

Para $5 \leq i \leq 10$, temos ações semelhantes por σ_{mn}. Como σ_{mn} é de ordem 2, assim como φ, temos $(\sigma_{mn},\varphi)^2 = (1,1)$ e portanto, associamos os idempotentes dois a dois.

$$\begin{aligned} T_5 =& R\left(e_{(1,1)} + e_{(\sigma_{12},1)}\right) \oplus R\left(e_{(\rho,1)} + e_{(\sigma_{23},1)}\right) \oplus R\left(e_{(\rho^2,1)} + e_{(\sigma_{13},1)}\right) \\ & \oplus R\left(e_{(1,\varphi)} + e_{(\sigma_{12},\varphi)}\right) \oplus R\left(e_{(\rho,\varphi)} + e_{(\sigma_{23},\varphi)}\right) \oplus R\left(e_{(\rho^2,\varphi)} + e_{(\sigma_{13},\varphi)}\right) \end{aligned}$$

$$\begin{aligned} T_6 =& R\left(e_{(1,1)} + e_{(\sigma_{12},\varphi)}\right) \oplus R\left(e_{(\rho,1)} + e_{(\sigma_{23},\varphi)}\right) \oplus R\left(e_{(\rho^2,1)} + e_{(\sigma_{13},\varphi)}\right) \\ & \oplus R\left(e_{(1,\varphi)} + e_{(\sigma_{12},1)}\right) \oplus R\left(e_{(\rho,\varphi)} + e_{(\sigma_{23},1)}\right) \oplus R\left(e_{(\rho^2,\varphi)} + e_{(\sigma_{13},1)}\right) \end{aligned}$$

$$\begin{aligned} T_7 =& R\left(e_{(1,1)} + e_{(\sigma_{13},1)}\right) \oplus R\left(e_{(\rho,1)} + e_{(\sigma_{12},1)}\right) \oplus R\left(e_{(\rho^2,1)} + e_{(\sigma_{23},1)}\right) \\ & \oplus R\left(e_{(1,\varphi)} + e_{(\sigma_{13},\varphi)}\right) \oplus R\left(e_{(\rho,\varphi)} + e_{(\sigma_{12},\varphi)}\right) \oplus R\left(e_{(\rho^2,\varphi)} + e_{(\sigma_{23},\varphi)}\right) \end{aligned}$$

$$\begin{aligned} T_8 =& R\left(e_{(1,1)} + e_{(\sigma_{13},\varphi)}\right) \oplus R\left(e_{(\rho,1)} + e_{(\sigma_{12},\varphi)}\right) \oplus R\left(e_{(\rho^2,1)} + e_{(\sigma_{23},\varphi)}\right) \\ & \oplus R\left(e_{(1,\varphi)} + e_{(\sigma_{13},1)}\right) \oplus R\left(e_{(\rho,\varphi)} + e_{(\sigma_{12},1)}\right) \oplus R\left(e_{(\rho^2,\varphi)} + e_{(\sigma_{23},1)}\right) \end{aligned}$$

$$\begin{aligned} T_9 =& R\left(e_{(1,1)} + e_{(\sigma_{23},1)}\right) \oplus R\left(e_{(\rho,1)} + e_{(\sigma_{13},1)}\right) \oplus R\left(e_{(\rho^2,1)} + e_{(\sigma_{12},1)}\right) \\ & \oplus R\left(e_{(1,\varphi)} + e_{(\sigma_{23},\varphi)}\right) \oplus R\left(e_{(\rho,\varphi)} + e_{(\sigma_{13},\varphi)}\right) \oplus R\left(e_{(\rho^2,\varphi)} + e_{(\sigma_{12},\varphi)}\right) \end{aligned}$$

$$\begin{aligned} T_{10} =& R\left(e_{(1,1)} + e_{(\sigma_{23},\varphi)}\right) \oplus R\left(e_{(\rho,1)} + e_{(\sigma_{13},\varphi)}\right) \oplus R\left(e_{(\rho^2,1)} + e_{(\sigma_{12},\varphi)}\right) \\ & \oplus R\left(e_{(1,\varphi)} + e_{(\sigma_{23},1)}\right) \oplus R\left(e_{(\rho,\varphi)} + e_{(\sigma_{13},1)}\right) \oplus R\left(e_{(\rho^2,\varphi)} + e_{(\sigma_{12},1)}\right) \end{aligned}$$

Por fim, temos

$$T_{11} = R\left(\sum_{\sigma\in S_3} e_{(\sigma,1)}\right) \oplus R\left(\sum_{\sigma\in S_3} e_{(\sigma,\varphi)}\right)$$

$$T_{12} = R \sum_{(\sigma,\tau)\in G} e_{(\sigma,\tau)} \simeq R$$

Pelo Teorema 2.3.2, temos que T_i são R-álgebras separáveis e G-fortes enquanto subálgebras de S.

Claramente temos H_2 normal: dado $(\sigma,\tau) \in G$, $(\sigma,\tau)(t) \in T_2$, para todo $t \in T_2$. Logo T_2 é extensão galoisiana de R com grupo de Galois $G_2 = G/H_2 \simeq S_3$.

Observe que H_3 e H_4 também são subgrupos normais de G. Basta observar que os elementos de G permutam os idempotentes de uma mesma parcela, ou "trocam as parcelas" da soma direta. Sendo assim, temos que T_3 e T_4 são extensões galoisiana de R, com grupo de Galois $G_3 = G/H_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ e $G_4 = G/H_4 \simeq \mathbb{Z}_2$, respectivamente.

Exemplo. Sejam R um anel comutativo com unidade e G um grupo finito. Considere $S = \bigoplus_{\sigma\in G} Re_\sigma$, onde $e_\sigma e_\tau = \delta_{\sigma,\tau} e_\sigma$ e $\sum_{\sigma\in G} e_\sigma = 1$. A ação de G em S é dada por $\sigma(e_\tau) = e_{\sigma\tau}$.

Então, com $x_i = y_i = e_\sigma$, para $1 \leq i \leq |G| = n$, temos

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \sum_{\tau\in G} e_\tau \sigma(e_\tau) = \sum_{\tau\in G} \delta_{\tau,\sigma\tau} e_\tau = \delta_{1,\sigma}$$

e portanto, x_i, y_i são um sistema de coordenadas de Galois para S, que por sua vez é uma extensão galoisiana de R. Note que este exemplo engloba os exemplos anteriores.

2.4 Homomorfismos de Extensões Galoisianas

Nesta seção, estaremos estudando os homomorfismos de extensões galoisianas. Em especial, iremos mostrar que se existe um homomorfismo de R-álgebras e G-módulos entre duas extensões com mesmo grupo de Galois, então estas extensões são isomorfas.

Teorema 2.4.1. *Sejam S uma extensão galoisiana de R com grupo de Galois G, A uma R-álgebra comutativa, $f, g : S \to A$ homomorfismos de R-álgebras.*

Então existe um único conjunto $\{e_\sigma \mid \sigma \in G\}$ *de idempotentes dois a dois ortogonais de* A*, alguns possivelmente nulos, tais que* $\sum_{\sigma\in G} e_\sigma = 1$ *e*

$$g(s) = \sum_{\sigma\in G} f(\sigma(s))e_\sigma$$

Além disso, se f *é um homomorfismo de* R*-álgebras, qualquer aplicação* $g : S \to A$ *definida desta forma também será.*

Demonstração. Seja θ a composição

$$E \xrightarrow{h^{-1}} S \otimes S \xrightarrow{f\otimes g} A \otimes A \xrightarrow{k} A$$

onde $h : S \otimes S \to E$ é dado por $h(s \otimes t)(\sigma) = s\sigma(t)$ e $k(a_1 \otimes a_2) = a_1a_2$.

Seja $e_\sigma = \theta(v_\sigma)$, onde $v_\sigma \in E$ é definido por $v_\sigma(\tau) = \delta_{\sigma,\tau}$. Temos $e_\sigma e_\tau = \theta(v_\sigma v_\tau)$; vimos anteriormente, na página 36, que os elementos $v_\sigma \in E$, $\sigma \in G$ são idempotentes dois a dois ortogonais, e portanto $\theta(v_\sigma) = e_\sigma$ também o são. Além disso, $\sum_{\sigma\in G} e_\sigma = \sum_{\sigma\in G} \theta(v_\sigma) = \theta\left(\sum_{\sigma\in G} v_\sigma\right) = 1$.

Tomemos $h : S \otimes S \to E$ dada por $h(s \otimes t)(\sigma) = s\sigma(t)$, como no Teorema 2.2.4. Então, temos que $h(1\otimes s) = \sum_{\sigma\in G} \sigma(s)v_\sigma$: dado qualquer $\tau \in G$, temos $h(1 \otimes s)(\tau) = 1\tau(s) = \tau(s)$, e por outro lado

$$\left(\sum_{\sigma\in G} \sigma(s)v_\sigma\right)(\tau) = \sum_{\sigma\in G} \sigma(s)v_\sigma(\tau) = \sum_{\sigma\in G} \sigma(s)\delta_{\sigma,\tau} = \tau(s).$$

Aplicando θ na equação $h(1\otimes s) = \sum_{\sigma\in G} \sigma(s)v_\sigma$, temos $\theta(h(1\otimes s)) = g(s)$:

$$\begin{aligned}\theta(h(1 \otimes s)) &= k\left(f \otimes g\left(h^{-1}\left(h\left(1 \otimes s\right)\right)\right)\right)\\ &= k\left(f \otimes g\left(1 \otimes s\right)\right)\\ &= f(1)g(s) = g(s)\end{aligned}$$

Assim:

$$\begin{aligned} g(s) = \theta(h(1 \otimes s)) &= \theta\left(\sum_{\sigma \in G} \sigma(s) v_\sigma\right) = \sum_{\sigma \in G} \theta\left(\sigma(s)\right) e_\sigma \\ &= \sum_{\sigma \in G} k\left(f \otimes g\left(h^{-1}\left(\sigma(s)\right)\right)\right) e_\sigma = \sum_{\sigma \in G} k\left(f \otimes g\left(\sigma(s) \otimes 1\right)\right) e_\sigma \\ &= \sum_{\sigma \in G} k\left(f\left(\sigma(s)\right) \otimes g(1)\right) e_\sigma = \sum_{\sigma \in G} f\left(\sigma(s)\right) e_\sigma \end{aligned}$$

Para mostrar a unicidade, suponha $\{d_\sigma \mid \sigma \in G\}$ elementos idempotentes de A, dois a dois ortogonais, que satisfazem as condições $\sum_{\sigma \in G} d_\sigma = 1$ e $g(s) = \sum_{\sigma \in G} f(\sigma(s)) d_\sigma$, para todo $s \in S$. Seja $h^{-1}(v_\sigma) = \sum_{i=1}^{r} s_i \otimes t_i$; então $\sum_{i=1}^{r} s_i \rho(t_i) = v_\sigma(\rho) = \delta_{\sigma,\rho}$ e

$$\begin{aligned} e_\sigma = \theta(v_\sigma) &= \sum_{i=1}^{r} f(s_i) g(t_i) = \sum_{i=1}^{r} f(s_i) \left(\sum_{\rho \in G} f(\rho(t_i)) d_\rho\right) \\ &= \sum_{i=1}^{r} \sum_{\rho \in G} f(s_i) f(\rho(t_i)) d_\rho = \sum_{\rho \in G} \sum_{i=1}^{r} f(s_i \rho(t_i)) d_\rho \\ &= \sum_{\rho \in G} f\left(\sum_{i=1}^{r} s_i \rho(t_i)\right) d_\rho = \sum_{\rho \in G} \delta_{\sigma,\rho} d_\rho = d_\sigma \end{aligned}$$

Por fim, vamos mostrar que se f é um homomorfimos de R-álgebras, então $g(s) = \sum_{\sigma \in G} f(\sigma(s)) e_\sigma$ também é. Sejam $s, t \in S$, $r \in R$. Temos então

- $\begin{aligned} g(s+t) &= \sum_{\sigma \in G} f(\sigma(s+t)) e_\sigma \\ &= \sum_{\sigma \in G} f(\sigma(s)) e_\sigma + \sum_{\sigma \in G} f(\sigma(t)) e_\sigma \\ &= g(s) + g(t) \end{aligned}$

- $\begin{aligned} g(rs) &= \sum_{\sigma \in G} f(\sigma(rs)) e_\sigma \\ &= \sum_{\sigma \in G} r f(\sigma(s)) e_\sigma \\ &= r g(s) \end{aligned}$

- $g(s)g(t) = \left(\sum_{\sigma\in G} f(\sigma(s))e_\sigma\right)\left(\sum_{\rho\in G} f(\rho(s))e_\rho\right)$
  $= \sum_{\sigma\in G} f(\sigma(s))e_\sigma \sum_{\rho\in G} f(\rho(s))e_\rho$
  $= \sum_{\sigma\in G} f(\sigma(s)) \sum_{\rho\in G} f(\rho(s))e_\rho e_\sigma$
  $= \sum_{\sigma\in S} f(\sigma(s))f(\sigma(t))e_\sigma$
  $= \sum_{\sigma\in S} f(\sigma(st))e_\sigma = g(st)$

Assim, encerramos a demonstração. □

Note que se A não tem idempotentes diferentes de 0 e 1, então existe um único elemento $\sigma \in G$ tal que $e_\sigma = 1$, e portanto $g(s) = f(\sigma(s))$, para todo $s \in S$.

Sejam S uma extensão galoisiana de R com grupo de Galois G, W o semigrupo multiplicativo dos endomorfismos de anéis de S que mantém R fixo, isto é, $W \subset \mathrm{Hom}_R(S,S)$. Desta forma, sendo $j : D \to \mathrm{Hom}_R(S,S)$ o isomorfismo dado por $j(s\delta_\sigma) = s\sigma$ como no Teorema 2.2.4, segue que $j^{-1}(W)$ consiste em todos os elementos de D da forma $\sum_{\sigma\in G} e_\sigma\delta_\sigma$, com e_σ idempotentes dois a dois ortogonais de S tais que $\sum_{\sigma\in G} e_\sigma = 1$.

De fato, tomando $A = S$ e $f = \mathrm{id}_S$ no Teorema 2.4.1, temos que existe um conjunto de idempotentes $\{e_\sigma \mid \sigma \in G\} \subset S$, tais que $\sum_{\sigma\in G} e_\sigma = 1$ e $g(s) = \sum_{\sigma\in G} \sigma(s)e_\sigma$, isto é, $j^{-1}(g) = \sum_{\sigma\in G} e_\sigma\delta_\sigma$.

Corolário 2.4.2. *Nas notações acima, se todo idempotente de S pertence a R, então todo elemento de W é um automorfismo, e portanto o grupo de R-automorfismos de S é isomorfo, via j^{-1}, ao subgrupo multiplicativo do grupo $R(G) \subseteq D$, que consiste dos elementos da forma $\sum_{\sigma\in G} e_\sigma\sigma$. Além disso, S não tem idempotentes além de 0 e 1 se e somente se $W = G$, isto é, se G é o conjunto de todos os R-endomorfismos de S.*

Demonstração. Se todos os idempotentes de S estão contidos em R, então $e_\sigma \in R$, e temos que

$$\left(\sum_{\sigma\in G} e_\sigma\delta_\sigma\right)\left(\sum_{\sigma\in G} e_\sigma\delta_{\sigma^{-1}}\right) = \sum_{\sigma\in G} e_\sigma\delta_\sigma \sum_{\rho\in G} e_\rho\delta_{\rho^{-1}}$$
$$= \sum_{\sigma\in G}\sum_{\rho\in G} e_\sigma\sigma(e_\rho)\delta_{\sigma\rho^{-1}}$$
$$= \sum_{\sigma\in G}\sum_{\rho\in G} e_\sigma e_\rho\delta_{\sigma\rho^{-1}}$$
$$= \sum_{\sigma\in G} e_\sigma\delta_1 = 1 \in D$$

assim, todo endomorfismo de W tem inverso, logo são todos R-automorfismos de S.

Se S não tem idempotentes além de 0 e 1, temos que todos seus idempotentes pertencem a R, logo todo endomorfismo de S é um automorfismo. Assim, todos são escritos da forma $f = \sum_{\sigma\in G} e_\sigma\sigma$; como $\sum_{\sigma\in G} e_\sigma = 1$, temos que $f = \sigma$, para algum $\sigma \in G$. Logo, $W = G$. □

Teorema 2.4.3. *Sejam S, S' extensões galoisianas de R com mesmo grupo de Galois G, e seja $f : S \to S'$ um homomorfismo de R-álgebras e G-módulos. Então f é um isomorfismo.*

Demonstração. Tomemos $x_1, \ldots, x_r, y_1, \ldots, y_r \in S$ um sistema de coordenadas de Galois, conforme visto no Teorema 2.2.4. Para qualquer $x' \in S'$,

temos

$$\begin{aligned} f\left(\sum_{i=1}^{r} x_i tr(f(y_i)x')\right) &= \sum_{i=1}^{r} f(x_i)tr(f(y_i)x') \\ &= \sum_{i=1}^{r}\sum_{\sigma\in G} f(x_i)\sigma(f(y_i)x') \\ &= \sum_{\sigma\in G}\sigma(x')\sum_{i=1}^{r} f(x_i)f(\sigma(y_i)) \\ &= \sum_{\sigma\in G}\sigma(x')f\left(\sum_{i=1}^{r} x_i\sigma(y_i)\right) \\ &= \sum_{\sigma\in G}\sigma(x')\delta_{1,\sigma} = x' \end{aligned}$$

e, portanto, f é sobrejetivo.

Tomemos agora $x \in S$ tal que $f(x) = 0$. Então, $\sigma(f(x)) = 0$, o que implica $\sigma(f(x))f(\sigma(y_i)) = f(\sigma(xy_i)) = 0$, e portanto, $\sum_{\sigma\in G} f(\sigma(xy_i)) = f(tr(xy_i)) = 0$. Como $tr(xy_i) \in R$, segue que $f(tr(xy_i)) = tr(xy_i)$. Logo

$$x = \sum_{i=1}^{r} x_i tr(xy_i) = 0$$

e, portanto, f é injetiva. Assim, f é um isomorfismo. □

Teorema 2.4.4. *Sejam S um anel comutativo sem idempotentes além de 0 e 1, G um grupo arbitrário de automorfismos de S e $R = S^G$.*

Assuma que S é uma R-álgebra separável e um R-módulo finitamente gerado. Então G é finito, S é uma extensão galoisiana de R com grupo de Galois G e G é o grupo de todos os R automorfismos de S.

Demonstração. Sejam $s_1, \ldots, s_r$ geradores de S como R-módulo. Vamos mostrar que $|G| \leq r$.

$S \otimes S$ é gerado como um S módulo por $1 \otimes s_1, \ldots, 1 \otimes s_r$ e é uma S-álgebra separável, como visto no item 1 do Teorema 2.2.4. Se $\sigma_1, \ldots, \sigma_n$ são elementos distintos de G, defina os seguintes homomorfismos de S-álgebras:

$$f_i : S \otimes S \to S,\ f_i = k(1 \otimes \sigma_i)$$

com $k(s_1 \otimes s_2) = s_1 s_2$. Como S não tem idempotentes além de 0 e 1, f_i são fortemente distintos, satisfazendo o Lema 2.2.2, logo existem idempotentes $e_1, \ldots, e_n$ em $S \otimes S$ com $f_i(e_i) = 1$ e $f_i(x)e_i = xe_i$, para qualquer $x \in S \otimes S$. Logo a restrição de f_i em $(S \otimes S)e_i$ é um isomorfismo de S-módulos entre $(S \otimes S)e_i$ e S.

Se $e = 1 - e_1 - \cdots - e_n$, então

$$S \otimes S = (S \otimes S)e \oplus \bigoplus_{i=1}^{n} (S \otimes S)\, e_i$$

como S-módulos. Portanto, $S \otimes S$ possui um somando direto que é um S-módulo livre de dimensão n.

Se p é um ideal maximal qualquer de S, então n é menor do que a dimensão do espaço vetorial $(S \otimes S)/p(S \otimes S)$ sobre S/p, que é menor ou igual a r, pois r é o número de geradores de $S \otimes S$ sobre S. Logo, G é finito.

Pelo Teorema 2.2.4, S é uma extensão galoisiana de R com grupo de Galois G, e pelo corolário acima, G é o grupo de todos os R-automorfismos de S. □

2.5 Localização e Bases Normais

Seja $\mathcal{P}$ um ideal primo de R, e M um R-módulo. Denotamos por $M_{\mathcal{P}} = (R \setminus \mathcal{P})^{-1}M$ a localização de M com respeito a $\mathcal{P}$, como na página 24.

Em [5], Bourbaki define que um R-módulo projetivo S é de posto n se é finitamente gerado e se $S_{\mathcal{P}}$ é um $R_{\mathcal{P}}$-módulo de posto n, para todo ideal primo $\mathcal{P}$ de R. Denotamos por $rank(S) = n$. No caso de R-módulos livres, então R^n é de posto n, de forma análoga a espaços vetoriais.

Lema 2.5.1. *Seja S extensão galoisiana de R com grupo de Galois G, $|G| = n$, e $\mathcal{P}$ um ideal primo de R. Então $S_{\mathcal{P}} \simeq R_{\mathcal{P}} \otimes S$ é um $R_{\mathcal{P}}$-módulo livre de posto n, isto é, S é um R-módulo projetivo de posto n no sentido acima.*

Demonstração. Suponha R um anel local. Então, pelo Teorema 2.2.4 (c) e pelo Corolário 1.2.9, temos que S é um R-módulo livre, de posto m, e $S \otimes S$ é

um R-módulo livre de posto m^2. Por outro lado, o item (e) do Teorema 2.2.4 mostra que $S \otimes S$ é um S-módulo livre de posto n. Logo é um R-módulo livre de posto mn. Assim, $m^2 = mn \Rightarrow n = m$.

Seja R um anel comutativo arbitrário e $\mathcal{P}$ um ideal primo de R. Pelo Lema 2.2.9, $S_{\mathcal{P}} \simeq R_{\mathcal{P}} \otimes S$ é uma extensão de Galois de $R_{\mathcal{P}}$ com grupo de Galois G. Pelo argumento acima, $S_{\mathcal{P}}$ é um $R_{\mathcal{P}}$-módulo livre de posto n. □

Para o Lema a seguir, iremos utilizar um ideal radical – um ideal que pode ser expresso como a intersecção de ideais primos.

Lema 2.5.2. *[18; Lemma 3.14.] Sejam R um anel, J um ideal radical de R e V_1, V_2 R-módulos projetivos finitamente gerados. Seja também $f : V_1/JV_1 \to V_2/JV_2$ um isomorfismo de R-módulos. Então f é induzido por um isomorfismo $V_1 \to V_2$.*

Demonstração. Seja $p_i : V_i \to V_i/JV_i$ a aplicação canônica. Então, fp_1 é um epimorfismo de V_1 em V_2/JV_2. Como V_1 é projetivo, existe $g : V_1 \to V_2$ tal que $p_2 g = fp_1$. Como f e p_1 são epimorfismos, temos que $g(V_1) + JV_2 = V_2$. Mas J é um ideal radical e $V_2/g(V_1)$ é finitamente gerado, logo $V_2/g(V_1) = 0$, então g é um epimorfismo. Como $g(V_1) = V_2$ é projetivo, g cinde e $\ker g$ é somando direto de V_1. Isso implica $p_1(\ker g) = \ker g/J \ker g$ e também que $\ker g$ é finitamente gerado, então $p_1(\ker g) = 0$ somente se $\ker g = 0$. Mas $fp_1(\ker g) = p_2 g(\ker g) = 0$ e f é um isomorfismo, então $\ker g = 0$ de fato, logo g é um isomorfismo. □

Nosso objetivo é caracterizar os anéis de grupos de extensões galoisianas. Para isso, precisaremos do Teorema de Krull-Schmidt, que garante que um módulo não-nulo de comprimento finito pode ser decomposto como uma soma direta de partes indecomponíveis.

Teorema (Krull-Schmidt)**.** *[2; Theorem 12.9, p.147] Seja M um módulo não-nulo de comprimento finito. Então M tem uma decomposição finita em elementos indecomponíveis*

$$M = M_1 \oplus \cdots \oplus M_n$$

que é única, exceto por permutações e isomorfismos.

Em especial, o Teorema 2.5.3 traz um isomorfismo entre $R(G)$ e S como $R(G)$-módulos quando R é um anel semi-local, isto é, R possui um número finito de ideais maximais.

Dizemos que uma extensão galoisiana S de R tem base normal se existe $s \in S$ tal que $\{\sigma(s) \mid \sigma \in G\}$ forma uma base para S.

Teorema 2.5.3. *Seja S extensão galoisiana de R com grupo de Galois G. Sejam $R(G)$ e $S(G)$ os anéis de grupo de G sobre R e S, respectivamente. Vejamos S e $S \otimes S$ como $R(G)$ e $S(G)$-módulos, respectivamente, pelas ações a seguir:*

$$(r\sigma)(s) = r\sigma(s)$$
$$s\sigma(s_1 \otimes s_2) = ss_1 \otimes \sigma(s_2)$$

Então, temos que

1. *$S \otimes S \simeq S(G) \simeq S \otimes R(G)$ como $S(G)$-módulo e S é um $R(G)$-módulo projetivo.*

2. *Se S é um R-módulo livre e $|G| = n$, então a soma direta de n cópias de S é $R(G)$-isomorfa a soma direta de n-cópias de $R(G)$.*

3. *Se R é um anel semi-local, então $S \simeq R(G)$ como $R(G)$-módulo, isto é, S possui uma base normal.*

Demonstração. A S-álgebra E, das funções de G em S, é um G-módulo pela ação

$$(\sigma v)(\tau) = v(\tau\sigma)$$

e portanto, a aplicação

$$\begin{aligned} \gamma : E &\to S(G) \\ v &\mapsto \sum_{\sigma \in G} v(\sigma)\sigma^{-1} \end{aligned}$$

é um $S(G)$-isomorfismo de E em $S(G)$:

$$\begin{aligned} & \gamma(v) = 0 \\ & \textstyle\sum_{\sigma\in G} v(\sigma)\sigma^{-1} = 0 \\ \Rightarrow \quad & v(\sigma) = 0, \quad \forall \sigma \in G \\ \Rightarrow \quad & v = 0 \end{aligned}$$

Seja agora $\alpha = \sum_{\sigma\in G} a_\sigma \sigma^{-1} \in S(G)$. Temos então que existe $v \in E$, $v = \sum_{\sigma\in G} a_\sigma v_{\sigma^{-1}}$, tal que

$$\begin{aligned} \gamma(v) &= \gamma\left(\sum_{\sigma\in G} a_\sigma v_{\sigma^{-1}}\right) \\ &= \sum_{\rho,\sigma\in G} \left(a_\sigma v_{\sigma^{-1}}(\rho)\rho^{-1}\right) \\ &= \sum_{\rho\in G} a_\rho \rho^{-1} = \alpha \end{aligned}$$

Porém, com a estrutura de $S(G)$-módulo definida em $S\otimes S$, temos que h se torna um isomorfismo de $S(G)$-módulos entre E e $S\otimes S$, com $h(s_1\otimes s_2)(\sigma) = s_1\sigma(s_2)$. Assim, se $h(s_1\otimes s_2) = 0$, temos que $s_1\sigma(s_2) = 0$, para todo $\sigma \in G$. Assim $s_1 s_2 = 0$. Seguem então os isomorfismos $S \otimes S \simeq S(G) \simeq S \otimes R(G)$. Como S é um R-módulo projetivo, $S \otimes S$ é um $R(G)$-módulo projetivo. Mas pelo Lema 2.2.7, S é um $R(G)$-somando direto de $S \otimes S$ e portanto, é um $R(G)$-módulo projetivo, provando (1).

Se S é um R-módulo livre, segue do Lema 2.5.1 que S tem rank n. Então $S \otimes S$ é $R(G)$-isomorfo a soma direta de n cópias de S. Por outro lado, $S(G) \simeq S \otimes R(G)$ é $R(G)$-isomorfo a soma direta de n cópias de $R(G)$. A partir de (1), provamos (2).

Seja agora J o radical de Jacobson de R – a intersecção (finita) de todos os ideais maximais, e tomemos $R' = R/J$. Então R' e $R'(G)$ são anéis com a condição mínima para o teorema de Krull-Schmidt.

Agora, $S' = S/JS \simeq R' \otimes S$ e portanto, pelo Lema 2.2.9, S' é uma extensão galoisiana de R' com grupo de Galois G. Como R' é soma direta de um número finito de corpos, pelo Lema 2.5.1 mostra que S' é um R'-módulo

projetivo de rank $n = |G|$. Então, por (2) e pelo Teorema de Krull-Schmidt, S' é $R'(G)$-isomorfa a $R'(G)$. Além disso, $R'(G) \simeq R' \otimes R(G) \simeq R(G)/JR(G)$ e $JR(G)$ é o radical de Jacobson de $R(G)$. Portanto, os $R(G)$-módulos projetivos S e $R(G)$ são isomorfos módulo $JR(G)$. Portanto, eles são $R(G)$-módulos isomorfos, pelo Lema 2.5.2 $\square$

Capítulo 3

Cohomologia de Galois

O Capítulo 3 está destinado ao estudo da cohomologia galoisiana [7; §5]. Os resultados são desenvolvidos na seção 3.2 deste capítulo, apresentando a generalização de dois resultados importantes: o Teorema 90 de Hilbert e o isomorfismo entre o grupo de Brauer e o segundo grupo de cohomologia.

Na primeira seção, temos a construção do grupo de Brauer para anéis comutativos, apresentada inicialmente por Auslander e Goldman em [4]. Esta construção é bastante sucinta, com objetivo de compreender os resultados apresentados na segunda seção acerca do grupo de Brauer.

3.1 Grupo de Brauer

O grupo de Brauer é inicialmente definido sobre corpos. Ele consiste de classes de equivalência de álgebras simples centrais de dimensão finita. O Teorema de Wedderburn, enunciado a seguir, permite definir uma relação de equivalência entre as álgebras A_1, A_2 com base nas álgebras de divisão D_1, D_2.

Sejam R um anel comutativo com unidade e A uma R-álgebra, não necessariamente comutativa. Denotamos por $C(A)$ o centro de A, definido por $C(A) = \{x \in A \mid ax = xa, \forall a \in A\}$. Se $C(A) = R$, então A é uma R-álgebra central. Observe que $\mathbb{C}$ é uma $\mathbb{R}$-álgebra que não é central, pois $C(\mathbb{C}) = \mathbb{C}$, e

não $\mathbb{R}$. Por outro lado, o conjunto $\mathbb{H}$ dos quatérnios é uma $\mathbb{R}$-álgebra central.

Teorema 3.1.1 (Wedderburn)**.** *[17; Theorem 1] Sejam K um corpo e A uma K-álgebra simples de dimensão finita. Então existe um único $n \in N$ e uma única K-álgebra de divisão D (a menos de isomorfismos), tal que*

$$A \simeq M_n(D).$$

Por outro lado, qualquer álgebra da forma $M_n(D)$, onde D é uma álgebra de divisão, é simples.

Dizemos que duas K-álgebras simples centrais $A_1 \simeq M_{n_1}(D_1)$ e $A_2 \simeq M_{n_2}(D_2)$ são similares, denotado por $A_1 \sim A_2$, se $D_1 \simeq D_2$. Claramente, $\sim$ é uma relação de equivalência. Dada uma K-álgebra simples central de dimensão finita A, denotamos a classe de equivalência de A por $[A]$, e o grupo de Brauer $Br(K)$ é a coleção destas classes, com produto definido por

$$[A][B] = [A \otimes_K B].$$

Para verificar que $Br(K)$ é de fato um grupo abeliano, utiliza-se as propriedades do produto tensorial, que garantem que o produto definido acima é associativo e comutativo. Além disso, mostra-se que a operação está bem-definida, possui elemento neutro e que cada elemento não nulo possui inverso – $[M_n(K)]$ e $[A^o]$, respectivamente. Caso seja interesse do leitor, sugerimos [11]. Nesta seção, estamos interessados em detalhar a construção do grupo de Brauer de um anel.

A construção a seguir, realizada por Auslander e Goldman, coincide com o grupo de Brauer $Br(R)$ quando o anel R é um corpo e, por analogia, é nomeado grupo de Brauer do anel R, e também denotado por $Br(R)$.

O grupo de Brauer $Br(R)$ de um anel comutativo R é definido sobre classes de equivalência de R-álgebras centrais e separáveis, chamadas R-álgebras de Azumaya. Detalharemos a relação de equivalência na sequência do texto. Para definirmos a operação de $Br(R)$, além de determinarmos suas propriedades, vamos seguir a construção apresentada em [4].

Sejam $\mathcal{A}(R)$ o conjunto das classes de equivalência das R-álgebras de Azumaya com respeito a isomorfismo, isto é, uma classe $[S] \in \mathcal{A}(R)$ é formada por R-álgebras de Azumaya isomorfas, e $\mathcal{A}_0(R)$ o subconjunto que consiste das R-álgebras da forma $\mathrm{Hom}_R(E, E)$, onde E é um R-módulo projetivo finitamente gerado e fiel. As proposições a seguir, encontradas em [4], mostram que $\mathcal{A}(R)$ e $\mathcal{A}_0(R)$ são conjuntos fechados com respeito ao produto tensorial.

Proposição 3.1.2. *Sejam R_1 e R_2 R-álgebras comutativas, A_1 uma R_1-álgebra separável e A_2 uma R_2-álgebra separável. Então $A_1 \otimes_R A_2$ é igual a 0 ou é uma $R_1 \otimes_R R_2$-álgebra separável. Além disso o centro de $A_1 \otimes_R A_2$ é $C(A_1) \otimes_R C(A_2)$.*

Demonstração. Seja $S = A_1 \otimes_R A_2$, não nula. Então $S^e = S \otimes_{R_1 \otimes R_2} S^o = A_1^e \otimes_R A_2^e$. Pelo Teorema 2.1.7, as aplicações $\mu_i : A_i^e \to A_i$ cindem, e portanto a aplicação $\mu : S^e \to S$ também cinde. Assim, S é uma $R_1 \otimes R_2$-álgebra separável. Em particular, se g_i é a inversa de μ_i, então $g = g_1 \otimes_R g_2$ é a inversa de μ. Então $C(A_i) = \mu_i(g_i(1)A_i^e)$, logo $C(S)$ é $\mu(g(1)S^e) = C(A_1) \otimes C(A_2)$. □

Seja A um R-módulo. Definimos o anulador de A por $ann(A) = \{x \in R \mid xA = 0\} \subset R$. Observe que o anulador é um ideal de R.

Proposição 3.1.3. *[4; Proposition 5.1.] Seja R um anel comutativo.*

1. *Se E é um R-módulo projetivo finitamente gerado tal que $ann(E) \subset R$, então $Hom_R(E, E)$ é separável sobre R e seu centro é $R/ann(E)$;*

2. *Se E' é outro R-módulo projetivo finitamente gerado, então $E \otimes_R E'$ é um R-módulo projetivo finitamente gerado e $Hom_R(E \otimes E', E \otimes E') \simeq Hom_R(E, E) \otimes_R Hom_R(E', E')$.*

3. *Se E e E' são fieis, então $E \otimes E'$ também é fiel.*

Vamos introduzir uma relação de equivalência sobre $\mathcal{A}(R)$, onde $A_1 \sim A_2$ se existem álgebras $\Omega_1, \Omega_2 \in \mathcal{A}_0(R)$ tais que

$$A_1 \otimes_R \Omega_1 \simeq A_2 \otimes_R \Omega_2.$$

Pelas Proposições 3.1.2 e 3.1.3, temos que a relação de equivalência está bem-definida, e é compatível com a operação de produto tensorial. Assim, podemos considerar o conjunto das classes

$$Br(R) = \mathcal{A}(R)/\sim.$$

Claramente, a classe $[R]$ é o elemento neutro de $Br(R)$. O Teorema a seguir mostra que a classe da álgebra oposta de A, $[A^o]$, é o inverso da classe $[A]$.

Teorema 3.1.4. *[4; Theorem 2.1.] Se A é uma álgebra sobre $C = C(A)$, então são equivalentes as seguintes afirmações:*

1. *A é uma C-álgebra separável;*
2. *$A^e Hom_{A^e}(A, A^e) \simeq A^e$;*
3. *A aplicação $\eta : A^e \to Hom_C(A, A)$ dada por $\eta(x \otimes y)(z) = xzy$ é um isomorfismo e A é um C-módulo projetivo finitamente gerado;*
4. *A aplicação η (como acima) é um isomorfismo e C é um somando direto de A, enquanto C-módulo.*

Assim, como A é um R-módulo projetivo finitamente gerado e fiel, temos $[A][A^o] = [A^e] = [\mathrm{Hom}_R(A, A)] = [R]$. O Corolário 1.3. de [4] afirma que se A é R-separável e I é um ideal em C, então $IA \cap C(A) = I$, e nos permite mostrar que A é fiel. Tomando o anulador de A, $ann(A) \subset C(A)$, temos que $ann(A)A \cap C(A) = ann(A)$. Mas $ann(A)A = 0$, portanto $ann(A) = 0$ e A é fiel. Logo $Br(R)$ é, de fato, um grupo abeliano.

Retornando ao grupo de Brauer de um corpo, vamos observar extensões de corpos. Seja $L\,|_K$ uma extensão de corpos e A uma K-álgebra simples central. Definimos $A_L = A \otimes_K L$. Dizemos que L é um corpo de fatoração para A se A_L e $M_n(L)$ são L-álgebras isomorfas. Se L é uma álgebra de fatoração para A, então também será para qualquer álgebra similar a A. As classes de álgebras que se fatoram sobre uma extensão $L\,|_K$ formam um subgrupo de $Br(K)$ que é chamado grupo de Brauer relativo à extensão $L\,|_K$, denotado por $Br(L/K)$.

Para verificar que $Br(L/K)$ é de fato um subgrupo de $Br(K)$, precisamos observar que isso segue do fato de que se A é uma K-álgebra simples central e A_L é uma L-álgebra simples central, então a correspondência $[A] \mapsto [A_L]$ determina uma aplicação $\iota_{L/K} : Br(K) \to Br(L)$. Além disso, existe um isomorfismo de L-álgebras

$$(A \otimes_K B) \otimes_K L \simeq (A \otimes_K L) \otimes_L (B \otimes_K L)$$

que mostra que $\iota_{L/K}$ é um homomorfismo de grupos. Temos, então, que $Br(L/K)$ é justamente o núcleo de $\iota_{L/K}$.

Vamos retornar agora ao caso de anéis, e observar as extensões de anéis e as álgebras de Azumaya. Seja S uma R-álgebra comutativa. Pela proposição a seguir, a aplicação $A \mapsto S \otimes_R A$ induz uma aplicação de $\mathcal{A}(R)$ em $\mathcal{A}(S)$ que leva $\mathcal{A}_0(R)$ em $\mathcal{A}_0(S)$.

Proposição 3.1.5. *[4; Proposition 5.5.] Sejam E um R-módulo projetivo finitamente gerado e S uma R-álgebra comutativa. Então:*

1. *$S \otimes_R E$ é um S-módulo projetivo finitamente gerado;*
2. *$Hom_S(S \otimes_R E, S \otimes_R E) \simeq S \otimes_R Hom_R(E, E)$;*
3. *Se E é um R-módulo fiel, então $S \otimes_R E$ é um S-módulo fiel.*

Esta aplicação, que leva $[A] \mapsto [S \otimes_R A]$, induz um homomorfismo de $Br(R)$ em $Br(S)$ para qualquer R-álgebra comutativa S. Em particular, se $f : R \to S$ é um homomorfismo de anéis, então podemos ver S como R-álgebra e portanto existe um homomorfismo induzido $Br(f) : Br(R) \to Br(S)$. Isso mostra que $Br(\cdot)$ é um funtor covariante da categoria de anéis comutativos para a categoria de grupos abelianos.

Seja $f : R \to S$ um homomorfismo de anéis comutativos. Então, o núcleo de $Br(f) : Br(R) \to Br(S)$ é formado pelas classes de R-álgebras A que satisfazem

$$S \otimes_R A \simeq \mathrm{Hom}_S(M, M)$$

para algum S-módulo projetivo finitamente gerado e fiel M. Neste caso, S fatora A, e o núcleo de $Br(f)$ é denotado $Br(S/R)$, chamado de grupo de Brauer das R-álgebras de Azumaya que se fatoram por S.

Vejamos um exemplo de grupo de Brauer. Seja K um corpo algebricamente fechado, e D uma K-álgebra de divisão de dimensão finita. Tomemos $d \in D$. Como D tem dimensão finita sobre K, os elementos $1, d, d^2, \ldots$ são linearmente depentendes, e portanto d satisfaz um polinômio minimal $f \in K[x]$, irredutível sobre K; porém, como K é algebricamente fechado, temos que $d \in K$. Assim, $D \subset K$ e portanto, $D = K$. Assim, pelo Teorema de Wedderburn, temos que todas as K-álgebras simples centrais são isomorfas a $M_n(K)$, para algum $n \in \mathbb{N}$. Desta forma, temos que o grupo $Br(K)$ é trivial.

Outro exemplo que podemos ver é o grupo de Brauer do corpo $\mathbb{R}$ dos números reais. Pelo Teorema de Frobenius [8; Theorem 3.2.3., p.16], temos que as únicas $\mathbb{R}$-álgebras de divisão são $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$, e $\mathbb{C}$ não é uma $\mathbb{R}$-álgebra central. Vamos observar o homomorfismo de $\mathbb{R}$-álgebras $\phi : \mathbb{H} \to \mathbb{H}^o$ dado por

$$\phi(a + bi + cj + dk) = a - bi - cj - dk.$$

Claramente, ϕ é um isomorfismo. Desta forma, temos que $\mathbb{H} \simeq \mathbb{H}^o$, e portanto $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^o \simeq \mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$. Assim, temos que o único elemento não nulo em $Br(\mathbb{R})$, a classe $[\mathbb{H}]$, satisfaz $[\mathbb{H}]^2 = [\mathbb{R}]$. Assim, temos que $Br(\mathbb{R}) = \mathbb{Z}_2$. Em [8], Chen desenvolve os requisitos necessários para o estudo do grupo de Brauer de corpos locais, com objetivo de determinar o grupo $Br(\mathbb{Q})$, a saber

$$Br(\mathbb{Q}) = \left\{ (a, x) \mid a \in \left\{0, \frac{1}{2}\right\}, x \in \bigoplus_p \mathbb{Q}/\mathbb{Z} \text{ e } a + \sum x_p = 0 \right\}.$$

Seja S um anel e R um subanel de S. Dizemos que um elemento $x \in S$ é integral sobre R se existe $a_0, \ldots, a_{n-1} \in R$ tais que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, ou seja, $x \in S$ é raiz de um polinômio mônico com coeficientes em R [10; p.43, Definição 2.1.1]. Se K é uma extensão finita de $\mathbb{Q}$, chamamos de anel de inteiros de K ao conjunto dos elementos de K que são integrais sobre $\mathbb{Z}$ [10; p.66].

Em 1971, Morris desenvolveu, utilizando a sequência (3.8), apresentada na seção seguinte, obtida por Chase e Rosenberg em [6], o teorema a seguir.

Teorema. *[14; Theorem 5.0] Sejam $K = \mathbb{Q}(\sqrt{m})$ com m um inteiro sem fatores quadráticos e S o anel de inteiros de K. Então o grupo de Brauer $Br(S/\mathbb{Z})$ é trivial quando $m = -3, -1, 2, 3$ ou 5.*

3.2 Cohomologia Galoisiana

A teoria de cohomologia foi introduzida em uma conferência internacional em Moscou, em 1935. James Alexander e Andrey Kolmogoroff desenvolveram, separados, resultados muito semelhantes. Ambos trouxeram uma operação associativa e anticomutativa nos grupos de cohomologia.

Para compreendermos os resultados que serão apresentados neste capítulo, originalmente apresentados por Chase, Harrison, e Rosenberg em [7; §5], vamos precisar saber um pouco mais de cohomologia. Para isso, vamos utilizar a construção apresentada por Lima em [13; p.51], motivada por Harper em [12].

Sejam G um grupo, A um G-módulo, isto é, A é um grupo abeliano (aditivo) com uma ação de $\mathbb{Z}G$, e $n \in \mathbb{N}$. Uma n-cocadeia de G sobre A é uma função $f : G^n \to A$, onde $G^n = G \times \cdots \times G$ se $n > 0$, ou um elemento de A, se $n = 0$. Denotamos por $C^n(G, A)$ o conjunto das n-cocadeias de G sobre A. Note que $C^n(G, A)$ é um grupo abeliano com a operação de adição.

A partir de uma n-cocadeia f, definimos o homomorfismo de grupos abelianos $\delta : C^n(G, A) \to C^{n+1}(G, A)$, chamado cobordo, que determina uma $(n+1)$-cocadeia δf, definida por

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

Por exemplo, seja f uma 3-cocadeia. Então δf será a 4-cocadeia dada por

$$\begin{aligned}\delta f(\sigma_1,\ldots,\sigma_4) = \sigma_1 f(\sigma_2,\sigma_3,\sigma_4) &- f(\sigma_1\sigma_2,\sigma_3,\sigma_4)\\ &+ f(\sigma_1,\sigma_2\sigma_3,\sigma_4)\\ &- f(\sigma_1,\sigma_2,\sigma_3\sigma_4)\\ &+ f(\sigma_1,\sigma_2,\sigma_3).\end{aligned}$$

Temos que δ é um homomorfismo de G-módulos e $\delta\delta f = 0$. A demonstração pode ser encontrada em [13; p.52].

Uma sequência de grupos abelianos e homomorfismos

$$\cdots \to G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \to \cdots$$

em que os homomorfismos satisfazem $f_i \circ f_{i-1} = 0$ é chamada cocadeia complexa.

Sejam $Z^n(G,A) = \ker\delta \subseteq C^n(G,A)$ e $B^n(G,A) = \delta(C^{n-1}(G,A))$, se $n > 0$, e $B^0(G,A) = 0$. Chamamos $f \in Z^n(G,A)$ de n-cociclo e, para $f' \in C^{n-1}(G,A)$, $\delta f' \in B^n(G,A)$ de n-cobordo.

Como $\delta\delta = 0$, temos

$$B^n(G,A) \subseteq Z^n(G,A) \subset G^n(G,A)$$

e, como $C^n(G,A)$ é um grupo abeliano, seus subgrupos são normais. Assim, podemos definir o quociente

$$H^n(G,A) = \frac{Z^n(G,A)}{B^n(G,A)},$$

chamado de n-ésimo grupo de cohomologia de G sobre A.

Os resultados da seção 5 de [7] são uma generalização de dois grandes resultados da teoria de Galois clássica. O primeiro deles é o Teorema 90 de Hilbert:

Teorema (Teorema 90 de Hilbert)**.** *Seja $L\,|_K$ uma extensão galoisiana de corpos com grupo de Galois G, não necessariamente finita, e seja $U(L)$ o grupo multiplicativo de L. Então*

$$H^1\left(G,U(L)\right) = 0,$$

isto é, o primeiro grupo de cohomologia de G sobre o grupo multiplicativo de L é trivial.

O outro resultado é referente ao segundo grupo de cohomologia do grupo de Galois, onde se prova que este é isomorfo ao grupo de Brauer. Na seção 3.1 temos a construção do grupo de Brauer, além de alguns resultados de Auslander e Goldman [4].

Iniciaremos agora o desenvolvimento dos resultados obtidos por Chase, Harrison, e Rosenberg, a partir da construção realizada por Amitsur em [1].

Sejam R um anel comutativo, T uma R-álgebra comutativa e T^n o produto tensorial de T sobre R com n fatores, representado por $T \otimes_R \cdots \otimes_R T$. Sejam $\varepsilon_i : T^{n+1} \to T^{n+2}$ os homomorfismos de R-álgebras definidos por

$$\varepsilon_i(t_0 \otimes \cdots \otimes t_n) = t_0 \otimes \cdots \otimes t_{i-1} \otimes 1 \otimes t_i \otimes \cdots \otimes t_n$$

Lema 3.2.1. *Sejam S extensão galoisiana de R com grupo de Galois G, E^n a S-álgebra das funções de n variáveis de G em S e $S^{n+1} = S \otimes \cdots \otimes S$ uma S-álgebra, com S agindo no primeiro fator.*

Então $h_n : S^{n+1} \to E^n$ definido por

$$h_n(s_0 \otimes \cdots \otimes s_n)(\sigma_1, \ldots, \sigma_n) = s_0 \left(\sigma_1(s_1)\right) \left(\sigma_1\sigma_2(s_2)\right) \cdots \left(\sigma_1 \cdots \sigma_n(s_n)\right)$$

é um isomorfismo de S-álgebras.

Demonstração. Sejam $r \in S$, $s, s' \in S^{n+1}$, $s = s_0 \otimes \cdots \otimes s_n$ e $s' = s'_0 \otimes \cdots \otimes s'_n$, e $\sigma = (\sigma_1, \ldots, \sigma_n) \in G^n$. Mostremos que h_n é um S-homomorfismo:

- $$\begin{aligned} r \cdot h_n(s)(\sigma) &= r\left(s_0 \cdots (\sigma_1 \cdots \sigma_n(s_n))\right) \\ &= (rs_0) \cdots (\sigma_1 \cdots \sigma_n(s_n)) \\ &= h_n(rs_0 \otimes \cdots \otimes s_n)(\sigma) \\ &= h_n(r \cdot s)(\sigma) \end{aligned}$$

- $$\begin{aligned} h_n(s)h_n(s')(\sigma) &= \left(s_0 \cdots (\sigma_1 \cdots \sigma_n(s_n))\right)\left(s'_0 \cdots (\sigma_1 \cdots \sigma_n(s'_n))\right) \\ &= (s_0 s'_0) \cdots (\sigma_1 \cdots \sigma_n(s_n s'_n)) \\ &= h_n(s_0 s'_0 \otimes \cdots \otimes s_n s'_n)(\sigma) \\ &= h_n(s \cdot s')(\sigma) \end{aligned}$$

Além disso, pelo Teorema 2.2.4, h_1 é um isomorfismo. Suponha agora que h_{n-1} é um isomorfismo. Vamos mostrar que h_n é um isomorfismo, por indução em n.

Como h_{n-1} é um isomorfismo, temos que

$$S^{n+1} \simeq S \otimes S^n \simeq S \otimes E^{n-1}$$

onde o segundo isomorfismo é dado por $1 \otimes h_{n-1}$. Agora, tome a ação de G em E^n dada por

$$(\sigma f)(\sigma_1, \ldots, \sigma_n) = \sigma \left(f(\sigma^{-1}\sigma_1, \sigma_2, \ldots, \sigma_n) \right)$$

Tomemos D o S-módulo livre com geradores δ_σ, $\sigma \in G$, como definido na página 36. Temos então que E^n é um D-módulo, tomando a ação $\delta_\sigma f = \sigma f$. Assim, $(E^n)^G$ é o conjunto das funções $f \in E^n$ tais que

$$\sigma(f(\sigma_1, \ldots, \sigma_n)) = f(\sigma\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Defina então $\psi : E^{n-1} \to (E^n)^G$ por

$$(\psi g)(\sigma_1, \ldots, \sigma_n) = \sigma_1(g(\sigma_2, \ldots, \sigma_n)),$$

para qualquer $g \in E^{n-1}$. Temos que ψ é um isomorfismo de R-álgebras, com inversa

$$(\psi^{-1} f)(\sigma_2, \ldots, \sigma_n) = f(1, \sigma_2, \ldots, \sigma_n)$$

Logo, $1 \otimes \psi : S \otimes E^{n-1} \to S \otimes (E^n)^G$ é um isomorfismo de S-álgebras.

Pelo Teorema 2.2.4, $\omega : S \otimes (E^n)^G \to E^n$, definido por $\omega(s \otimes f) = sf$ é um isomorfismo de S-álgebras. Assim, temos

$$
\begin{aligned}
&\omega(1\otimes\psi)(1\otimes h_{n-1})(s_0\otimes\cdots\otimes s_n)(\sigma_1,\ldots,\sigma_n)\\
&=\omega(1\otimes\psi)(s_0\otimes h_{n-1}(s_1\otimes\cdots\otimes s_n)(\sigma_1,\ldots,\sigma_n))\\
&=\omega\left(s_0\otimes\sigma_1 h_{n-1}(s_1\otimes\cdots\otimes s_n)(\sigma_2,\ldots,\sigma_n)\right)\\
&=\omega\left(s_0\otimes\sigma_1\left(s_1\sigma_2(s_2)\cdots\sigma_2\cdots\sigma_n(s_n)\right)\right)\\
&=s_0\sigma_1\left(s_1\sigma_2(s_2)\cdots(\sigma_2\cdots\sigma_n)(s_n)\right)\\
&=s_0\sigma_1(s_1)\cdots(\sigma_1\cdots\sigma_n)(s_n)\\
&=h_n(s_0\otimes\cdots\otimes s_n)(\sigma_1,\ldots,\sigma_n).
\end{aligned}
$$

Portanto, $\omega(1\otimes\psi)(1\otimes h_{n-1})=h_n$ é um isomorfismo de S-álgebras. □

Definimos então, com S extensão galoisiana de R com grupo de Galois G, e E^n a S-álgebra das funções de n variáveis de G em S, os homomorfismos de R-álgebras $\theta_i : E^n \to E^{n+1}$, onde

$$
\begin{aligned}
(\theta_0 f)(\sigma_1,\ldots,\sigma_{n+1}) &= \sigma_1 f(\sigma_2,\ldots,\sigma_{n+1})\\
(\theta_i f)(\sigma_1,\ldots,\sigma_{n+1}) &= f(\sigma_1,\ldots,\sigma_i\sigma_{i+1},\ldots,\sigma_{n+1}),\ (1\le i\le n)\\
(\theta_{n+1} f)(\sigma_1,\ldots,\sigma_{n+1}) &= f(\sigma_1,\ldots,\sigma_n)
\end{aligned}
$$

Vamos mostrar que o diagrama abaixo é comutativo.

$$
\begin{array}{ccc}
S^{n+1} & \xrightarrow{\ h_n\ } & E^n\\
\big\downarrow{\scriptstyle \varepsilon_i} & & \big\downarrow{\scriptstyle \theta_i}\\
S^{n+2} & \xrightarrow{\ h_{n+1}\ } & E^{n+1}
\end{array}
\tag{3.1}
$$

Para $i=0$, o resultado de $\theta_0\circ h_n$ é

$$
\begin{aligned}
&\theta_0(h_n(s_0\otimes\cdots\otimes s_n))(\sigma_1,\ldots,\sigma_{n+1})\\
=\ &\sigma_1(h_n(s_0\otimes\cdots\otimes s_n)(\sigma_2,\ldots,\sigma_{n+1}))\\
=\ &\sigma_1\left(s_0\sigma_2(s_1)\cdots(\sigma_2\cdots\sigma_{n+1})(s_n)\right)\\
=\ &\sigma_1(s_0)\sigma_1\sigma_2(s_1)\cdots(\sigma_1\cdots\sigma_{n+1})(s_n),
\end{aligned}
\tag{3.2}
$$

enquanto para $h_{n+1} \circ \varepsilon_0$ temos

$$\begin{aligned} & h_{n+1}(\varepsilon_0(s_0 \otimes \cdots \otimes s_n))(\sigma_1, \ldots, \sigma_{n+1}) \\ = \; & h_{n+1}(1 \otimes s_0 \otimes \cdots \otimes s_n)(\sigma_1, \ldots, \sigma_{n+1}) \\ = \; & 1\sigma_1(s_0)\sigma_1\sigma_2(s_1) \cdots (\sigma_1 \cdots \sigma_{n+1})(s_n). \end{aligned} \tag{3.3}$$

Assim, pelas equações (3.2) e (3.3), temos que o diagrama é comutativo para $i = 0$. Para $1 \leq i \leq n$ temos

$$\begin{aligned} & \theta_i(h_n(s_0 \otimes \cdots \otimes s_n))(\sigma_1, \ldots, \sigma_{n+1}) \\ = \; & h_n(s_0 \otimes \cdots \otimes s_n)(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{n+1}) \\ = \; & s_0 \cdots (\sigma_1 \cdots \sigma_i\sigma_{i+1})(s_i) \cdots (\sigma_1 \cdots \sigma_{n+1})(s_n), \end{aligned} \tag{3.4}$$

enquanto pelo outro lado

$$\begin{aligned} & h_{n+1}(\varepsilon_i(s_0 \otimes \cdots \otimes s_n))(\sigma_1, \ldots, \sigma_{n+1}) \\ = \; & h_{n+1}((s_0 \otimes \cdots \otimes 1 \otimes s_i \otimes \cdots \otimes s_n))(\sigma_1, \ldots, \sigma_{n+1}) \\ = \; & s_0 \cdots (\sigma_1 \cdots \sigma_i)(1)(\sigma_1 \cdots \sigma_{i+1})(s_i) \cdots (\sigma_1 \cdots \sigma_{n+1})(s_n). \end{aligned} \tag{3.5}$$

Logo, pelas equações (3.4) e (3.5), temos que o diagrama é comutativo para todo $i \leq n$. Falta apenas verificar para $i = n + 1$:

$$\begin{aligned} & \theta_{n+1}(h_n(s_0 \otimes \cdots \otimes s_n))(\sigma_1, \ldots, \sigma_{n+1}) \\ = \; & h_n(s_0 \otimes \cdots \otimes s_n)(\sigma_1, \ldots, \sigma_n) \\ = \; & s_0 \cdots (\sigma_1 \cdots \sigma_n)(s_n) \end{aligned} \tag{3.6}$$

por um lado, e por outro

$$\begin{aligned} & h_{n+1}(\varepsilon_{n+1}(s_0 \otimes \cdots \otimes s_n)) \\ = \; & h_{n+1}(s_0 \otimes \cdots \otimes s_n \otimes 1)(\sigma_1, \ldots, \sigma_{n+1}) \\ = \; & s_0 \cdots (\sigma_1 \cdots \sigma_n)(s_n)(\sigma_1 \cdots \sigma_{n+1})(1) \end{aligned} \tag{3.7}$$

Assim, como consequência das equações (3.2)-(3.7), segue que o diagrama (3.1) é comutativo.

Agora, sejam F um funtor covariante da categoria de R-álgebras comutativas para a categoria de grupos abelianos e T uma R-álgebra comutativa. Definimos uma cocadeia complexa $C(T/R, F)$ por $C^n(T/R, F) =$

$F(T^{n+1})$, com cobordo $\Delta^n : C^n(T/R, F) \to C^{n+1}(T/R, F)$, dado por $\Delta^n = \sum_{i=0}^{n+1}(-1)^i F(\varepsilon_i)$.

$$\cdots \xrightarrow{\Delta^{n-2}} F(T^n) \xrightarrow{\Delta^{n-1}} F(T^{n+1}) \xrightarrow{\Delta^n} F(T^{n+2}) \cdots$$

Denotamos por $B^n(T/R, F)$ os n-cobordos e por $Z^n(T/R, F)$ os n-cociclos desta cocadeia complexa. Então o n-ésimo grupo de cohomologia desta cocadeia complexa, denotado por

$$H^n(T/R, F) := \frac{Z^n(T/R, F)}{B^n(T/R, F)},$$

é chamado n-ésimo grupo de cohomologia de Amitsur de T/R com valores em F.

Para obtermos o principal resultado da seção 5 de [7], uma sequência exata de sete termos que relaciona o segundo grupo de cohomologia de Amitsur e o grupo de Brauer da extensão galoisiana T sobre R com grupo de Galois G, iremos derivá-la da sequência exata

$$\begin{aligned} 0 \to H^1(S/R, U) \to & P(R) \to H^0(S/R, P) \to H^2(S/R, U) \\ & \to Br(S/R) \to H^1(S/R, P) \to H^3(S/R, U) \end{aligned} \tag{3.8}$$

apresentada em [6]. Para isso, vamos mostrar que no caso de uma extensão galoisiana T de R com grupo de Galois G, temos $H^n(T/R, F) \simeq H^n(G, F(T))$.

Novamente, seja F um funtor covariante da categoria de R-álgebras comutativas para a categoria de grupos abelianos. Se J é um conjunto finito, seja S_j uma R-álgebra comutativa, para cada $j \in J$. Assim, as projeções

$$p_i : \bigoplus_{j \in J} S_j \to S_i$$

determinam homomorfismos $F(p_i) : F\left(\bigoplus_{j \in J} S_j\right) \to F(S_i)$, que por sua vez dão origem a um homomorfismo

$$\varphi_J : F\left(\bigoplus_{j \in J} S_j\right) \to \bigoplus_{j \in J} F(S_j)$$

definido por

$$(\varphi_J)(x) = \sum_{i \in J} F(p_i)(x)$$

para $x \in F\left(\bigoplus_{j \in J} S_j\right)$. Aqui vemos um elemento do produto direto como uma função do conjunto de índices. Dizemos que F é um funtor aditivo se o homomorfismo φ_J acima é um isomorfismo, qualquer que seja o conjunto finito J.

Agora, tomemos S extensão galoisiana de R com grupo de Galois G e F um funtor aditivo. Seja J o produto cartesiano $G^n = G \times \cdots \times G$, e $S_j = S$, para todo $j \in J$; além disso, denotemos $\bigoplus_{j \in J} F(S_j)$ por E_F^n.

Observe que E_F^n é o conjunto de todas as funções de n variáveis de G, que são representadas no índice j, em $F(S)$. Dessa forma, são exatamente os grupos $C^n(G, F(S))$, grupo das n-cocadeias de G em $F(S)$.

Escrevendo φ_J como φ_n, obtemos o isomorfismo $\varphi_n : F(E^n) \to E_F^n$. O homomorfismo de R-álgebras $\theta_i : E^n \to E^{n+1}$ dá origem a um homomorfismo $\theta_{i,F} : E_F^n \to E_F^{n+1}$ tal que $\varphi_{n+1} F(\theta_i) = \theta_{i,F} \varphi_n$. Além disso, $\theta_{i,F}$ é definido de forma explícita pela fórmula

$$(\theta_{i,F} f)(\sigma_1, \ldots, \sigma_{n+1}) = \begin{cases} \sigma_1 f(\sigma_2, \ldots, \sigma_{n+1}) & \text{para } i = 0 \\ f(\sigma_1, \ldots, \sigma_i \sigma_{i+1}, \ldots, \sigma_{n+1}) & \text{para } 1 \leq i \leq n \\ f(\sigma_1, \ldots, \sigma_n) & \text{para } i = n+1 \end{cases}$$

Assim, se definimos $\delta^n : E_F^n \to E_F^{n+1}$ por $\delta^n = \sum_{i=0}^{n+1} (-1)^i \theta_{i,F}$, temos que os grupos abelianos E_F^n, junto com os homomorfismos δ^n, formam a cocadeia complexa $C(G, F(S))$ do grupo G com coeficientes no G-módulo $F(S)$, como na construção da página 74:

$$\cdots \to E_F^{n-1} \xrightarrow{\delta^{n-1}} E_F^n \xrightarrow{\delta^n} E_F^{n+1} \to \cdots$$

Definição 3.2.2. Sejam $\mathcal{C} = \{G^i, \delta^i\}$ e $\mathcal{C}' = \{H^i, \Delta^i\}$ duas cocadeias complexas. Um homomorfismo de cocadeias complexas $f : \mathcal{C} \to \mathcal{C}'$ é uma sequência de homomorfismos de grupos $f^n : G^n \to H^n$ que satisfaz $\Delta^n f^n = f^{n+1} \delta^n$, de forma que o diagrama abaixo é comutativo, para todo $n \geq 0$.

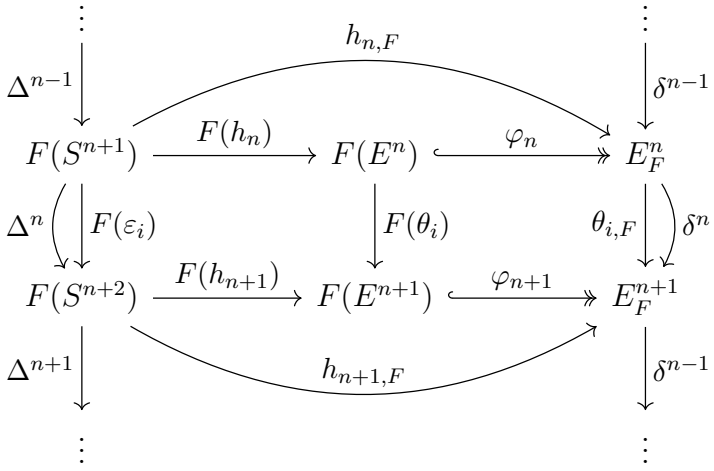
$$\begin{array}{ccccccc} \cdots & \longrightarrow & G^n & \xrightarrow{\delta^n} & G^{n+1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f^n} & & \downarrow{\scriptstyle f^{n+1}} & & \\ \cdots & \longrightarrow & H^n & \xrightarrow{\Delta^n} & H^{n+1} & \longrightarrow & \cdots \end{array}$$

Caso $f^n : G^n \to H^n$ seja um isomorfismo para todo $n \geq 0$, temos que f é um isomorfismo de cocadeias complexas.

Teorema 3.2.3. *Sejam F um funtor aditivo da categoria de R-álgebras comutativas para a categoria de grupos abelianos e S extensão galoisiana de R com grupo de Galois G. Então $C(S/R, F) \simeq C(G, F(S))$ como cocadeias complexas, e $H^n(S/R, F) \simeq H^n(G, F(S))$, para $n \geq 0$.*

Demonstração. Como h_n são isomorfismos, assim como φ_n, a demonstração segue dos isomorfismos $h_{n,F} : F(S^{n+1}) \to E_F^n$ definidos por $h_{n,F} = \varphi_n F(h_n)$. Assim, temos que $\theta_i h_n = h_{n+1}\varepsilon_i$ e pela construção dos parágrafos anteriores, $\theta_{i,F} h_{n,F} = h_{n+1,F} F(\varepsilon_i)$, e portanto $\delta^n h_{n,F} = h_{n+1,F}\Delta^n$, a partir das definições. Lembrando que $E_F^n = C^n(G, F(S))$, temos os isomorfismos. □

O diagrama a seguir ilustra a construção até aqui. As cocadeias complexas correspondem à primeira e à terceira coluna do diagrama, e a segunda coluna à composição $h_{n,F} = \varphi_n F(h_n)$.



Sejam A, B R-álgebras comutativas, e seja F um funtor. A composição dos homomorfismos induzidos pelas projeções p_A e p_B e inclusões i_A e i_B de A e B em $A \oplus B$

$$F(A \oplus B) \to F(A) \oplus F(B)$$

dada por $x \mapsto (F(p_A)(x), F(p_B)(x))$ e

$$F(A) \oplus F(B) \to F(A \oplus B)$$

dado por $(x, y) \mapsto F(i_A)(x) + F(i_B)(y)$ para um $x \in F(A \oplus B)$ resulta em

$$x \mapsto F(i_A)(F(p_A)(x)) + F(i_B)(F(p_B)(x)).$$

Disto segue que se $F(i_A \circ p_A + i_B \circ p_B) \overset{*}{=} F(i_A \circ p_A) + F(i_B \circ p_B)$ então

$$\begin{aligned}
&F(i_A)(F(p_A)(x)) + F(i_B)(F(p_B)(x)) \\
&= (F(i_A) \circ F(p_A))(x) + (F(i_B) \circ F(p_B))(x) \\
&= F(i_A \circ p_A)(x) + F(i_B \circ p_B)(x) \\
&= (F(i_A \circ p_A) + F(i_B \circ p_B))(x) \\
&\overset{*}{=} F((i_A \circ p_A) + (i_B \circ p_B))(x) \\
&= F(\operatorname{id}_{A \oplus B})(x) = \operatorname{id}_{F(A \oplus B)}(x) = x,
\end{aligned}$$

ou seja, a aplicação $x \mapsto (F(p_A)(x), F(p_B)(x))$ é um isomorfismo. Assim, $F(A \oplus B) \simeq F(A) \oplus F(B)$, o que implica que, para um conjunto finito de índices J,

$$\bigoplus_{j \in J} F(A_j) \simeq F\left(\bigoplus_{j \in J} A_i\right)$$

e portanto F é aditivo. Isto nos mostra que para verificar se um funtor F é aditivo, é suficiente verificar a igualdade $F(i_A \circ p_A + i_B \circ p_B) = F(i_A \circ p_A) + F(i_B \circ p_B)$, para quaisquer A, B R-álgebras comutativas.

Sejam agora U e P os funtores covariantes da categoria de R-álgebras comutativas para a categoria de grupos abelianos definidos a seguir: seja T uma R-álgebra comutativa, $U(T)$ é o grupo multiplicativo dos elementos invertíveis de T, e $P(T)$ é o grupo de T-módulos projetivos finitamente gerados de posto 1.

Lema 3.2.4. *Seguindo as notações acima, o funtor U é aditivo.*

Demonstração. Como um morfismo $f : S \to T$ na categoria R-álgebras comutativas satisfaz $f(s \cdot t) = f(s) \cdot f(t)$, para quaisquer $s, t \in s$, temos que $f|_{U(S)} : U(S) \to U(T)$ é um morfismo de grupos abelianos. Portanto definimos, dado $f : S \to T$ um morfismo da categoria de R-álgebras comutativas, $U(f) := f|_{U(S)}$. Dessa forma, é claro que

$$U(i_S \circ p_S) + U(i_T \circ p_T) = i_S \circ p_S + i_T \circ p_T = U(i_S \circ p_S + i_T \circ p_T).$$

Logo, U é um funtor aditivo. □

Bourbaki constrói o grupo abeliano $P(T)$ dos T-módulos projetivos finitamente gerados de posto 1 em [5; II,§5.4.]. Este é um grupo abeliano com a operação de produto tensorial, com elemento neutro $\overline{T}$ e, dado $\overline{M} \in P(T)$, o inverso é $\overline{M}^{-1} = \overline{M^*}$, onde $M^* = \mathrm{Hom}_T(M, T)$. Vamos mostrar que P é um funtor aditivo.

Sejam S, T R-álgebras comutativas. Então, dado um homomorfismo $f : S \to T$, temos que T é um S-módulo (em particular, uma S-álgebra) com ação $s \cdot t = f(s)t$. Desta forma, um S-módulo M pode ser associado ao T-módulo $T \otimes_S M = M_T$, onde $t'(t \otimes m) = t't \otimes m$. Note que a aplicação que leva $M \mapsto M_T$ satisfaz $M_T \otimes_T N_T = (M \otimes_S N)_T$ para quaisquer S-módulos M, N. Desta forma, temos que este é um homomorfismo de grupos entre $P(S)$ e $P(T)$.

Lema 3.2.5. *Seguindo as notações acima, o funtor P é aditivo.*

Demonstração. Para mostar que o funtor P é aditivo, vamos mostrar que

$$\varphi : P(S \oplus T) \to P(S) \oplus P(T)$$

dado por $\varphi(M) = P(p_S)(M) + P(p_T)(M)$, onde $p_S : S \oplus T \to S$ e $p_T : S \oplus T \to T$ são as projeções canônicas e $P(p_S)(M) = M_S$ (analogamente para $P(p_T)$), é um isomorfismo. Note que, como p_S e p_T são homomorfismos

de $S \oplus T$ em S e T respectivamente, $P(p_S)$ e $P(p_T)$ são homomorfismos de grupos abelianos entre $P(S \oplus T)$ e $P(S)$ ou $P(T)$. Assim,

$$\begin{aligned}\varphi(M \otimes_{S\oplus T} N) &= P(p_S)(M \otimes_{S\oplus T} N) + (P(p_T)(M \otimes_{S\oplus T} N) \\ &= P(p_S)(M) \otimes_S P(p_S)(N)) + (P(p_T)(M) \otimes_T P(p_T)(N) \\ &= P(p_S)(M) + P(p_T)(M) \star P(p_S)(N) + P(p_T)(N) \\ &= \varphi(M) \star \varphi(N)\end{aligned}$$

Assim, basta verificar se o homomorfismo φ é uma bijeção. Sejam $M \in P(S)$ e $N \in P(T)$. Podemos ver S e T como $S \oplus T$-módulos, com ação dada por $(s+t)s' = ss'$ e $(s+t)t' = tt'$. Da mesma forma para os módulos M e N. Vamos mostrar que $\varphi(M \oplus N) = M + N$.

$$\begin{aligned}\varphi(M \oplus N) &= P(p_S)(M \oplus N) + P(p_T)(M \oplus N) \\ &= S \otimes_{S\oplus T} (M \oplus N) + T \otimes_{S\oplus T} (M \oplus N) \\ &= ((S \otimes_{S\oplus T} M) \oplus (S \otimes_{S\oplus T} N)) + ((T \otimes_{S\oplus T} M) \oplus (T \otimes_{S\oplus T} N))\end{aligned}$$

Neste caso, dado qualquer $s \otimes n \in S \otimes_{S\oplus T} N$, que $s \otimes n = 1(s+0) \otimes n = 1 \otimes (s+0)n = 1 \otimes 0 = 0$. De forma semelhante, temos que $T \otimes_{S\oplus T} S = 0$, e obtemos

$$\varphi(M \oplus N) = S \otimes_{S\oplus T} M + T \otimes_{S\oplus T} N,$$

mas $S \otimes_{S\oplus T} M \simeq M$ e $T \otimes_{S\oplus T} N \simeq N$. Portanto, $\varphi(M \oplus N) = M + N$ e este é um epimorfismo.

Para verificar a injetividade, tomemos dois $S \oplus T$-módulos M, N. Então

$$\begin{aligned}\varphi(M) &= \varphi(N) \\ P(p_S)(M) + P(p_T)(M) &= P(p_S)(N) + P(p_T)(N) \\ M_S + M_T &= N_S + N_T\end{aligned}$$

e portanto, $M_S \simeq N_S$ como S-módulos, e $M_T \simeq N_T$ como T-módulos. Logo, $M \simeq N$ como $S \oplus T$-módulos e φ é injetivo. □

Assim, obtemos o corolário a seguir, que é o principal resultado de [7].

Corolário 3.2.6. *Seja S extensão galoisiana de R com grupo de Galois G. Então existe uma sequência exata*

$$0 \to H^1(G, U(S)) \to P(R) \to H^0(G, P(S)) \to H^2(G, U(S)) \\ \to Br(S/R) \to H^1(G, P(S)) \to H^3(G, U(S))$$

onde $Br(S/R)$ é o grupo de Brauer das R-álgebras de Azumaya fatoradas por S.

Demonstração. A partir do Teorema 2.2.4, temos que S é um R-módulo projetivo finitamente gerado e, portanto, a sequência (3.8), a lembrar

$$0 \to H^1(S/R, U) \to P(R) \to H^0(S/R, P) \to H^2(S/R, U) \\ \to Br(S/R) \to H^1(S/R, P) \to H^3(S/R, U)$$

é exata [6; Theorem 7.6.]. Ainda, pelos Lemas 3.2.4 e 3.2.5, os funtores U e P são aditivos. Pelo Teorema 3.2.3, temos $H^n(S/R, U) \simeq H^n(G, U(S))$ e $H^n(S/R, P) \simeq H^n(G, P(S))$. Assim segue o resultado. □

Dois teoremas apresentados por Auslander e Goldman em [4] são consequências diretas do Corolário 3.2.6, e generalizam o Teorema 90 de Hilbert e o isomorfismo entre o segundo grupo de cohomologia e o grupo de Brauer, resultados já conhecidos para corpos. Mais uma vez, sejam S extensão galoisiana de R com grupo de Galois G. Então:

Corolário 3.2.7. *[4; Theorem A.9.] Se todo R-módulo projetivo finitamente gerado de posto 1 é livre, então $H^1(G, U(S)) = 0$.*

Demonstração. Suponha que todo R-módulo projetivo finitamente gerado de posto 1 é livre. Logo temos que $P(R)$, o grupo abeliano dos R-módulos projetivos finitamente gerados de posto 1, é trivial, pois são todos isomorfos a R^1. Portanto a sequência $0 \to H^1(G, U(S)) \to 0$ implica que $H^1(G, U(S)) = 0$. □

Corolário 3.2.8. *[4; Theorem A.15.] Suponha que todo S-módulo projetivo finitamente gerado de posto 1 é livre. Então, a sequência*

$$0 \to H^2(G, U(S)) \to Br(R) \to Br(S)$$

é exata.

Demonstração. Suponha que todo S-módulo projetivo finitamente gerado de posto 1 é livre. Logo, temos que $P(S)$ é trivial, pois são todos isomorfos a S^1. Portanto, os grupos de cohomologia $H^0(G, P(S))$ e $H^1(G, P(S))$ são triviais e implicam, pelo Corolário 3.2.6, a sequência exata $0 \to H^2(G, U(S)) \to Br(S/R) \to 0$, de onde segue o isomorfismo $H^2(G, U(S)) \simeq Br(S/R)$.

Por outro lado, a sequência

$$0 \to Br(S/R) \hookrightarrow Br(R) \xrightarrow{f} Br(S)$$

é exata, uma vez que $Br(S/R)$ é o núcleo da aplicação $f : Br(R) \to Br(S)$. Logo segue o resultado.

□

Referências Bibliográficas

[1] S. A. Amitsur. Simple algebras and cohomology groups of arbitrary fields. *Transactions of the American Mathematical Society*, 90, 1959.

[2] F. W. Anderson e K. R. Fuller. *Rings and Categories of Modules*, volume 13 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1974.

[3] M. F. Atiyah e I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[4] M. Auslander e O. Goldman. The Brauer group of a commutative ring. *Transactions of the American Mathematical Society*, 97, 1960.

[5] N. Bourbaki. *Commutative Algebra*. Springer-Verlag Berlin Heidelberg, 1989.

[6] S. U. Chase e A. Rosenberg. Amitsur cohomology and the Brauer group. *Memoirs of the American Mathematical Society*, 52, 1964.

[7] S. U. Chase, D. K. Harrison, e A. Rosenberg. Galois theory and Galois cohomology of commutative rings. *Memoirs of the American Mathematical Society*, 52, 1965.

[8] H. Chen. *The Brauer Group of Rational Numbers*. Tese de Doutorado, University of Oxford, 2019.

[9] G. A. da C. Barreiros. *Grupos e Extensões de Galois*. Tese de Doutorado, Universidade do Porto, 2005.

[10] R. R. de Araujo. *Anéis de inteiros de corpos de números e aplicações*. Tese de Doutorado, Univerisade Estadual Paulista "Júlio de Mesquita Filho", 2015.

[11] G. L. A. de Camargo. Grupo de Brauer e o teorema de Merkurjev-Suslin. Dissertação de Mestrado, Universidade de São Paulo, 2013.

[12] K. Harper. Group cohomology and Krummer theory. *The University of Chicago*, 2010.

[13] V. L. Lima. Dualidade de grupos, cohomologia galoisiana e correspondências de Krummer. Dissertação de Mestrado, Universidade Federal de Minas Gerais, 2015.

[14] R. A. Morris. On the Brauer group of $\mathbb{Z}$. *Pacific Journal of Mathematics*, 39(3), 1971.

[15] A. Paques. *Teoría de Galois sobre Anillos Conmutativos*. Universidad de los Andes, 1999.

[16] A. Paques e T. Tamusiunas. The Galois correspondence theorem for grupoid actions. *Journal of Algebra*, 2018.

[17] I. Rapinchuk. The Brauer group of a field, 2012. URL `https://sites.google.com/site/irapinchuk1/home`.

[18] A. Rosenberg e D. Zelinsky. On Amitsur's complex. *Trans. Amerc. Math. Soc.*, 97, 1960.

[19] A. A. Sant'Ana. Uma introdução ao estudo dos anéis semissimples, 2016.

[20] I. Stewart. *Galois Theory*. Taylor & Francis, fourth edition, 2015.

[21] O. Zariski e P. Samuel. *Commutative Algebra I*, volume 29 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1975.