Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

Teoria de Galois Parcial e Representação Via Semirreticulados

Dissertação de Mestrado

PATRÍCIA LIMA DA SILVA

Porto Alegre, 07 de agosto de 2015.

Dissertação submetida por Patrícia Lima da Silva*, como requisito parcial para a obtenção do grau de Mestre em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:

Prof. Dr. Antonio Paques (UFRGS)

Banca examinadora:

Profa. Dra. Andrea Morgado (UFPEL)

Profa. Dra. Daiana Aparecida da Silva Flôres(UFSM)

Profa. Dra. Daiane da Silva Freitas (FURG)

Profa. Dra. Saradia Sturza Della Flora (UFSM)

*Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)

Agradecimentos

Quero agradecer primeiramente a Deus por todas as oportunidades nesta vida. Aos meu pais pelo apoio nestes longos anos de estudo. Ao meu namorado pela companheirismo durante meu mestrado. Ao meu orientador, pela paciência em me ensinar e dividir o seu conhecimento comigo. Aos meus colegas da pós-graduação que foram fundamentais para que eu conseguisse chegar até aqui. A todos vocês, muito obrigada!

Resumo

Aqui exploramos a ideia de ação parcial de um grupo sobre um anel. Desenvolvemos a Teoria de Galois Parcial e mostramos como representar uma ação parcial utilizando semirreticulados.

Abstract

Here we will explore the idea of group partial action in a ring. We develop the Partial Galois Theory and we show how to represent a partial action using semi lattice.

Índice

Introdução

A busca por soluções para uma equação algébrica por meio de radicais é um problema muito antigo. Sabe-se que em 2.000 a.C. os babilônicos sabiam resolver equações de segundo grau, mesmo que ainda sem a preocupação com a demonstração de seus métodos. Essa preocupação começou com os gregos. A resolução de uma equação de terceiro grau foi obtida apenas no século XVI por del Ferro, Tartaglia e Cardano. Neste mesmo século foi obtido por Ferrari, um método para a resolução de equações de quarto grau. Passaram-se quase trezentos anos até que Abel, no início do século XIX, influenciado pelos trabalhos de Lagrange e Ruffini, encontrasse uma solução para as equações de grau cinco.

Surge então a pergunta natural: quando uma equação algébrica qualquer pode ser resolúvel por radicais? A resposta definitiva para esta questão é dada pelo matemático francês Évariste Galois (1811 - 1832), cujos trabalhos foram publicados apenas no ano de 1846. O Teorema Fundamental da Teoria de Galois estabelece uma bijeção entre os corpos intermediários de uma extensão de corpos L de K e os subgrupos do grupo dos K-automorfismos de L. A grande contribuição da teoria desenvolvida por Galois é a ligação entre os conceitos de polinômio, grupo e corpo. Aliás, os conceitos de grupo e corpo surgiram com Galois. Em função disto muitos autores afirmam que a Álgebra moderna nasce com Galois.

A Teoria que Galois desenvolveu deu origem a vários estudos dentro da Matemática. Aqui destacamos a contribuição de Chase, Harrison e Rosenberg em 1965 (ver [2]), onde é desenvolvida uma Teoria de Galois para anéis comutativos, com algumas hipóteses necessárias sobre as extensões e o grupo de Galois considerados. Neste contexto já não faz mais sentido falar em resolução de uma equação algébrica e o conceito extensão de Galois possui uma definição diferente da sua ideia original. Um conceito que permeia esta teoria é o de ação global de um grupo sobre um anel.

Em [6] R. Exel, no ano de 1994, define a noção de ação parcial de um grupo no contexto de C^*-álgebras. Ações parciais de grupos sobre álgebras foram consideradas pela primeira vez por M. Dokuchaev e R. Exel em [4], somente em 2005. Essa noção é o centro deste trabalho e a seção 1.2 é destinada a definir ação parcial, e dar alguns exemplos e propriedades. A seção 1.1 tem por objetivo expor algumas resultados sobre módulos, necessários ao desenvolvimento do capítulo seguinte.

Em 2007 M. Dokuchaev, M. Ferrero e A. Paques [5] publicaram um artigo onde foi introduzida a noção de extensão de Galois parcial e é desenvolvida uma teoria de Galois parcial para anéis comutativos. O objetivo do Capítulo 2 é demonstrar o Teorema 4.1 de [5] de forma detalhada e criar meios de provar o Teorema 5.1 de [5] sem exigir que os ideais envolvidos na ação parcial considerada sejam todos não nulos. Para os nossos propósitos será necessário introduzir a noção parcial de homomorfismos de anéis fortemente distintos.

O último capítulo é baseado no artigo [9] de K. Jung-Miao e G. Szeto e traz uma interessante maneira de representarmos ações parciais de grupos em anéis utilizando as noções de semigrupo booleano e semirreticulado.

Capítulo 1

Preliminares

Neste capítulo expomos definições e observações que são pré-requisitos para a teoria desenvolvida nos próximos capítulos. O que apresentamos aqui será usado durante todo texto.

1.1 Módulos

Esta seção tem o objetivo tornar a leitura dos próximos capítulos acessível aos leitores que ainda não tenham tido contado com as definições e teoremas usados durante o texto. Para facilitar a leitura, não vamos apresentar as demonstrações dos resultados aqui enunciados. O conteúdo exposto pode ser encontrado nas referências [1], [3], [10] e [12].

Começamos definindo módulo, álgebra e seus homomorfismos.

Definição 1.1.1. *Seja A um anel com elemento unidade 1_A. Dizemos que um grupo abeliano $(M, +)$ é um A-módulo à esquerda se existe uma aplicação*

$$\begin{aligned} \cdot : \quad A \times M &\longrightarrow M \\ (a, m) &\longmapsto a \cdot m := am, \end{aligned}$$

satisfazendo os seguintes axiomas

(i) $a(m_1 + m_2) = am_1 + am_2$;

(ii) $(a + b)m = am + bm$;

(iii) $1_A m = m$;

(iv) $(ab)m = a(bm)$;

para quaisquer $a, b \in A$, $m, m_1, m_2 \in M$.

Observamos que A é um A-módulo à esquerda. A noção de A-módulo à direita é definida de forma análoga. Em particular, se A é um anel comutativo, então todo A-módulo à esquerda é também um A-módulo à direita e, neste caso, dizemos simplesmente que A é um A-módulo.

Dados M e N A-módulos à esquerda, uma aplicação $f : M \to N$ é um homomorfismo de A-módulos à esquerda (ou A-linear à esquerda), se

$$f(m_1 + m_2) = f(m_1) + f(m_2)$$

$$f(am) = af(m)$$

para quaisquer $a \in A$, $m_1, m_2, m \in M$. O kernel do homomorfismo f é o conjunto dado por

$$ker(f) = \{m \in M \mid f(m) = 0_N\}.$$

A imagem de f é o conjunto dado por

$$Im(f) = f(M) = \{f(m) \mid m \in M\}.$$

Temos que f é injetiva se, e somente se, $ker(f) = 0_M$. Dizemos que f é um isomorfismo se é injetiva e sobrejetiva.

Definição 1.1.2. *Seja A um anel comutativo com 1_A. Dizemos que um conjunto S é uma A-álgebra, se:*

- *S é um anel com unidade 1_S;*
- *S é um A-módulo;*
- *$(ax)y = x(ay) = a(xy)$, para todo $a \in A, x, y \in S$.*

Um homomorfismo de A-álgebras $f : S \longrightarrow S'$ é um homomorfismo de anéis e de A-módulos.

Dados A-módulos à esquerda M e N, denotamos por $Hom_A(M, N)$ o grupo dos homomorfismos de M em N com a operação $f + g$ definida por $(f + g)(m) = f(m) + g(m)$, para todo $m \in M$. Se A é comutativo podemos definir $a \cdot f$ por $(a \cdot f)(m) = af(m)$,para quaisquer $a \in A$ e $m \in M$. Se $M = N$ então $f : M \longrightarrow M$ é um endomorfismo de M e escrevemos $End_A(M)$ ao invés de $Hom_A(M, M)$. Com a composição de homomorfismo $End_A(M)$ é um anel e, se A é comutativo, temos que $End_A(M)$ é uma A-álgebra.

Definição 1.1.3. *Uma sequência de A-módulos (à esquerda) e A-homomorfismos (à esquerda)*

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

é dita exata em M_i se $Im(f_i) = ker(f_{i+1})$. A sequência é dita exata se for exata em cada M_i.

Uma sequência exata curta possui a forma

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0.$$

Segue da definição de sequência exata, que f é um A-homomorfismo injetor e que g um A-homomorfismo sobrejetor. Uma sequência exata $M \xrightarrow{g} N \longrightarrow 0$ (respectivamente, $0 \longrightarrow N \xrightarrow{f} M$) cinde se existe um homomorfismo de A-módulos

$\theta : N \to M$ (respectivamente, $\theta : M \to N$) com $g \circ \theta = Id_N$ (respectivamente, $\theta \circ f = Id_N$). Se $M \xrightarrow{g} N \longrightarrow 0$ cinde então $N \simeq Im(\theta)$, $Im(\theta) \cap ker(g) = 0$ e $M = Im(\theta) \oplus ker(g)$. (Analogamente se $0 \longrightarrow N \xrightarrow{f} M$ cinde, temos que $M = Im(f) \oplus ker(\theta)$).

Sejam A anel comutativo com unidade e M, N, P A-módulos. A aplicação $f : M \times N \to P$ é dita A-bilinear se, para cada $m \in M$, a aplicação $n \mapsto f(m, n)$ de N em P é A-linear, e para cada $n \in N$ a aplicação $m \mapsto f(m, n)$ de M em P é A-linear.

Sejam A anel comutativo com unidade e M, N A-módulos. Então existe um par (P, f), onde P é um A-módulo e $f : M \times N \to P$ é uma aplicação A-bilinear, que satisfaz a seguinte propriedade universal:

Dado qualquer A-módulo T e qualquer aplicação A-bilinear $g : M \times N \to T$, existe um único homomorfismo de A-módulos $h : P \to T$ tal que $h \circ f = g$.

Além disso, (P, f) é único a menos de isomorfismo. O A-módulo P é o produto tensorial de M e N sobre A e é denotado por $M \otimes_A N$, ou somente $M \otimes N$ se não houver ambiguidade sobre o anel A. Para qualquer $m \in M$ e $n \in N$, o elemento $f((m, n))$ é denotado por $m \otimes n$. Um elemento qualquer de $M \otimes_A N$ é uma soma finita do tipo $\sum_{fin} m_i \otimes n_i$.

Sejam A anel comutativo com unidade e M, N, P A-módulos. A seguir, listamos algumas propriedades do produto tensorial:

- $M \otimes_A N \simeq N \otimes_A M$;
- $M \otimes_A A \simeq M$;
- $(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P)$;
- $M \otimes_A (N \oplus P) \simeq (M \otimes_A N) \oplus (M \otimes_A P)$.

Dizemos que um A-módulo à esquerda L é livre, com base $\{x_i \mid i \in I\}$, se todo elemento $x \in L$ escreve-se de forma única como $x = \sum_{i \in I} a_i x_i$, onde $a_i \in A$ são todos nulos exceto um número finito de índices. Se I é finito, dizemos que L é um A-módulo à esquerda livre finitamente gerado.

Dizemos que um A-módulo à esquerda P é projetivo se P é somando direto de um A-módulo à esquerda livre L. Se, em particular, L for finitamente gerado, então dizemos que P é um A-módulo à esquerda projetivo finitamente gerado.

As seguintes afirmações são equivalentes:

- P é projetivo;
- Toda sequência exata de A-módulos à esquerda $M \xrightarrow{f} L \longrightarrow 0$ cinde;
- Existem conjuntos $\{p_i \mid i \in I\}$ em P e $\{f_i \mid i \in I\}$ em $Hom_A(P, A)$ tais que para todo $p \in P$, $p = \sum_i f_i(p) p_i$, onde $f_i(p) = 0$ exceto para um número finito de índices.

O conjunto I do último item é finito se e somente se P é finitamente gerado. E chamamos a coleção $\{p_i, f_i\}$ de base dual de P.

Corolário 1.1.4. *Seja P um A-módulo projetivo à esquerda. Seja*

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

uma sequência exata de A-módulos à esquerda. Então a sequência

$$0 \longrightarrow M' \otimes_A P \xrightarrow{f \otimes Id_P} M \otimes_A P \xrightarrow{g \otimes Id_P} M'' \otimes_A P \longrightarrow 0$$

é exata.

Dizemos que um A-módulo à esquerda M é fiel se o conjunto

$$ann_A(M) = \{a \in A \mid a \cdot m = 0, \text{ para todo } m \in M\}$$

é nulo, ou seja, $ann_A(M) = 0_A$. O conjunto $ann_A(M)$ é chamado de anulador de M em A.

Corolário 1.1.5. *Seja A um anel comutativo com unidade 1_A. Se P é um A-módulo projetivo finitamente gerado e fiel, então o ideal de A gerado por*

$$\{f(p) \mid p \in P \text{ e } f \in Hom_A(P, A)\}$$

é igual a A.

Sejam A um anel comutativo com unidade 1_A, S uma A-álgebra com unidade 1_S e S^o a A-álgebra oposta de S (isto é, S^o é um anel com o mesmo grupo aditivo de S e o produto ab em S^o é o produto ba em S). Definimos a álgebra envolvente de S como $S^e = S \otimes_A S^o$. Observamos que se S é comutativa, então $S^e = S \otimes_A S$. Notemos que S é um S^e-módulo esquerdo via a ação $(r \otimes s) \cdot t = rts$, para quaisquer $r, s, t \in S$. Seja $\mu : S^e \longrightarrow S$ a aplicação A-linear induzida pela multiplicação de S, isto é, $\mu(\sum_i r_i \otimes s_i) = \sum_i r_i s_i$. É fácil ver que μ é um homomorfismo de S^e-módulos sobrejetivo. Se, além disso, S é comutativa então μ é um homomorfismo de S^e-álgebras. Observemos que $J = ker(\mu)$ é um ideal de S^e gerado por

$$\{s \otimes 1_S - 1_S \otimes s \mid s \in S\}.$$

Dizemos que S é separável sobre A (ou uma A-álgebra separável, ou ainda A-separável) se acontece uma (e portanto todas) das seguintes condições equivalentes:

- Existe $e \in S^e$ tal que $\mu(e) = 1_S$ e $Je = 0$. O elemento e é chamado de idempotente de separabilidade;
- S é um S^e-módulo projetivo;
- A seguinte sequência exata de A^e-módulos à esquerda

  $$0 \longrightarrow J \longrightarrow S^e \xrightarrow{\mu} S \longrightarrow 0$$

  cinde.

1.2 Ação Parcial

Começamos definindo ação global de um grupo sobre um anel unitário.

Definição 1.2.1. *Sejam G um grupo e A um anel unitário. Uma ação global de G sobre A é um homomorfismo de grupos*

$$\begin{array}{rccc} \beta: & G & \longrightarrow & Aut(A) \\ & g & \longmapsto & \beta_g. \end{array}$$

Denotamos $\beta_g(x) = g(x)$, para todo $g \in G$ e $x \in A$.

Exemplo 1.2.2. *Sejam R um anel com unidade, $A = R \times R \times R$ e $G = \langle g \mid g^3 = 1 \rangle$, o grupo cíclico de ordem 3. Considere a seguinte ação (global) de G sobre A:*

$$\begin{array}{rccc} \beta: & G & \longrightarrow & Aut(A) \\ & 1 & \longmapsto & \beta_1 : (a,b,c) \mapsto (a,b,c) \\ & g & \longmapsto & \beta_g : (a,b,c) \mapsto (c,a,b) \\ & g^2 & \longmapsto & \beta_{g^2} : (a,b,c) \mapsto (b,c,a). \end{array}$$

Agora, definimos ação parcial de um grupo sobre um anel unitário. Esta é a definição central deste trabalho.

Definição 1.2.3. *Sejam G um grupo e A um anel unitário. Dizemos que $\alpha = (\{D_g\}, \{\alpha_g\})_{g \in G}$ é uma ação parcial de G sobre A se, para cada $g \in G$, D_g é um ideal de A e $\alpha_g : D_{g^{-1}} \to D_g$ é um isomorfismo de anéis tal que, para quaisquer $g, h \in G$, as seguintes afirmações são satisfeitas:*

(i) $D_1 = A$ *e* $\alpha_1 = Id_A$ *(o automorfismo identidade de A);*

(ii) $\alpha_g(D_{g^{-1}} \cap D_h) = D_g \cap D_{gh}$;

(iii) $\alpha_g \circ \alpha_h(x) = \alpha_{gh}(x)$, *para todo* $x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$.

Note que $\alpha_h(D_{h^{-1}} \cap D_{(gh)^{-1}}) = D_h \cap D_{g^{-1}}$. Então se $x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$ temos que $\alpha_h(x) \in D_{g^{-1}}$. Portanto, podemos compor $\alpha_g \circ \alpha_h(x)$, para todo $x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$.

Se $D_g = A$, para todo $g \in G$, a ação α é dita global.

Dada uma ação global β de um grupo G sobre um anel A, é sempre possível construir uma ação parcial α, que é chamada de restrição da ação β. A seguir apresentamos um exemplo de ação parcial obtida restringindo a ação global do exemplo 1.2.2.

Exemplo 1.2.4. *Sejam R um anel com unidade, $A = R \times R \times R$, $I = \{0\} \times R \times R$ e $G = \langle g \mid g^3 = 1 \rangle$. Restringimos a ação (global) β de G sobre A definida no exemplo 1.2.2 a uma ação parcial α de G sobre I da seguinte maneira: $D_1 = I$, $D_g = I \cap g(I) = \{0\} \times \{0\} \times R$, $D_{g^2} = I \cap g^2(I) = \{0\} \times R \times \{0\}$, $\alpha_1 = Id_A|_I$, e:*

$$\begin{array}{rcl} \alpha_g = g|_{D_{g^2}} : D_{g^2} & \to & D_g \\ (0,b,0) & \mapsto & (0,0,b) \end{array} \quad , \quad \begin{array}{rcl} \alpha_{g^2} = g^2|_{D_g} : D_g & \to & D_{g^2} \\ (0,0,c) & \mapsto & (0,c,0). \end{array}$$

Exemplo 1.2.5. *Considere G um grupo finito e A um anel unitário. Sejam $D_1 = A$, $\alpha_1 = Id_A$, $D_g = 0_A$, para todo $g \neq 1$, e $\alpha_g : D_{g^{-1}} \longrightarrow D_g$ o isomorfismos nulo, para todo $g \neq 1$. É fácil verificar que $\alpha = (\{D_g\}, \{\alpha_g\})_{g \in G}$ é uma ação parcial.*

Exemplo 1.2.6. *Sejam R um anel com unidade, $A = R \times R \times R$ e $G = \{1, g, h, gh\}$, o grupo de Klein. Considere a seguinte ação parcial de G sobre A:*
$D_1 = A$, $D_g = R \times \{0\} \times R$, $D_h = R \times R \times \{0\}$ e $D_{gh} = \{0\} \times R \times R$; e isomorfismos $\alpha_1 = Id_A$, e:

$$\begin{array}{rcl} \alpha_g : D_g & \to & D_g \\ (a,0,c) & \mapsto & (c,0,a) \end{array} \quad , \quad \begin{array}{rcl} \alpha_h : D_h & \to & D_h \\ (a,b,0) & \mapsto & (b,a,0) \end{array} \quad , \quad \begin{array}{rcl} \alpha_{gh} : D_{gh} & \to & D_{gh} \\ (0,b,c) & \mapsto & (0,c,b). \end{array}$$

Exemplo 1.2.7. *Sejam R um anel com unidade, $A = R \times R \times R$ e $G = \langle g \mid g^4 = 1 \rangle$, o grupo cíclico de ordem 4. Considere a seguinte ação parcial de G sobre A:*
$D_1 = A$, $D_g = \{0\} \times R \times R$, $D_{g^2} = \{0\} \times R \times \{0\}$ e $D_{g^3} = R \times R \times \{0\}$; e

isomorfismo $\alpha_1 = Id_A$*, e:*

$$\begin{array}{lllll} \alpha_g : D_{g^3} & \to & D_g & , \quad \alpha_{g^2} : D_{g^2} & \to & D_{g^2} & , \quad \alpha_{g^3} : D_g & \to & D_{g^3} \\ (a,b,0) & \mapsto & (0,b,a) & \quad (0,b,0) & \mapsto & (0,b,0) & \quad (0,b,c) & \mapsto & (c,b,0). \end{array}$$

Neste trabalho consideramos que cada ideal D_g é unitário, com elemento identidade 1_g, podendo ser eventualmente nulo. É imediato ver que cada 1_g é um idempotente central de A e $D_g = A1_g = 1_gA$, para todo $g \in G$. Além disso, $\alpha_g(1_{g^{-1}}) = 1_g$, pois α_g é um isomorfismo de anéis. Como cada $D_g = 1_gA$ é unitário, temos que $D_g \cap D_h = D_gD_h$. De fato, se $x \in D_g \cap D_h$ então $x = 1_gx = 1_g(1_hx) = 1_g1_hx$, ou seja, $x \in D_gD_h$. Claramente, $D_gD_h \subset D_g \cap D_h$, pois D_g e D_h são ideais de A.

Definição 1.2.8. *Dizemos que uma ação parcial* α *de* G *sobre* A *é globalizável se existe um anel* B*, uma ação global* β *de* G *em* B *por automorfismos de* B*, um homomorfismo injetor de anéis* φ *de* A *em* B *tal que* $\varphi(A)$ *é um ideal de* B *e, para todo* $g \in G$*, as seguintes condições são satisfeitas:*

(i) $B = \sum_{g \in G} g(\varphi(A))$*;*

(ii) $\varphi(D_g) = \varphi(A) \cap g(\varphi(A))$*;*

(iii) $\varphi \circ \alpha_g(x) = g \circ \varphi(x)$*, para cada* $x \in D_{g^{-1}}$*.*

Denotaremos por (B, β) a globalização da ação parcial α de G em A, também chamada de ação envolvente de α. Neste caso, dizemos que B é o anel envolvente de A. Sempre que temos uma ação global podemos restringi-la a uma ação parcial, seguindo os passos feitos no exemplo 1.2.4. A pergunta natural que surge é a seguinte: se temos uma ação parcial, quando encontramos uma ação global cuja restrição coincida com a ação parcial? O Teorema a seguir responde esta pergunta:

Teorema 1.2.9 ([4], Teorema 4.5)**.** *Seja* A *uma álgebra unitária. Então a ação parcial* α *do grupo* G *sobre* A *admite uma ação envolvente* β *se e somente se cada*

ideal $D_g (g \in G)$ é uma álgebra unitária. Além disso, β, se existe, é única a menos de equivalência.

Como mencionado acima, estamos considerando ações parciais em anéis unitários tais que seus respectivos ideais são unitários, portanto as ações parciais consideradas neste trabalho sempre possuem globalização. Apesar disso, no próximo capítulo construiremos a Teoria de Galois parcial sem utilizar a globalização, seguindo assim um caminho diferente do apresentado em [5].

Lema 1.2.10. *Seja $\alpha = (\{D_g\}, \{\alpha_g\})_{g\in G}$ uma ação parcial globalizável do grupo G sobre o anel A, com globalização (B, β). Então, para quaisquer $g, h \in G$ e $x \in A$, temos que:*

(i) $1_g = 1_A g(1_A)$;

(ii) $\alpha_g(x1_{g^{-1}}) = g(x)1_A$;

(iii) $\alpha_g(1_h 1_{g^{-1}}) = 1_g 1_{gh}$;

(iv) $\alpha_g(\alpha_h(x1_{h^{-1}})1_{g^{-1}}) = \alpha_{gh}(x1_{(gh)^{-1}})1_g$.

Demonstração. (i) $B1_g = B1_A1_g = A1_g = A \cap g(A) = B1_A \cap Bg(1_A) = B1_Ag(1_A)$, portanto $1_g = 1_Ag(1_A)$.

(ii) Pelo item (i) e pela Definição 1.2.8 (iii), temos que:

$\alpha_g(x1_{g^{-1}}) = g(x1_Ag^{-1}(1_A)) = g(xg^{-1}(1_A)) = g(x)1_A$, onde $g(x) \in B$, portanto $\alpha_g(x1_{g^{-1}}) = g(x)1_A$.

(iii) Pelos itens (i) e (ii), decorre que:

$\alpha_g(1_h1_{g^{-1}}) = g(1_h)1_A = g(1_Ah(1_A))1_A = g(1_A)gh(1_A)1_A = 1_Ag(1_A)1_Agh(1_A)$ $= 1_g1_{gh}$, portanto $\alpha_g(1_h1_{g^{-1}}) = 1_g1_{gh}$.

(iv) Pelo item (iii), temos que:

$\alpha_g(\alpha_h(x1_{h^{-1}})1_{g^{-1}}) = \alpha_g(\alpha_h(x1_{h^{-1}})1_h1_{g^{-1}}) = \alpha_g(\alpha_h(x1_{h^{-1}})\alpha_h(1_{h^{-1}}1_{(gh)^{-1}}))$
$= \alpha_g(\alpha_h(x1_{h^{-1}}1_{(gh)^{-1}})) = \alpha_{gh}(x1_{h^{-1}}1_{(gh)^{-1}}) = \alpha_{gh}(x1_{(gh)^{-1}})\alpha_{gh}(1_{h^{-1}}1_{(gh)^{-1}})$
$= \alpha_{gh}(x1_{(gh)^{-1}})1_{gh}1_g = \alpha_{gh}(x1_{(gh)^{-1}})1_g$, portanto $\alpha_g(\alpha_h(x1_{h^{-1}})1_{g^{-1}}) = \alpha_{gh}(x1_{(gh)^{-1}})1_g$.

□

Definição 1.2.11. *Seja α uma ação parcial de um grupo G sobre um anel A. Definimos o conjunto*

$$A^\alpha = \{x \in A \mid \alpha_g(x1_{g^{-1}}) = x1_g, \text{ para todo } g \in G\}.$$

Observe que A^α é um subanel de A, o qual é chamado de subanel dos invariantes de A pela ação α.

Exemplo 1.2.12. *Vamos calcular A^α do exemplo 1.2.6, onde $A = R \times R \times R$ e $G = \{1, g, h, gh\}$ é o grupo de Klein. Seja $x = (a, b, c) \in A$. Se $x \in A^\alpha$, então:*

1) $(c, 0, a) = \alpha_g(x1_g) = x1_g = (a, 0, c) \Rightarrow a = c$;

2) $(b, a, 0) = \alpha_h(x1_h) = x1_h = (a, b, 0) \Rightarrow a = b$;

3) $(0, c, b) = \alpha_{gh}(x1_{gh}) = x1_{gh} = (0, b, c) \Rightarrow b = c$.

Portanto, $A^\alpha = \{(r, r, r) \mid r \in R\}$.

Exemplo 1.2.13. *Vamos determinar A^α do exemplo 1.2.7, onde $A = R \times R \times R$ e $G = \langle g \mid g^4 = 1\rangle$. Se $x = (a, b, c) \in A^\alpha$, então:*

1) $(0, b, a) = \alpha_g(x1_{g^3}) = x1_g = (0, b, c) \Rightarrow a = c$;

2) $(0, b, 0) = \alpha_{g^2}(x1_{g^2}) = x1_{g^2} = (0, b, 0)$. *Isto não nos acrescenta nenhuma restrição;*

3) $(c, b, 0) = \alpha_{g^3}(x1_g) = x1_{g^3} = (a, b, 0) \Rightarrow a = c.$

Assim, temos que $A^\alpha = \{(r, s, r) \mid r, s \in R\}$.

Para o que segue, vamos considerar G um grupo finito.

Definição 1.2.14. *O skew anel de grupo parcial, denotado por* $A \star_\alpha G$*, é o conjunto das somas formais finitas* $\sum_{g \in G} x_g u_g$*, em que* $x_g \in D_g$ *e* u_g *são símbolos. A adição é a usual e a multiplicação é determinada por*

$$(x_g u_g)(y_h u_h) = \alpha_g(\alpha_{g^{-1}}(x_g) y_h) u_{gh},$$

para quaisquer $x_g \in D_g$ *e* $y_h \in D_h$.

Observe que a multiplicação está bem definida, dado $x_g \in D_g$, $\alpha_{g^{-1}}(x_g) \in D_{g^{-1}}$ e $y_h \in D_h$. Como todos ideais de α são unitários, então $\alpha_g(D_{g^{-1}} D_h) = \alpha_g(D_{g^{-1}} \cap D_h)$ $= D_g \cap D_{gh} \subset D_{gh}$, ou seja, $\alpha_g(\alpha_{g^{-1}}(x_g) y_h) \in D_{gh}$.

Note que $\alpha_g(\alpha_{g^{-1}}(x_g) y_h) u_{gh} = \alpha_g(\alpha_{g^{-1}}(x_g) 1_{g^{-1}} y_h) u_{gh} = x_g \alpha_g(1_{g^{-1}} y_h) u_{gh}$, então a multiplicação em $A \star_\alpha G$ também pode ser definida da seguinte maneira:

$$(x_g u_g)(y_h u_h) = x_g \alpha_g(y_h 1_{g^{-1}}) u_{gh}.$$

Existe um homomorfismo de anéis injetor

$$\begin{aligned} A &\longrightarrow A \star_\alpha G \\ x &\longmapsto x u_1. \end{aligned}$$

Assim, A é isomorfo a Au_1. Como cada D_g é um anel com identidade, então, pelo Corolário 3.2 de [4], $A \star_\alpha G$ é associativo. Assim temos que $A \star_\alpha G$ com a soma usual e a multiplicação definida acima é um anel com elemento identidade $1_A u_1$.

Observamos que em geral $A \star_\alpha G$ não é comutativo. De fato, usando a ação parcial definida no Exemplo 1.2.6 do grupo de Klein, $\{1, g, h, gh\}$, sobre o anel

$A = R \times R \times R$, temos, para quaisquer $a, b, x, y \in R$, que:

$$((a,0,b)u_g)((x,y,0)u_h) = (0,0,bx)u_{gh}, \text{enquanto}$$

$$((x,y,0)u_h)((a,0,b)u_g) = (0,ya,0)u_{gh}.$$

E $(0,0,bx)u_{gh} \neq (0,ya,0)u_{gh}$ sempre que $bx \neq 0$ ou $ya \neq 0$.

Definimos a aplicação traço parcial $tr_\alpha : A \to A$ por $tr_\alpha(x) = \sum_{g\in G} \alpha_g(x1_{g^{-1}})$, para todo $x \in A$.

Observação 1.2.15. *Note que $tr_\alpha(A) \subset A^\alpha$. De fato, seja $x \in A$, pelo Lema 1.2.10, item (iv), temos que:*

$$\begin{aligned}\alpha_h(tr_\alpha(x)1_{h^{-1}}) &= \alpha_h(\sum_{g\in G} \alpha_g(x1_{g^{-1}})1_{h^{-1}}) = \sum_{g\in G} \alpha_h(\alpha_g(x1_{g^{-1}})1_{h^{-1}}) \\ &= \sum_{g\in G} \alpha_{hg}(x1_{(hg)^{-1}})1_h = \sum_{k\in G} \alpha_k(x1_{k^{-1}})1_h = tr_\alpha(x)1_h.\end{aligned}$$

Além disso, a aplicação traço é A^α-linear. De fato, sejam $a \in A^\alpha$ e $x \in A$, então:

$$\begin{aligned}tr_\alpha(ax) &= \sum_{g\in G} \alpha_g(ax1_{g^{-1}}) \\ &= \sum_{g\in G} \alpha_g(a1_{g^{-1}})\alpha_g(x1_{g^{-1}}) \\ &= \sum_{g\in G} a1_g\alpha_g(x1_{g^{-1}}) \\ &= a\sum_{g\in G} \alpha_g(x1_{g^{-1}}) \\ &= atr_\alpha(x).\end{aligned}$$

Capítulo 2

Teoria de Galois Parcial

Neste capítulo será demonstrado o Teorema das equivalências para a definição de extensão de Galois α-parcial e o Teorema Fundamental da Teoria de Galois Parcial. Para isto usamos como base o artigo de M. Dokuchaev, M. Ferrero e A. Paques [5] e apresentamos aqui as demonstrações detalhadas dos teoremas citados, porém sob outro ponto de vista. Ao longo de todo o capítulo A denotará um anel unitário e α uma ação parcial globalizável de um grupo finito G sobre o anel A. Além disso, vamos supor que A^α está contido no centro de A. Usaremos $\otimes$ para abreviar $\otimes_{A^\alpha}$.

2.1 Extensões de Galois Parciais

Iniciamos fazendo algumas observações sobre as estruturas usadas no Teorema das equivalências para a definição de extensão de Galois α-parcial.

Note que, $A \star_\alpha G$ é um A-módulo via a ação $x \cdot (x_g u_g) = (xu_1)(x_g u_g)$, para quaisquer $x \in A$ e $x_g \in D_g$. Em particular é um A^α-módulo, e é uma A^α-álgebra. Também temos que $End_{A^\alpha}(A)$ é um A-módulo à esquerda, com elemento identidade Id_A, via a ação $(x \cdot f)(x') = xf(x')$ para quaisquer $x, x' \in A$ e $f \in End_{A^\alpha}(A)$. Além

disso, $End_{A^\alpha}(A)$ é uma A^α-álgebra, com as operações usuais.

Seja $\varphi : A \star_\alpha G \to End_{A^\alpha}(A)$ definida por $\varphi(\sum_{g\in G} x_g u_g)(z) = \sum_{g\in G} x_g\alpha_g(z1_{g^{-1}})$, para todo $z \in A$. É fácil ver que φ é um homomorfismo de A-módulos à esquerda e de A^α-álgebras.

O anel A é um $A\star_\alpha G$-módulo à esquerda via φ, ou seja, $(x_g u_g)\cdot z = \varphi(x_g u_g)(z) = x_g\alpha_g(z1_{g^{-1}})$, para quaisquer $z \in A, x_g \in D_g$ e $g \in G$. De fato, sejam $z \in A, x_g \in D_g$ e $y_h \in D_h$, então

$$\begin{aligned}
(x_g u_g)\cdot[(y_h u_h)\cdot z] &= (x_g u_g)\cdot[y_h\alpha_h(z1_{h^{-1}})] \\
&= x_g\alpha_g(y_h\alpha_h(z1_{h^{-1}})1_{g^{-1}}) \\
&= x_g\alpha_g(y_h1_{g^{-1}})\alpha_g(\alpha_h(z1_{h^{-1}})1_{g^{-1}}) \\
&= x_g\alpha_g(y_h1_{g^{-1}})\alpha_{gh}(z1_{(gh)^{-1}})1_g \\
&= x_g\alpha_g(y_h1_{g^{-1}})\alpha_{gh}(z1_{(gh)^{-1}}) \\
&= [x_g\alpha_g(y_h1_{g^{-1}})u_{gh}]\cdot z \\
&= [(x_g u_g)(y_h u_h)]\cdot z
\end{aligned}$$

e $(1_A u_1)\cdot z = 1_A\alpha_1(z1_A) = 1_A z = z$.

Seja M um $A\star_\alpha G$-módulo à esquerda. Como podemos identificar os elementos $x \in A$ com os elementos $xu_1 \in A\star_\alpha G$, então M é um A-módulo à esquerda. Denotamos por

$$M^G = \{m \in M \mid (1_g u_g)\cdot m = 1_g m,\ \textit{para todo } g \in G\}$$

o conjunto dos elementos invariantes de M sobre G.

Se $M = A$ na definição dos invariantes acima temos que

$$A^G = \{x \in A \mid (1_g u_g)\cdot x = 1_g x,\ \text{para todo } g \in G\}.$$

Como $(1_g u_g)\cdot x = 1_g\alpha_g(x1_{g^{-1}}) = \alpha_g(x1_{g^{-1}})$, então

$$A^G = \{x \in A \mid \alpha_g(x1_{g-1}) = 1_g x,\ \text{para todo } g \in G\},$$

ou seja, coincide com a definição de A^α do capítulo anterior.

Definição 2.1.1. *Seja α uma ação parcial de um grupo finito G sobre um anel A. Dizemos que A é uma extensão de Galois α-parcial de A^α se existem elementos $x_i, y_i \in A, 1 \leq i \leq n$, tais que, para cada $g \in G$, temos*

$$\sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} 1_A,$$

onde 1 denota o elemento identidade do grupo G. O conjunto $\{x_i, y_i\}_{1 \leq i \leq n}$ é chamado de sistema de coordenadas de Galois α-parciais de A sobre A^α.

Teorema 2.1.2. *Seja α uma ação parcial de um grupo finito G sobre um anel A. Então, as seguintes afirmações são equivalentes:*

(i) A é uma extensão de Galois α-parcial de A^α.

(ii) A é um A^α-módulo projetivo finitamente gerado e $\varphi : A \star_\alpha G \to End_{A^\alpha}(A)$ é um isomorfismo de A-módulos à esquerda e de A^α-álgebras.

(iii) Para todo $A \star_\alpha G$-módulo à esquerda M, a aplicação $\mu : A \otimes M^G \to M$, dada por $\mu(x \otimes m) = x \cdot m$, é um isomorfismo de A-módulos à esquerda.

(iv) A aplicação $\psi : A \otimes A \to \prod_{g \in G} D_g$, dada por $\psi(x \otimes y) = (x\alpha_g(y1_{g^{-1}}))_{g \in G}$, é um isomorfismo de A-módulos à esquerda.

Demonstração.

(i) $\Rightarrow$ (ii) Sejam $x_i, y_i \in A, 1 \leq i \leq n$, tais que $\sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} 1_A$, para todo $g \in G$. Definimos $f_i \in Hom_{A^\alpha}(A, A^\alpha)$ por $f_i(x) = tr_\alpha(y_i x) = \sum_{g \in G} \alpha_g(y_i x 1_{g^{-1}})$, para todo $x \in A$. Então, para todo $x \in A$, temos:

$$\begin{aligned} \sum_{i=1}^{n} f_i(x) x_i &= \sum_{i=1}^{n} x_i f_i(x) = \sum_{i=1}^{n} \sum_{g \in G} x_i \alpha_g(y_i x 1_{g^{-1}}) \\ &= \sum_{g \in G} (\sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}})) \alpha_g(x 1_{g^{-1}}) = \sum_{g \in G} \delta_{1,g} \alpha_g(x 1_{g^{-1}}) = x. \end{aligned}$$

Então o conjunto $\{f_i, x_i\}_{1\leq i\leq n}$, forma uma base dual para A sobre A^α. Portanto A é um A^α-módulo projetivo finitamente gerado.

Para mostrar que $\varphi : A\star_\alpha G \to End_{A^\alpha}(A)$ é sobrejetor, dado $f \in End_{A^\alpha}(A)$, consideramos $w = \sum_{g\in G}\sum_{i=1}^{n} f(x_i)\alpha_g(y_i 1_{g^{-1}})u_g \in A\star_\alpha G$. Então, para qualquer $x \in A$ temos:

$$\begin{aligned}
\varphi(w)(x) &= \sum_{g\in G}\sum_{i=1}^{n} f(x_i)\alpha_g(y_i 1_{g^{-1}})\alpha_g(x1_{g^{-1}}) \\
&= \sum_{i=1}^{n} f(x_i)\sum_{g\in G}\alpha_g(y_i x 1_{g^{-1}}) \\
&= \sum_{i=1}^{n} f(x_i)tr_\alpha(y_i x) \\
&= \sum_{i=1}^{n} f(x_i)f_i(x) \\
&= \sum_{i=1}^{n} f(x_i f_i(x)) \\
&= f(\sum_{i=1}^{n} x_i f_i(x)) = (x).
\end{aligned}$$

Portanto, $\varphi(w) = f$ e φ é sobrejetora.

Para mostrar que φ é injetora, consideramos $v = \sum_{g\in G} x_g u_g \in Ker(\varphi)$, então temos que $\varphi(v)(x) = 0$, para todo $x \in A$. Em particular, $\varphi(v)(x_i) = 0$, $1 \leq i \leq n$, logo:

$$\begin{aligned}
0 &= \sum_{h\in G}\sum_{i=1}^{n} \varphi(v)(x_i)\alpha_h(y_i 1_{h^{-1}})u_h \\
&= \sum_{h\in G}\sum_{g\in G}\sum_{i=1}^{n} x_g\alpha_g(x_i 1_{g^{-1}})\alpha_h(y_i 1_{h^{-1}})u_h \\
&= \sum_{h\in G}\sum_{g\in G}\sum_{i=1}^{n} x_g\alpha_g(x_i 1_{g^{-1}})\alpha_h(y_i 1_{h^{-1}})1_g u_h \\
&= \sum_{h\in G}\sum_{g\in G}\sum_{i=1}^{n} x_g\alpha_g(x_i 1_{g^{-1}})\alpha_g(\alpha_{g^{-1}}(\alpha_h(y_i 1_{h^{-1}})1_g))u_h \\
&= \sum_{h\in G}\sum_{g\in G}\sum_{i=1}^{n} x_g\alpha_g(x_i 1_{g^{-1}})\alpha_g(\alpha_{g^{-1}h}(y_i 1_{(g^{-1}h)^{-1}})1_{g^{-1}})u_h \\
&= \sum_{h\in G}\sum_{g\in G} x_g\alpha_g(\sum_{i=1}^{n} x_i\alpha_{g^{-1}h}(y_i 1_{h^{-1}g})1_{g^{-1}})u_h \\
&= \sum_{h\in G}\sum_{g\in G} x_g\alpha_g(\delta_{g,h}1_{g^{-1}})u_h \\
&= \sum_{g\in G} x_g\alpha_g(1_{g^{-1}})u_g = \sum_{g\in G} x_g u_g \\
&= v.
\end{aligned}$$

(ii) $\Rightarrow$ (iii) Primeiro observemos que $A \otimes M^G$ é um A-módulo à esquerda via a ação $x' \cdot (x \otimes m) = x'x \otimes m$, para quaisquer $x', x \in A$ e $m \in M^G$. Note que, μ é homomorfismo de A-módulos à esquerda, pois para quaisquer $x', x \in A$ e $m \in M$ temos

$$\mu(x' \cdot (x \otimes m)) = \mu(x'x \otimes m) = x'x \cdot m = x' \cdot (x \cdot m) = x' \cdot \mu(x \otimes m).$$

Para mostrar que μ é isomorfismo, vamos construir a sua inversa, que será denotada por ν. Mas antes disso, observemos alguns fatos.

Como A é um A^α-módulo projetivo finitamente gerado, então existem $x_i \in A$ e $f_i \in Hom_{A^\alpha}(A, A^\alpha) \subseteq End_{A^\alpha}(A)$, $1 \leq i \leq n$, tais que $x = \sum_{i=1}^{n} f_i(x)x_i$, para todo $x \in A$. Como φ é sobrejetora, seja $v_i \in A \star_\alpha G$ tal que $\varphi(v_i) = f_i$, $1 \leq i \leq n$.

Observe que para todo $z \in A$ temos

$$\varphi(\sum_{i=1}^{n} x_i \cdot v_i)(z) = \sum_{i=1}^{n} x_i\varphi(v_i)(z) = \sum_{i=1}^{n} x_i f_i(z) = z,$$

ou seja, $\varphi(\sum_{i=1}^{n} x_i \cdot v_i) = Id_A = 1_{End_{A^\alpha}(A)}$. Como φ é isomorfismo de anéis, temos que $\sum_{i=1}^{n} x_i \cdot v_i = 1_{A\star_\alpha G}$.

Agora observemos que, como $A\star_\alpha G$ é um A-módulo à esquerda e φ é isomorfismo de A-módulos à esquerda e de anéis, então, para todo $x \in A, g \in G$ e $1 \leq i \leq n$, temos que

$$\begin{aligned} \varphi((1_g u_g)v_i)(x) &= (\varphi(1_g u_g)\varphi(v_i))(x) = \varphi(1_g u_g)(\varphi(v_i)(x)) = \varphi(1_g u_g)(f_i(x)) \\ &= 1_g\alpha_g(f_i(x)1_{g^{-1}}) = 1_g f_i(x) = 1_g\varphi(v_i)(x) = \varphi(1_g v_i)(x). \end{aligned}$$

Portanto, $\varphi((1_g u_g)v_i) = \varphi(1_g v_i)$. Como φ é isomorfismo, então para todo $g \in G$ e $1 \leq i \leq n$,

$$(1_g u_g)v_i = 1_g v_i.$$

Disto segue que $v_i \cdot m \in M^G$, para todo $m \in M$. De fato,

$$1_g u_g \cdot (v_i \cdot m) = ((1_g u_g)v_i) \cdot m = (1_g v_i) \cdot m = 1_g(v_i \cdot m).$$

Agora definimos:

$$\begin{array}{rccc} \nu: & M & \longrightarrow & A \otimes M^G \\ & m & \longmapsto & \sum_{i=1}^{n} x_i \otimes v_i \cdot m. \end{array}$$

Para demonstrar que ν é a inversa de μ necessitamos da seguinte igualdade: $v \cdot (x \cdot m) = \varphi(v)(x) \cdot m$, para todo $x \in A$, $m \in M^G$ e $v = x_g u_g \in A \star_\alpha G$. De fato,

$$\begin{aligned} v \cdot (x \cdot m) &= v \cdot (xu_1 \cdot m) = (v \cdot xu_1) \cdot m \\ &= ((x_g u_g)(xu_1)) \cdot m = (x_g \alpha_g(x 1_{g^{-1}}) u_g) \cdot m \\ &= (\varphi(x_g u_g)(x) 1_g u_g) \cdot m = \varphi(v)(x)((1_g u_g) \cdot m) \\ &= \varphi(v)(x)(1_g m) = (x_g \alpha_g(x 1_{g^{-1}}) 1_g) \cdot m \\ &= x_g \alpha_g(x 1_{g^{-1}}) \cdot m = \varphi(v)(x) \cdot m. \end{aligned}$$

Agora estamos aptos a mostrar que a aplicação ν é a inversa da μ. De fato, se $x \otimes m \in A \otimes M^G$, então:

$$\begin{aligned} \nu \circ \mu(x \otimes m) &= \nu(x \cdot m) = \sum_{i=1}^{n} x_i \otimes v_i \cdot (x \cdot m) \\ &= \sum_{i=1}^{n} x_i \otimes (\varphi(v_i)(x) \cdot m) = \sum_{i=1}^{n} x_i \otimes f_i(x) \cdot m \\ &= \sum_{i=1}^{n} x_i f_i(x) \otimes m = x \otimes m. \end{aligned}$$

A penúltima igualdade segue do fato que $f_i(x) \in A^\alpha$. Por outro lado, se $m \in M$, então:

$$\begin{aligned} \mu \circ \nu(m) &= \mu(\sum_{i=1}^{n} x_i \otimes v_i \cdot m) \\ &= \sum_{i=1}^{n} x_i \cdot (v_i \cdot m) = 1_{A \star_\alpha G} \cdot m = m. \end{aligned}$$

(iii) $\Rightarrow$ (iv) Por um argumento análogo ao feito no item anterior e observando que $\prod_{g \in G} D_g$ é um A-módulo à esquerda via multiplicação de A, verifica-se que ψ é homomorfismo de A-módulos à esquerda.

Considere o conjunto $\mathcal{F} = \{f : G \longrightarrow A \mid f(g) \in D_g, \text{ para todo } g \in G\}$. Definindo as operações $(f_1 + f_2)(g) = f_1(g) + f_2(g)$ e $(x \cdot f)(g) = xf(g)$, para quaisquer $f_1, f_2 \in \mathcal{F}$, $g \in G$ e $x \in A$, temos que $\mathcal{F}$ é um A-módulo à esquerda.

Observe que $\mathcal{F}$ é isomorfo a $\prod_{g\in G} D_g$ como A-módulo à esquerda, via a aplicação que associa a cada $f \in \mathcal{F}$ o elemento $(f(g))_{g\in G} \in \prod_{g\in G} D_g$. Além disso, $\mathcal{F}$ é um $A \star_\alpha G$-módulo à esquerda via $(x_g u_g \cdot f)(h) = x_g \alpha_g(f(g^{-1}h)1_{g^{-1}})$, para quaisquer $f \in \mathcal{F}, g, h \in G$ e $x_g \in D_g$, pois para todo $k \in G$, temos que:

$$\begin{aligned}
((x_g u_g)\cdot((y_h u_h)\cdot f))(k) &= x_g\alpha_g((y_h u_h)\cdot f(g^{-1}k)1_{g^{-1}}) \\
&= x_g\alpha_g(y_h\alpha_h(f(h^{-1}g^{-1}k)1_{h^{-1}})1_{g^{-1}}) \\
&= x_g\alpha_g(y_h 1_{g^{-1}})\alpha_g(\alpha_h(f(h^{-1}g^{-1}k)1_{h^{-1}})1_{g^{-1}}) \\
&= x_g\alpha_g(y_h 1_{g^{-1}})\alpha_{gh}(f(h^{-1}g^{-1}k)1_{(gh)^{-1}})1_g \\
&= x_g\alpha_g(y_h 1_{g^{-1}})\alpha_{gh}(f(h^{-1}g^{-1}k)1_{(gh)^{-1}}) \\
&= (x_g\alpha_g(y_h 1_{g^{-1}})u_{gh}\cdot f)(k) \\
&= (((x_g u_g)(y_h u_h))\cdot f)(k)
\end{aligned}$$

e $(1_A u_1)\cdot f(h) = 1_A\alpha_1(f(h)) = 1_A f(h) = f(h)$, para todo $h \in G$.

Por hipótese, a aplicação $\mu : A \otimes \mathcal{F}^G \to \mathcal{F}$ é um isomorfismo de A-módulos à esquerda. Como, além disso, $\mathcal{F}$ e $\prod_{g\in G} D_g$ são isomorfos como A-módulos à esquerda então $\mu' : A \otimes \mathcal{F}^G \to \prod_{g\in G} D_g$, dada por $\mu'(x \otimes f) = (xf(g))_{g\in G}$ é um isomorfismo de A-módulos à esquerda.

Para completar a demonstração, mostremos que a aplicação $\theta : A \to \mathcal{F}^G$ definida por $\theta(x)(h) = \alpha_h(x1_{h^{-1}})$, para todo $x \in A$ e $h \in G$, é um isomorfismo de A^α-módulos à esquerda. Primeiramente observe que θ está bem definida pois, para todo $h \in G$, temos:

$$\begin{aligned}
((1_g u_g)\cdot\theta(x))(h) &= 1_g\alpha_g(\theta(x)(g^{-1}h)1_{g^{-1}}) \\
&= 1_g\alpha_g(\alpha_{g^{-1}h}(x1_{h^{-1}g})1_{g^{-1}}) \\
&= 1_g\alpha_g(\alpha_{g^{-1}h}(x1_{h^{-1}g})1_{g^{-1}}) \\
&= 1_g\alpha_g(\alpha_{g^{-1}}(\alpha_h(x1_{h^{-1}})1_g)) \\
&= \alpha_h(x1_{h^{-1}})1_g \\
&= 1_g\theta(x)(h).
\end{aligned}$$

Agora, vejamos que θ é homomorfismo de A^α-módulos à esquerda. De fato, para

todo $a \in A^\alpha$, $x \in A$ e $h \in G$, temos

$$\theta(ax)(h) = \alpha_h(ax1_{h^{-1}}) = \alpha_h(a1_{h^{-1}})\alpha_h(x1_{h^{-1}}) = a\alpha_h(x1_{h^{-1}}) = a\theta(h).$$

Seja $x \in Ker(\theta)$. Então, $0 = \theta(x)$. Consequentemente, $\alpha_h(x1_{h^{-1}}) = \theta(x)(h) = 0$, para todo $h \in G$. Em particular, para $h = 1$ temos $0 = \alpha_1(x1_1) = x$. Logo, θ é injetora.

Mais ainda, θ é sobrejetora, pois dado $f \in \mathcal{F}^G$, escolhemos $x = f(1)$. Então

$$\theta(x)(h) = \alpha_h(f(1)1_{h^{-1}}) = \alpha_h(f(h^{-1}h)1_{h^{-1}}) = (1_h u_h \cdot f)(h) = 1_h f(h) = f(h),$$

para todo $h \in G$. Disto segue que, $\theta(x) = f$.

Logo, θ é isomorfismo de A^α-módulos à esquerda.

Portanto, $\mu \circ (Id_A \otimes \theta) : A \otimes A \to \prod_{g\in G} D_g$ dada por $\mu \circ (Id_A \otimes \theta)(x \otimes y) = (x\theta(y)(g))_{g\in G}$ é um isomorfismo de A-módulos à esquerda claramente igual a ψ.

(iv) $\Rightarrow$ (i) Considere $(\underbrace{1_A, 0, \cdots, 0}_{|G| \ vezes}) \in \prod_{g\in G} D_g$, onde a primeira entrada corresponde a $g = 1$. Como ψ é isomorfismo, então existe $\sum_{i=1}^{n} x_i \otimes y_i \in A \otimes A$ tal que $\psi(\sum_{i=1}^{n} x_i \otimes y_i) = (1_A, 0, \cdots, 0)$. Assim temos que $\sum_{i=1}^{n} x_i\alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g}1_A$. □

Observação 2.1.3. *Se A for comutativo então o isomorfismo ψ da afirmação (iv) é também de A^α-álgebras.*

Corolário 2.1.4. *Seja A uma extensão de Galois α-parcial de A^α. Então,*

(i) Existe um elemento $c \in A$ tal que $tr_\alpha(c) = \sum_{g\in G} \alpha_g(c1_{g^{-1}}) = 1_A$.

(ii) A^α é isomorfo a um somando direto de A como A^α-módulo.

(iii) Sejam S uma A^α-álgebra comutativa com unidade 1_S e

$$\gamma = (\{S \otimes D_g\}, \{\gamma_g = 1_S \otimes \alpha_g\})_{g\in G}$$

a ação parcial de G sobre $S \otimes A$ induzida por α via

$$\gamma_g(s \otimes x1_{g^{-1}}) = s \otimes \alpha_g(x1_{g^{-1}}),$$

para todo $x \in A, s \in S, g \in G$. Então $S \otimes A$ é uma extensão de Galois γ-parcial de S.

Demonstração.

(i) Pela Observação 1.2.15 temos que $tr_\alpha(A) \subseteq A^\alpha$ e tr_α é A^α-linear. Consideremos o isomorfismo de A-módulos à esquerda $\varphi : A \star_\alpha G \to End_{A^\alpha}(A)$ da afirmação (ii) de Teorema 2.1.2 definido por $\varphi(\sum_{g\in G} x_g u_g)(x) = \sum_{g\in G} x_g\alpha_g(x1_{g^{-1}})$, para todo $x \in A$. Observemos que, para todo $x \in A$,

$$\varphi(\sum_{g\in G} u_g)(x) = \sum_{g\in G} \alpha_g(x1_{g^{-1}}) = tr_\alpha(x),$$

e consequentemente $tr_\alpha = \varphi(\sum_{g\in G} u_g)$. Seja $t = \sum_{g\in G} u_g \in A \star_\alpha G$, assim $tr_\alpha = \varphi(t)$.

Afirmação: $Hom_{A^\alpha}(A, A^\alpha) = \varphi(tA)$, ou seja, tr_α gera $Hom_{A^\alpha}(A, A^\alpha)$ como A-módulo à direita. De fato, para quaisquer $x, y \in A$, temos

$$\varphi(tx) = \varphi((\sum_{g\in G} u_g)(xu_1)) = \varphi(\sum_{g\in G} \alpha_g(x1_{g^{-1}})u_g)$$

e, portanto,

$$\begin{aligned}
\varphi(tx)(y) &= \varphi(\sum_{g\in G} \alpha_g(x1_{g^{-1}})u_g)(y) \\
&= \sum_{g\in G} \alpha_g(x1_{g^{-1}})\alpha_g(y1_{g^{-1}}) \\
&= \sum_{g\in G} \alpha_g(xy1_{g^{-1}}) \\
&= tr_\alpha(xy) \in A^\alpha.
\end{aligned}$$

Isto prova que $\varphi(tA) \subseteq Hom_{A^\alpha}(A, A^\alpha)$. Sejam $f \in Hom_{A^\alpha}(A, A^\alpha) \subseteq Hom_{A^\alpha}(A, A)$ e seja $w = \sum_{g\in G} x_g u_g \in A \star_\alpha G$ tal que $\varphi(w) = f$. Então, para todo $x \in A$, $\varphi(w)(x) = f(x) \in A^\alpha$, ou seja, $\sum_{g\in G} x_g\alpha_g(x1_{g^{-1}}) \in A^\alpha$. Logo, para todo $k \in G$,

$$\alpha_k(\sum_{g\in G} x_g\alpha_g(x1_{g^{-1}})1_{k^{-1}}) = \sum_{g\in G} x_g\alpha_g(x1_{g^{-1}})1_k,$$

implicando que

$$\begin{aligned}\sum_{g\in G} x_g\alpha_g(x1_{g^{-1}})1_k &= \alpha_k(\sum_{g\in G} x_g\alpha_g(x1_{g^{-1}})1_{k^{-1}})\\ &= \sum_{g\in G}\alpha_k(x_g1_{k^{-1}})\alpha_k(\alpha_g(x1_{g^{-1}})1_{k^{-1}})\\ &= \sum_{g\in G}\alpha_k(x_g1_{k^{-1}})\alpha_{kg}(x1_{(kg)^{-1}})1_k\\ &= \sum_{h\in G}\alpha_k(x_{k^{-1}h}1_{k^{-1}})\alpha_h(x1_{h^{-1}}),\end{aligned}$$

para qualquer $x \in A$. Então, para todo $x \in A$,

$$\varphi(\sum_{g\in G} x_g1_ku_g)(x) = \varphi(\sum_{g\in G}\alpha_k(x_{k^{-1}g}1_{k^{-1}})u_g)(x).$$

Como φ é isomorfismo, então

$$\sum_{g\in G} x_g1_ku_g = \sum_{g\in G}\alpha_k(x_{k^{-1}g}1_{k^{-1}})u_g.$$

Isto implica que $x_g1_k = \alpha_k(x_{k^{-1}g}1_{k^{-1}})$, para todo $k, g \in G$. Em particular, para $g = k$, temos $x_g = x_g1_g = \alpha_g(x_11_{g^{-1}})$, para todo $g \in G$.

Em consequência,

$$w = \sum_{g\in G} x_gu_g = \sum_{g\in G}\alpha_g(x_11_{g^{-1}})u_g = (\sum_{g\in G} u_g)(x_1u_1) = (\sum_{g\in G} u_g)x_1 = tx_1.$$

Portanto, $f = \varphi(w) = \varphi(tx_1) \in \varphi(tA)$. Portanto $Hom_{A^\alpha}(A, A^\alpha) = \varphi(tA)$. Isto conclui a prova da afirmação.

Portanto para todo $f \in Hom_{A^\alpha}(A, A^\alpha)$, existe $y \in A$ tal que $f = \varphi(ty) = \varphi(\sum_{g\in G} u_gy) = \varphi(\sum_{g\in G} u_g(yu_1)) = \varphi(\sum_{g\in G}\alpha_g(y1_{g^{-1}})u_g)$ e, consequentemente, $f(x) = \varphi(\sum_{g\in G}\alpha_g(y1_{g^{-1}})u_g)(x) = \sum_{g\in G}\alpha_g(y1_{g^{-1}})\alpha_g(x1_{g^{-1}}) = \sum_{g\in G}\alpha_g(yx1_{g^{-1}}) = tr_\alpha(yx)$, qualquer que seja $x \in A$. Isto mostra que para toda $f \in Hom_{A^\alpha}(A, A^\alpha)$, $f = tr_\alpha(y-)$, para algum $y \in A$.

Por outro lado, A é um A^α-módulo projetivo finitamente gerado (por (ii) do Teorema 2.1.2), fiel (pois $A^\alpha \subseteq A$) e A^α é comutativo (pois está contido no centro de A). Portanto, pelo Corolário 1.1.5, existem $f_1, \cdots, f_n \in Hom_{A^\alpha}(A, A^\alpha)$ e

$x_1, \cdots, x_n \in A$ tais que $\sum_{i=1}^{n} f_i(x_i) = 1_A$. Sabemos que existem $y_1, \cdots, y_n \in A$ tais que $f_i = tr_\alpha(y_i -)$, logo

$$1_A = \sum_{i=1}^{n} f_i(x_i) = \sum_{i=1}^{n} tr_\alpha(y_i x_i) = tr_\alpha(\sum_{i=1}^{n}(y_i x_i)) = tr_\alpha(c)$$

para $c = \sum_{i=1}^{n}(y_i x_i) \in A$.

(ii) Por (i) existe $c \in A$ tal que $tr_\alpha(c) = 1_A$. Portanto, $tr_\alpha : A \to A^\alpha$ é um homomorfismo de A^α-módulos sobrejetor e, consequentemente, a sequência

$$A \xrightarrow{tr_\alpha} A^\alpha \longrightarrow 0$$

é exata. Definimos $\theta : A^\alpha \to A$ por $\theta(x) = xc$, para todo $x \in S^\alpha$. Note que θ é um homomorfismo de A^α-módulos. Temos que $tr_\alpha \circ \theta(x) = tr_\alpha(xc) = xtr_\alpha(c) = x$, consequentemente $tr_\alpha \circ \theta = Id_{A^\alpha}$. Logo a sequência exata $A \xrightarrow{tr_\alpha} A^\alpha \longrightarrow 0$ cinde e $A \simeq A^\alpha \oplus ker(tr_\alpha)$.

(iii) Como, por (ii), $A \simeq A^\alpha \oplus N$, para algum A^α-módulo N, então

$$S \otimes A = (S \otimes A^\alpha) \oplus (S \otimes N)$$

e podemos identificar S com $(S \otimes A^\alpha)$ em $S \otimes A$. Sejam $\{x_i, y_i\}_{1 \leq i \leq n}$ as coordenadas de Galois α-parciais de A sobre A^α, ou seja, $\sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} 1_A$, para todo $g \in G$. Então, $\{1_S \otimes x_i, 1_S \otimes y_i\}_{1 \leq i \leq n} \subset S \otimes A$ e $\sum_{i=1}^{n}(1_S \otimes x_i)\gamma_g(1_S \otimes y_i 1_{g^{-1}}) = \sum_{i=1}^{n}(1_S \otimes x_i)(1_S \otimes \alpha_g(y_i 1_{g^{-1}})) = 1_S \otimes \sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) = 1_S \otimes \delta_{1,g} 1_A = \delta_{1,g} 1_S$.

Agora resta mostrar que $(S \otimes A)^\gamma = S \otimes A^\alpha = S$.

Sejam $\sum_{i=1}^{n} s_i \otimes x_i \in (S \otimes A)^\gamma$ e $c \in A$, tal que $tr_\alpha(c) = 1_A$. Então

$$\begin{aligned} \sum_{i=1}^{n} s_i \otimes x_i &= (\sum_{i=1}^{n} s_i \otimes x_i)(1_S \otimes 1_A) \\ &= (\sum_{i=1}^{n} s_i \otimes x_i)(1_S \otimes tr_\alpha(c)) \\ &= \sum_{i=1}^{n} s_i \otimes x_i tr_\alpha(c) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} s_i \otimes x_i \sum_{g\in G} \alpha_g(c1_{g^{-1}}) \\
&= \sum_{g\in G}\sum_{i=1}^{n} s_i \otimes x_i\alpha_g(c1_{g^{-1}}) \\
&= \sum_{g\in G}\sum_{i=1}^{n} (s_i \otimes x_i1_g)(1_S \otimes \alpha_g(c1_{g^{-1}})) \\
&= \sum_{g\in G}\sum_{i=1}^{n} (s_i \otimes \alpha_g(x1_{g^{-1}}))(1_S \otimes \alpha_g(c1_{g^{-1}})) \\
&= \sum_{i=1}^{n} s_i \otimes \sum_{g\in G} \alpha_g(x_i1_{g^{-1}})\alpha_g(c1_{g^{-1}}) \\
&= \sum_{i=1}^{n} s_i \otimes \sum_{g\in G} \alpha_g(x_ic1_{g^{-1}}) \\
&= \sum_{i=1}^{n} s_i \otimes tr_\alpha(x_ic) \in S \otimes A^\alpha \simeq S.
\end{aligned}
$$

Reciprocamente, para todo $\sum_{i=1}^{n} s_i \otimes x_i \in S \otimes A^\alpha = S$, temos que

$$\gamma_g(\sum_{i=1}^{n} s_i \otimes x_i1_{g^{-1}}) = \sum_{i=1}^{n} s_i \otimes \alpha_g(x_i1_{g^{-1}}) = \sum_{i=1}^{n} s_i \otimes x_i1_g = (\sum_{i=1}^{n} s_i \otimes x_i)(1_S \otimes 1_g),$$

qualquer que seja $g \in G$. Portanto $S \simeq S \otimes A^\alpha \subseteq (S \otimes A)^\gamma$.

Isto completa a demonstração do corolário. □

Definição 2.1.5. *Denotamos por G_0 o conjunto $\{g \in G \mid D_g \neq 0\}$.*

Observemos que nos Exemplos 1.2.4, 1.2.6 e 1.2.7 todos ideais considerados considerados nas ações parciais são não nulos, assim, G_0 coincide com o grupo considerado em cada caso, sendo trivialmente um subgrupo. Já no Exemplo 1.2.5, $G_0 = \{1\}$, que é um subgrupo do grupo G. Porém, nem sempre G_0 é um subgrupo do grupo considerado na ação parcial, como podemos ver no próximo exemplo.

Exemplo 2.1.6. *Sejam R um anel com unidade, $A = R\times R$ e $G = \{1, g, g^2, g^3, g^4\}$, o grupo cíclico de ordem 5. Considere a seguinte ação parcial de G sobre A:*
$D_1 = A$, $D_g = D_{g^4} = \{0\} \times \{0\}$, $D_{g^2} = \{0\} \times R$ e $D_{g^3} = R \times \{0\}$; e isomorfismos $\alpha_1 = Id_A$, $\alpha_g = \alpha_{g^4}$ isomorfismos nulos, e:

$$
\begin{aligned}
\alpha_{g^2} : D_{g^3} &\to D_{g^2} \quad , \quad \alpha_{g^3} : D_{g^2} \to D_{g^3} \\
(a, 0) &\mapsto (0, a) \qquad\qquad (0, b) \mapsto (b, 0).
\end{aligned}
$$

Neste exemplo, $G_0 = \{1, g^2, g^3\}$ *que não é um subgrupo de* G*.*

Definição 2.1.7. *Dois elementos* $g, h \in G_0$ *são ditos* α*-fortemente distintos, se para qualquer idempotente não nulo* $e \in D_g \cup D_h$*, existe* $x \in A$ *tal que* $\alpha_g(x1_{g^{-1}})e \neq \alpha_h(x1_{h^{-1}})e$*.*

Proposição 2.1.8. *Seja* A *um anel comutativo. Então,* A *é uma extensão de Galois* α*-parcial de* A^α *se, e somente se,* A *é separável sobre* A^α *e os elementos de* G_0 *são dois a dois* α*-fortemente distintos.*

Demonstração. ($\Rightarrow$) Como A é uma extensão de Galois α-parcial de A^α, existem $x_i, y_i \in A, 1 \leq i \leq n$, tais que $\sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} 1_A$, para todo $g \in G$. Em particular para $g = 1$ temos $\sum_{i=1}^{n} x_i y_i = 1_A$. Escolhemos $e = \sum_{i=1}^{n} x_i \otimes y_i \in A^e = A \otimes A$. Mostraremos que e é um idempotente de separabilidade de A sobre A^α. De fato, seja $\mu : A^e \to A$ o homomorfismo de A^e-módulos induzido pela multiplicação de A, então $\mu(e) = \sum_{i=1}^{n} x_i y_i = 1_A$. Além disso, para todo $x \in A$ temos que:

$$\begin{aligned}
(x \otimes 1_A)e &= \sum_{i=1}^{n} x x_i \otimes y_i \\
&= \sum_{i=1}^{n} (\sum_{g \in G} \alpha_g(x x_i 1_{g^{-1}}) \delta_{1,g}) \otimes y_i \\
&= \sum_{i=1}^{n} (\sum_{g \in G} \alpha_g(x x_i 1_{g^{-1}}) \sum_{j=1}^{n} x_j \alpha_g(y_j 1_{g^{-1}})) \otimes y_i \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} x_j (\sum_{g \in G} \alpha_g(x x_i y_j 1_{g^{-1}})) \otimes y_i \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} x_j tr_\alpha(x x_i y_j) \otimes y_i \\
&= \sum_{j=1}^{n} x_j \otimes \sum_{i=1}^{n} tr_\alpha(x x_i y_j) y_i \\
&= \sum_{j=1}^{n} x_j \otimes \sum_{i=1}^{n} \sum_{g \in G} \alpha_g(x y_j 1_{g^{-1}}) \alpha_g(x_i 1_{g^{-1}}) y_i \\
&= \sum_{j=1}^{n} x_j \otimes \sum_{g \in G} \alpha_g(x y_j 1_{g^{-1}}) \sum_{i=1}^{n} \alpha_g(x_i 1_{g^{-1}}) y_i \\
&= \sum_{j=1}^{n} x_j \otimes \sum_{g \in G} \alpha_g(x y_j 1_{g^{-1}}) \delta_{1,g} \\
&= \sum_{j=1}^{n} x_j \otimes x y_j = (1_A \otimes x)e.
\end{aligned}$$

Portanto, A é separável sobre A^α.

Agora vamos provar que os elementos de G_0 são dois a dois α-fortemente distintos. Consideremos $g, h \in G_0$ e $e \in D_g \cup D_h$ um idempotente não nulo. Suponhamos que $\alpha_g(x1_{g^{-1}})e = \alpha_h(x1_{h^{-1}})e$, para todo $x \in A$. Se $e \in D_g$, aplicando $\alpha_{g^{-1}}$ em ambos os lados da igualdade, obtemos $x\alpha_{g^{-1}}(e) = \alpha_{g^{-1}h}(x1_{h^{-1}g})\alpha_{g^{-1}}(e)$ para todo $x \in A$. Usando esta última igualdade para $x = y_i$ temos

$$\alpha_{g^{-1}}(e) = 1_A\alpha_{g^{-1}}(e) = \sum_{i=1}^{n} x_i y_i \alpha_{g^{-1}}(e) = \sum_{i=1}^{n} x_i \alpha_{g^{-1}h}(y_i 1_{h^{-1}g})\alpha_{g^{-1}}(e) = \delta_{1,g^{-1}h}\alpha_{g^{-1}}(e).$$

Como e é não nulo, então $\alpha_{g^{-1}}(e) \neq 0$, logo $g^{-1}h = 1$, ou seja, $g = h$. Se $e \in D_h$, aplicamos $\alpha_{h^{-1}}$ em ambos os lados da igualdade e, por argumento análogo, também concluímos que $g = h$. Portanto, se $g \neq h$, então existe $x \in A$ tal que $\alpha_g(x1_{g^{-1}})e \neq \alpha_h(x1_{h^{-1}})e$.

($\Leftarrow$) Suponhamos que A é uma álgebra separável sobre A^α e os elementos de G_0 são dois a dois α-fortemente distintos. Para $g \in G_0$, considere o homomorfismo de A-álgebras $\theta_g : A \otimes A \to A \otimes D_g$, definido por $\theta_g(x \otimes y) = x \otimes \alpha_g(y1_{g^{-1}})$, para quaisquer $x, y \in A$. Seja $e = \sum_{i=1}^{n} x_i \otimes y_i \in A \otimes A$ o idempotente de separabilidade de A sobre A^α e $\mu : A \otimes A \to A$ o homomorfismo de $A \otimes A$-módulos induzido pela multiplicação de A. Assim, temos que $\mu(e) = \sum_{i=1}^{n} x_i y_i = 1_A$ e $(x \otimes 1_A - 1_A \otimes x)e = 0$, para todo $x \in A$. Observamos que μ é um homomorfismo de anéis, pois A é comutativo. Para todo $g \in G_0$, seja $e_g = \mu(\theta_g(e)) = \sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) \in D_g$. Logo, para qualquer $g \in G_0$, temos $e_g^2 = \mu(\theta_g(e))\mu(\theta_g(e)) = \mu(\theta_g(e)\theta_g(e)) = \mu(\theta_g(e^2)) = \mu(\theta_g(e)) = e_g$, ou seja, e_g é um idempotente em D_g. Além disso, para todo $x \in A$, também temos que

$$\begin{aligned} xe_g &= x\mu(\theta_g(e)) = x1_g\mu(\theta_g(e)) \\ &= \mu(x \otimes 1_g)\mu(\theta_g(e)) = \mu((x \otimes 1_g)\theta_g(e)) \\ &= \mu(\theta_g(x \otimes 1_A)\theta_g(e)) = \mu(\theta_g((x \otimes 1_A)e)) \\ &= \mu(\theta_g((1_A \otimes x)e)) = \mu(\theta_g(1_A \otimes x)\theta_g(e)) \end{aligned}$$

$$
\begin{aligned}
&= \mu((1_A \otimes \alpha_g(x1_{g^{-1}}))\theta_g(e)) = \mu(1_A \otimes \alpha_g(x1_{g^{-1}}))\mu(\theta_g(e)) \\
&= \mu(1_A \otimes \alpha_g(x1_{g^{-1}}))e_g = \alpha_g(x1_{g^{-1}})e_g.
\end{aligned}
$$

Como os elementos de G_0 são dois a dois α-fortemente distintos, então $e_g = 0$ ou $g = 1$ e portanto, para todo $g \in G_0$, $\delta_{1,g} = e_g = \sum_{i=1}^{n} x_i\alpha_g(y_i1_{g^{-1}})$. Se $g \notin G_0$, então $1_g = 1_{g^{-1}} = 0$ e $\sum_{i=1}^{n} x_i\alpha_g(y_i1_{g^{-1}}) = 0$. Uma vez que $1 \in G_0$, pois $D_1 = A$, então $\sum_{i=1}^{n} x_i\alpha_g(y_i1_{g^{-1}}) = \delta_{1,g}$, para todo $g \in G$. □

Definição 2.1.9. *Sejam $\phi, \psi : S \to A$ homomorfismos de anéis tais que existem $g, h \in G_0$ satisfazendo $\phi(S) \subseteq D_g$ e $\psi(S) \subseteq D_h$. Dizemos que ϕ e ψ são homomorfismos α-fortemente distintos se, para todo idempotente não nulo $e \in D_g \cup D_h$, existe um elemento $s \in S$ tal que $\phi(s)e \neq \psi(s)e$.*

Exemplo 2.1.10. *Os homomorfismos $\alpha_g(\_\_1_{g^{-1}})$ e $\alpha_h(\_\_1_{h^{-1}})$ da ação parcial dada no exemplo 1.2.6 são α-fortemente distintos. De fato, $\alpha_g(A1_{g^{-1}}) \subseteq D_g$, $\alpha_h(A1_{h^{-1}}) \subseteq D_h$ e temos os seguintes idempotente não nulos em $D_g \cup D_h$: $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1), e_4 = (1,1,0), e_5 = (0,1,1), e_6 = (1,0,1)$ e $e_7 = (1,1,1)$. Tomando $x = (a,b,c) \in A$ com a,b,c todos não nulos e dois a dois distintos temos que $\alpha_g(x1_{g^{-1}}) = (c,0,a)$ e $\alpha_h(x1_{h^{-1}}) = (b,a,0)$. Assim, temos que $\alpha_g(x1_{g^{-1}})e_i \neq \alpha_h(x1_{h^{-1}})e_i$, para todo $i = 1, \cdots, 7$. De maneira análoga podemos mostrar que $\alpha_g(\_\_1_{g^{-1}})$, $\alpha_{gh}(\_\_1_{(gh)^{-1}})$ e $\alpha_h(\_\_1_{h^{-1}})$, são homomorfismos dois a dois α-fortemente distintos.*

Exemplo 2.1.11. *No exemplo 1.2.7 temos um caso de uma ação parcial com homomorfismos que não são α-fortemente distintos. De fato, tomando $e = (0,1,0)$, não existe $x \in S$ que satisfaça a Definição 2.1.9, para todo par de elementos de G.*

Lema 2.1.12. *Sejam A uma anel comutativo com unidade, S uma A-álgebra comutativa separável com elemento identidade 1_S e $f : S \to A$ um homomorfismo de A-álgebras. Então, existe um único idempotente $w \in S$ tal que $f(w) = 1_A$ e $sw = f(s)w$, para todo $s \in S$.*

Demonstração. Como S é um A-álgebra separável existem elementos $r_1, \cdots, r_n$, $s_1, \cdots, s_n \in S$ tais que $\sum_{j=1}^{n} r_j s_j = 1_S$ e $\sum_{j=1}^{n} sr_j \otimes_A s_j = \sum_{j=1}^{n} r_j \otimes_A s_j s$, para todo $s \in S$. Seja $f : S \to A$ um homomorfismo de A-álgebras e $w = \sum_{j=1}^{n} f(r_j)s_j \in S$, então

$$f(w) = f(\sum_{j=1}^{n} f(r_j)s_j) = \sum_{j=1}^{n} f(r_j)f(s_j) = f(\sum_{j=1}^{n} r_j s_j) = f(1_S) = 1_A.$$

Agora, para todo $r \in S$, temos:

$$\begin{aligned}
(f \otimes_A Id_S)(\sum_{j=1}^{n} rr_j \otimes_A s_j) &= (f \otimes_A Id_S)(\sum_{j=1}^{n} r_j \otimes_A s_j r) \\
\Rightarrow \sum_{j=1}^{n} f(rr_j) \otimes_A s_j &= \sum_{j=1}^{n} f(r_j) \otimes_A s_j r \\
\Rightarrow \sum_{j=1}^{n} 1_A \otimes_A f(rr_j)s_j &= \sum_{j=1}^{n} 1_A \otimes_A f(r_j)s_j r \\
\Rightarrow 1_A \otimes_A f(r)w &= 1_A \otimes_A rw.
\end{aligned}$$

Aplicando a esta igualdade o $S \otimes_A S$-homomorfismo $\mu : S \otimes_A S \to S$ induzido pela multiplicação de S obtemos $f(r)w = rw$. Se fizermos $r = 1_S$, teremos $w = 1_S w = f(1_S)w = 1_A w = f(w)w = w^2$.

Se w' é outro idempotente de S que satisfaz $f(w') = 1_A$ e $f(r)w' = rw'$, para todo $r \in S$, então $w' = 1_A w' = f(w)w' = ww' = w'w = f(w')w = 1_A w = w$. □

Lema 2.1.13. *Seja A uma anel comutativo com unidade, S uma A-álgebra comutativa separável com elemento identidade 1_S. Se $f_1, \cdots, f_n$ são homomorfismos de A-álgebras de S em A dois a dois α-fortemente distintos, tais que $f_i(S) \subseteq D_{g_i}$, com $g_i \in G_0$, então os correspondentes idempotentes $w_1, \cdots, w_n$ satisfazendo o Lema anterior, são dois a dois ortogonais e $f_i(w_j) = \delta_{ij}$.*

Demonstração. Sejam $f_1, \cdots, f_r : S \to A$ homomorfismos de A-álgebras dois a dois α-fortemente distintos e tais que $f_i(S) \subseteq D_{g_i}$, com $g_i \in G_0$. Sejam $w_1, \cdots, w_r \in S$ os correspondentes idempotentes que verificam $f_i(w_i) = 1_A$ e $f_i(s)w_i = sw_i$, para

todo $s \in S$. Observemos que $w_{ij} = f_i(w_j) \in D_{g_i}$ é idempotente em D_{g_i} pois $w_{ij}^2 = (f_i(w_j))^2 = f_i(w_j^2) = f_i(w_j) = w_{ij}$, para $i, j = 1, \cdots, n$. Também temos que, $f_i(s)w_{ij} = f_i(s)f_i(w_j) = f_i(sw_j) = f_i(f_j(s)w_j) = f_j(s)f_i(w_j) = f_j(s)w_{ij}$, para todo $s \in S$. Como f_i e f_j são α-fortemente distintos se $i \neq j$, concluímos que $w_{ij} = f_i(w_j) = 0$ sempre que $i \neq j$. Logo $f_i(w_j) = \delta_{ij}$, para $i, j = 1, \cdots, n$. Finalmente, $w_i w_j = f_j(w_i)w_j = \delta_{ij}w_j = 0$, se $i \neq j$. □

2.2 A correspondência de Galois

Nesta seção vamos provar o Teorema Fundamental da Teoria de Galois Parcial. Para tanto vamos assumir que toda extensão de Galois α-parcial é comutativa.

Seja $\mathcal{F} = \{f : G \to A \mid f(g) \in D_g, \text{ para todo } g \in G\}$. Note que $\mathcal{F}$ é uma A-álgebra com adição e multiplicação pontuais (em particular é uma A^α-álgebra).

Lema 2.2.1. *Seja A uma extensão de Galois α-parcial de A^α. Então, existe uma ação parcial α' de G sobre a álgebra $\mathcal{F}$ tal que $\mathcal{F}$ é uma extensão de Galois α'-parcial de A.*

Demonstração. Pelo Corolário 2.1.4, item 3, $A \otimes A$ é uma extensão de Galois γ-parcial de A, onde γ é uma ação parcial de G sobre $A \otimes A$ induzida pela ação parcial α via $\gamma_g(x \otimes y1_{g^{-1}}) = x \otimes \alpha_g(y1_{g^{-1}}), x, y \in A$. Além disso, temos que $\mathcal{F} \simeq \prod_{g \in G} D_g$ como A^α-álgebras, via:

$$\begin{aligned} \phi : \ \mathcal{F} &\to \prod_{g \in G} D_g \\ f &\mapsto (f(g))_{g \in G} \end{aligned}$$

com inversa dada por:

$$\begin{aligned} \phi^{-1} : \ \prod_{g \in G} D_g &\to \mathcal{F} \\ (x_g)_{g \in G} &\mapsto f : G \to A, f(g) = x_g, \forall g \in G. \end{aligned}$$

Pela observação 2.1.3, a aplicação

$$\begin{aligned} \psi: \quad A \otimes A &\to \prod_{g\in G} D_g \\ x \otimes y &\mapsto (x\alpha_g(y1_{g^{-1}}))_{g\in G} \end{aligned}$$

é um isomorfismo de A^α-álgebras. Logo, a aplicação $\eta = \phi^{-1} \circ \psi$ dada por

$$\begin{aligned} \eta: \quad A \otimes A &\to \mathcal{F} \\ x \otimes y &\mapsto \eta(x \otimes y) : G \to A, \end{aligned}$$

onde $\eta(x \otimes y)(g) = x\alpha_g(y1_{g^{-1}})$, para todo $g \in G$, é um isomorfismo de A^α-álgebras.

Este isomorfismo induz uma ação parcial $\alpha' = (\{\mathcal{F}_g\}, \{\alpha'_g\})_{g\in G}$ de G sobre $\mathcal{F} = \eta(A \otimes A)$ onde os ideais são dados por $\mathcal{F}_g = \eta(A \otimes D_g) = \eta((A \otimes A)(1_A \otimes 1_g)) = \eta(A\otimes A)\eta(1_A\otimes 1_g)$. Os isomorfismos são definidos de forma que o seguinte diagrama seja comutativo

$$\begin{array}{ccc} \mathcal{F}_{g^{-1}} & \xrightarrow{\alpha'_g} & \mathcal{F}_g \\ {\scriptstyle\simeq\eta}\uparrow & & \uparrow{\scriptstyle\simeq\eta} \\ A \otimes D_{g^{-1}} & \xrightarrow[\gamma_g]{} & A \otimes D_g \end{array}$$

ou seja, $\alpha'_g = \eta \circ \gamma_g \circ \eta^{-1}$.

Desta forma, $\mathcal{F}$ é uma extensão de Galois α'-parcial de A. □

Seja A uma extensão de Galois α-parcial de A^α. Para cada subgrupo H de G a restrição

$$\alpha_H = (\{D_h\}, \{\alpha_h\})_{h\in H}$$

de α a H é claramente uma ação parcial de H sobre A. Denotemos

$$A^{\alpha_H} = \{x \in A \mid \alpha_h(x1_{h^{-1}}) = x1_h, \textit{ para todo } h \in H\}$$

e observamos que A^{α_H} é sempre uma A^α-subálgebra de A.

Lema 2.2.2. *Seja A uma extensão de Galois α-parcial de A^α e H um subgrupo de G. Então, $f \in \mathcal{F}^{\alpha'_H}$ se, e somente se, $f(gh)1_g = f(g)1_{gh}$, para quaisquer $h \in H, g \in G$.*

Demonstração. Considere $f \in \mathcal{F}^{\alpha'_H}$, pela demonstração do Lema 2.2.1, a aplicação $\eta : A \otimes A \to \mathcal{F}$ dada por $\eta(x \otimes y)(g) = x\alpha_g(y1_{g^{-1}})$, para quaisquer $x, y \in A$, e $g \in G$, é um isomorfismo de A^α-álgebras. Logo, existe $x \otimes y \in A \otimes A$ tal que $f = \eta(x \otimes y)$. Assim,

$$
\begin{aligned}
& \eta(x \otimes y) \in \mathcal{F}^{\alpha'_H} \Leftrightarrow \\
\Leftrightarrow \quad & \alpha'_h(\eta(x \otimes y1_{h^{-1}})) = \eta(x \otimes y1_h), \text{ para todo } h \in H \\
\Leftrightarrow \quad & \eta(\gamma_h(x \otimes y1_{h^{-1}})) = \eta(x \otimes y1_h), \text{ para todo } h \in H \\
\Leftrightarrow \quad & \eta(x \otimes \alpha_h(y1_{h^{-1}})) = \eta(x \otimes y1_h), \text{ para todo } h \in H \\
\Leftrightarrow \quad & \eta(x \otimes \alpha_h(y1_{h^{-1}}))(g) = \eta(x \otimes y1_h)(g), \text{ para todo } h \in H, g \in G \\
\Leftrightarrow \quad & x\alpha_g(\alpha_h(y1_{h^{-1}})1_{g^{-1}}) = x\alpha_g(y1_h1_{g^{-1}}), \text{ para todo } h \in H, g \in G \\
\Leftrightarrow \quad & x\alpha_{gh}(y1_{(gh)^{-1}})1_g = x\alpha_g(y1_{g^{-1}})\alpha_g(1_h1_{g^{-1}}), \text{ para todo } h \in H, g \in G \\
\Leftrightarrow \quad & x\alpha_{gh}(y1_{(gh)^{-1}})1_{gh}1_g = x\alpha_g(y1_{g^{-1}})1_g1_{gh}, \text{ para todo } h \in H, g \in G \\
\Leftrightarrow \quad & \eta(x \otimes y)(gh)1_{gh}1_g = \eta(x \otimes y)(g)1_g1_{gh}, \text{ para todo } h \in H, g \in G \\
\Leftrightarrow \quad & f(gh)1_{gh}1_g = f(g)1_g1_{gh}, \text{ para todo } h \in H, g \in G \\
\Leftrightarrow \quad & f(gh)1_g = f(g)1_{gh}, \text{ para todo } h \in H, g \in G.
\end{aligned}
$$

□

Para cada A^α-subálgebra T de A definimos

$$H_T = \{g \in G \mid \alpha_g(t1_{g^{-1}}) = t1_g, \textit{para todo } t \in T\}.$$

Definição 2.2.3. *Uma A^α-subálgebra T de A é dita α-forte, se para cada par de elementos $g, h \in G_0$, com $g^{-1}h \notin H_T$, os homomorfismos $\alpha_g(-1_{g^{-1}})$ e $\alpha_h(-1_{h^{-1}})$ de T em A são α-fortemente distintos.*

O conjunto H_T nem sempre é um subgrupo de G, nem mesmo se exigirmos que T seja A^α-separável e α-forte, como podemos ver no exemplo abaixo.

Exemplo 2.2.4. *([5], Exemplo 6.3) Seja A uma extensão de Galois (global) cíclica de um anel comutativo R com grupo de Galois G gerado por g de ordem 6. Considere*

o conjunto $S = \sum_{1\leq i\leq 5} \oplus Ae_i$, *onde* $\{e_i \mid 1 \leq i \leq 5\}$ *é um conjunto de idempotentes ortogonais não nulos cuja soma é um. Defina a ação parcial* α *de* G *sobre* S *tomando* $A_{g^i} = Ae_{6-i}$ *e* $\alpha_{g^i}(ae_i) = g^i(a)e_{6-i}$, $1 \leq i \leq 5$. *Portanto temos uma ação parcial de* G *sobre* S *e* $S^\alpha = \{ae_1 + be_2 + ce_3 + g^2(b)e_4 + g(a)e_5 \mid a, b \in A, c \in A^{g^3}\}$.

Sejam $a_i, b_i \in A, 1 \leq i \leq m$, *um sistema de coordenadas de Galois de* A *sobre* R *e considere os elementos* $x_j = y_j = e_j$, $j = 1, 2, 4, 5$ *juntamente com os elementos* $x_{i3} = a_ie_3$, $y_{i3} = b_ie_3$. *É fácil ver que isto fornece um sistema de coordenadas de Galois de* S *sobre* S^α. *Consequentemente* S *é uma extensão de Galois* α*-parcial de* S^α.

Temos duas subálgebras separáveis e α*-forte* T *de* S *não triviais com* H_T *um subgrupo de* G*:* $T_1 = \{x_1e_1 + x_2e_2 + x_3e_3 + g^2(x_2)e_4 + x_5e_5 \mid x_i \in A\}$ *e* $T_2 = \{x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 \mid x_3 \in A^{g^3}, x_i \in A \text{ para } i \neq 3\}$. *Além disso a subálgebra* $T = \{x_1e_1 + x_2e_2 + x_3e_3 + g^2(x_2)e_4 + g(x_1)e_5 \mid x_i \in A\}$ *é* S^α*-separável e* α*-forte, porém* $H_T = \{1, g, g^2, g^4, g^5\}$ *não é um subgrupo de* G.

O teorema fundamental da Teoria de Galois Parcial estabelece uma correspondência bijetora entre os subgrupos H de G e as A^α-subálgebras separáveis T de A que são α-fortes, tais que H_T é subgrupo de G, dado por:

$$\begin{aligned} H &\rightarrow A^{\alpha_H} \\ H_T &\leftarrow T. \end{aligned}$$

Teorema 2.2.5. ***(Teorema Fundamental da Teoria de Galois Parcial)*** *Seja* A *uma extensão de Galois* α*-parcial de* A^α, *tal que* α *é uma ação parcial de um grupo finito* G *sobre um anel unitário* A.

(i) Seja H *um subgrupo de* G *e* $T = A^{\alpha_H}$. *Então* A *é uma extensão de Galois* α_H*-parcial de* T. *Além disso,* T *é* A^α*-separável,* α*-forte e* $H_T = H$.

(ii) Seja T *uma* A^α*-subálgebra separável e* α*-forte de* A *tal que* H_T *é um subgrupo de* G. *Então,* $A^{\alpha_H} = T$ *para* $H = H_T$.

Demonstração.

(i) Sejam $x_i, y_i, 1 \leq i \leq n$, as coordenadas de Galois α-parciais de A sobre A^α, ou seja, $\sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} 1_A$, para cada $g \in G$. Então a igualdade anterior vale para cada $g \in H$ e, consequentemente, A é uma extensão de Galois α_H-parcial de $T = A^{\alpha_H}$.

Como A é uma extensão de Galois α_H-parcial de T, então, pelo Teorema 2.1.2, item (ii), A é um T-módulo projetivo finitamente gerado. Assim, existe $r \in \mathbb{Z}^+$ e L um T-módulo projetivo tal que $T^r = A \oplus L$. Mais ainda, $A \otimes A$ é um $T \otimes T$-módulo projetivo, pois $(T \otimes T)^{r^2} = T^r \otimes T^r = (A \oplus L) \otimes (A \oplus L) = (A \otimes A) \oplus M$, onde $M = (A \otimes L) \oplus (L \otimes A) \oplus (L \otimes L)$.

Por outro lado, pela Proposição 2.1.8, A é separável sobre A^α e, por definição, A é um $A \otimes A$-módulo projetivo. Assim existe $s \in \mathbb{Z}^+$ e N um $A \otimes A$-módulo projetivo tal que $(A \otimes A)^s = A \oplus N$. Portanto $(T \otimes T)^{r^2 s} \simeq (A \otimes A)^s \oplus M^s = A \oplus N \oplus M^s$. Logo, podemos concluir que A é um $T \otimes T$-módulo projetivo. Como A é uma extensão de Galois α_H-parcial de T, então T é isomorfo a um somando direto de A como T-módulo pelo Corolário 2.1.4, item 2, e consequentemente um A^α-módulo somando direto de A. Então, $(T \otimes T)^{r^2 s} = A \oplus N \oplus M^s = T \oplus ker(tr_{\alpha_H}) \oplus N \oplus M^s$ e como consequência T um $T \otimes T$-módulo projetivo, o que é equivalente a T ser A^α-separável.

Agora vamos mostrar que T é α-forte. Como A é uma extensão de Galois α_H-parcial de T, segue do corolário 2.1.4, item 1, que existe $c \in A$ tal que $tr_{\alpha_H}(c) = \sum_{h \in H} \alpha_h(c 1_{h^{-1}}) = 1_A$. Consideremos novamente $\{x_i, y_i\}_{1 \leq i \leq n}$ as coordenadas de Galois α-parciais de A sobre A^α. Sejam $x_i' = tr_{\alpha_H}(x_i c) = \sum_{h \in H} \alpha_h(x_i c 1_{h^{-1}})$ e $y_i' = tr_{\alpha_H}(y_i) = \sum_{h \in H} \alpha_h(y_i 1_{h^{-1}})$, para $i = 1, \cdots, n$. Pela observação 1.2.15 temos que $x_i', y_i' \in T$, para todo $i = 1, \cdots, n$. Assim, dado $g \in G$, temos que:

$$\sum_{i=1}^{n} x_i' \alpha_g(y_i' 1_{g^{-1}}) \;=\; \sum_{i=1}^{n} \Big(\sum_{h \in H} \alpha_h(x_i c 1_{h^{-1}})\Big) \alpha_g\Big(\sum_{k \in H} \alpha_k(y_i 1_{k^{-1}}) 1_{g^{-1}}\Big)$$

$$
\begin{aligned}
&= \sum_{h,k\in H} \alpha_h(c1_{h^{-1}}) \sum_{i=1}^{n} \alpha_h(x_i 1_{h^{-1}})\alpha_g(\alpha_k(y_i 1_{k^{-1}})1_{g^{-1}}) \\
&= \sum_{h,k\in H} \alpha_h(c1_{h^{-1}}) \sum_{i=1}^{n} \alpha_h(x_i 1_{h^{-1}})\alpha_{gk}(y_i 1_{(gk)^{-1}})1_g \\
&= \sum_{h,k\in H} \alpha_h(c1_{h^{-1}}) \sum_{i=1}^{n} \alpha_h(x_i \alpha_{h^{-1}}(\alpha_{gk}(y_i 1_{(gk)^{-1}})1_h))1_g \\
&= \sum_{h,k\in H} \alpha_h(c1_{h^{-1}}) \sum_{i=1}^{n} \alpha_h(x_i \alpha_{h^{-1}gk}(y_i 1_{(h^{-1}gk)^{-1}})1_{h^{-1}})1_g \\
&= \sum_{h,k\in H} \alpha_h(c1_{h^{-1}})\alpha_h(\sum_{i=1}^{n} x_i \alpha_{h^{-1}gk}(y_i 1_{(h^{-1}gk)^{-1}})1_{h^{-1}})1_g \\
&= \sum_{h,k\in H} \alpha_h(c1_{h^{-1}})\alpha_h(\delta_{1,h^{-1}gk}1_A 1_{h^{-1}})1_g \\
&= \begin{cases} 1_g, se\ g \in H \\ 0, se\ g \notin H. \end{cases}
\end{aligned}
$$

Se escolhermos $g = 1$, na igualdade acima, teremos $\sum_{i=1}^{n} x_i' y_i' = 1_A$.

Sejam $g, h \in G_0$, tais que $g^{-1}h \notin H_T$. Temos que $H \subseteq H_T$, pela definição de H_T. Logo, $g^{-1}h \notin H$. Considere $e \in D_g \cup D_h$, um idempotente não nulo tal que $\alpha_g(t1_{g^{-1}})e = \alpha_h(t1_{h^{-1}})e$, para todo $t \in T$. Se $e \in D_g$, aplicando $\alpha_{g^{-1}}$ em ambos os lados da igualdade, obtemos $t\alpha_{g^{-1}}(e) = \alpha_{g^{-1}h}(t1_{h^{-1}g})\alpha_{g^{-1}}(e)$, para todo $t \in T$. Sejam $e' = \alpha_{g^{-1}}(e)$ e $t = y_i' \in T$, então

$$
e' = 1_A e' = (\sum_{i=1}^{n} x_i' y_i')e' = \sum_{i=1}^{n} x_i' \alpha_{g^{-1}h}(y_i' 1_{h^{-1}g})e' \overset{g^{-1}h\notin H}{=} 0e' = 0.
$$

Como $0 = e' = \alpha_{g^{-1}}(e)$, segue que $e = 0$, o que é uma contradição. Se $e \in D_h$, aplicamos $\alpha_{h^{-1}}$ em ambos os lados da igualdade, e também teremos um absurdo. Portanto, T é α-forte.

Observe que $A^{\alpha_{H_T}} = A^{\alpha_H} = T$. De fato, como $H \subseteq H_T$ temos $A^{\alpha_{H_T}} \subseteq A^{\alpha_H} = T$. Mais ainda, se $t \in T$, então $\alpha_g(t1_{g^{-1}}) = t1_g$, para todo $g \in H_T$, logo $T \subseteq A^{\alpha_{H_T}}$.

Pelo Teorema 2.1.2, item (iv), as aplicações

$$
\begin{aligned}
\psi : \quad A \otimes_T A &\to \prod_{h\in H} D_h \\
x \otimes y &\mapsto (x\alpha_h(y1_{h^{-1}}))_{h\in H}
\end{aligned}
$$

e

$$\begin{aligned} \widetilde{\psi}: \ A \otimes_T A &\to \prod_{h\in H_T} D_h \\ x\otimes y &\mapsto (x\alpha_h(y1_{h^{-1}}))_{h\in H_T} \end{aligned}$$

são isomorfismos de A-módulos à esquerda. Portanto $\prod_{h\in H} D_h \simeq \prod_{h\in H_T} D_h$. Como G é finito e $H_T \supseteq H$, então $H = H_T$.

(ii) Claramente $T \subseteq A^{\alpha_H}$. Agora vamos mostrar a inclusão contrária.

Pelo corolário 2.1.4, item 3, $A \otimes A$ é uma extensão de Galois γ-parcial de A, onde $\gamma = (\{A \otimes D_g\}, \{\gamma_g\})_{g\in G}$ é uma ação parcial de G sobre $A \otimes A$ induzida por α via $\gamma_g(x \otimes y1_{g^{-1}}) = x \otimes \alpha_g(y1_{g^{-1}})$, para quaisquer $x, y \in A$, e $g \in G$. Sendo $\mathcal{F} = \{v : G \to A \mid v(g) \in D_g, \text{ para todo } g \in G\}$ e $\eta : A \otimes A \to \mathcal{F}$ o isomorfismo de A^α-álgebras, dado por $\eta(x \otimes y)(g) = x\alpha_g(y1_{g^{-1}})$, temos, pelo lema 2.2.1, que $\mathcal{F}$ é uma extensão de Galois α'-parcial de A, onde $\alpha' = (\{\mathcal{F}_g = \eta(A \otimes D_g)\}$, $\{\alpha'_g = \eta \circ \gamma_g \circ \eta^{-1}\})_{g\in G}$ é uma ação parcial de G sobre $\mathcal{F}$. Como $\alpha'_g \circ \eta = \eta \circ \gamma_g$, para todo $g \in G$, e η é isomorfismo de A^α-álgebras, então para todo $v \in \mathcal{F}^{\alpha'_H}$ existe $x \otimes y \in A \otimes A$ tal que $v = \eta(x \otimes y)$. Portanto,

$$\begin{aligned} \eta(x\otimes y) \in \mathcal{F}^{\alpha'_H} &\Leftrightarrow \alpha'_h(\eta(x \otimes y1_{h^{-1}})) = \eta(x \otimes y1_h), \text{ para todo} h \in H \\ &\Leftrightarrow \eta(\gamma_h(x \otimes y1_{h^{-1}})) = \eta(x \otimes y1_h), \text{ para todo} h \in H \\ &\Leftrightarrow \eta(x\otimes y) \in \eta((A \otimes A)^{\gamma_H}). \end{aligned}$$

Então, temos que, $\mathcal{F}^{\alpha'_H} = \eta((A \otimes A)^{\gamma_H})$ e, consequentemente, $\eta^{-1}(\mathcal{F}^{\alpha'_H}) = (A \otimes A)^{\gamma_H}$.

Mais ainda, como $T \subseteq A^{\alpha_H} \subseteq A$ então as sequências

$$0 \to T \hookrightarrow A^{\alpha_H} \quad e \quad 0 \to A^{\alpha_H} \hookrightarrow A$$

são exatas. Pelo Teorema 2.1.2 item (ii), A é um A^α-módulo projetivo à esquerda, então, pelo Corolário 1.1.4, as sequências

$$0 \to A \otimes T \hookrightarrow A \otimes A^{\alpha_H} \quad e \quad 0 \to A \otimes A^{\alpha_H} \hookrightarrow A \otimes A$$

também são exatas. Logo, podemos identificar $A \otimes T$ com sua imagem em $A \otimes A^{\alpha_H}$ e $A \otimes A^{\alpha_H}$ com sua imagem em $A \otimes A$. Assim, temos que

$$A \otimes T \subseteq A \otimes A^{\alpha_H} \subseteq (A \otimes A)^{\gamma_H},$$

de onde seque que

$$\eta(A \otimes T) \subseteq \eta((A \otimes A)^{\gamma_H}) = \mathcal{F}^{\alpha'_H}.$$

Observemos que se $\mathcal{F}^{\alpha'_H} = \eta(A \otimes T)$ então $\eta^{-1}(\mathcal{F}^{\alpha'_H}) = A \otimes T$ e

$$A \otimes A^{\alpha_H} \subseteq (A \otimes A)^{\gamma_H} = \eta^{-1}(\mathcal{F}^{\alpha'_H}) = A \otimes T.$$

Aplicando $tr_\alpha \otimes 1_A$ a esta inclusão obtemos $tr_\alpha(A) \otimes A^{\alpha_H} \subseteq tr_\alpha(A) \otimes T$. Pelo Corolário 2.1.4, item 1, decorre que tr_α é sobrejetor em A^α e, portanto, $A^{\alpha_H} \simeq A^\alpha \otimes A^{\alpha_H} \subseteq A^\alpha \otimes T \simeq T$.

Portanto, para concluir a demonstração de 2 resta mostrar que $\mathcal{F}^{\alpha'_H} \subseteq \eta(A \otimes T)$.

Sejam $g_1, \cdots, g_r \in G$ representantes das classes laterais distintas de H em G. Seja $\{g_1, \cdots, g_k\}$ o subconjunto de $\{g_1, \cdots, g_r\}$, tal que $g_i \in G_0$, para todo $i = 1, \cdots, k$ e $g_1 = 1$. Para cada $1 \leq i \leq k$, seja $f_i : \mathcal{F} \to A$ o homomorfismo de A-álgebras definido por $f_i(v) = v(g_i)$, para todo $v \in \mathcal{F}$. Note que $v(g_i) \in D_{g_i}$, para todo $i = 1, \cdots, k$. Consideremos a restrição de f_i a $\eta(A \otimes T)$, para todo $i = 1, \cdots, k$.

Vamos mostrar que $f_1, \cdots, f_k : \eta(A \otimes T) \to A$ são homomorfismos de A-álgebras dois a dois α-fortemente distintos. Observemos que se $i, j \in \{1, \cdots, k\}$ são tais que $i \neq j$, então, como $H = H_T$, temos que $g_i^{-1} g_j \notin H_T$, pois se $g_i^{-1} g_j \in H_T$ então teríamos $g_j^{-1} g_i \in H$ e desta maneira $g_i H = g_j H$, o que é uma contradição pois g_i, g_j são representantes de classes laterais distintas de H em G. Portanto, como T é α-forte, então para cada par de elementos $g_i, g_j \in G_0$ com $g_i^{-1} g_j \notin H_T$ e para todo idempotente não nulo $e \in D_{g_i} \cup D_{g_j}$, existe $t \in T$ tal que $\alpha_{g_i}(t 1_{g_i^{-1}})e \neq \alpha_{g_j}(t 1_{g_j^{-1}})e$.

Logo,

$$f_i(\eta(1\otimes t))e = (\eta(1\otimes t)(g_i))e = \alpha_{g_i}(t1_{g_i^{-1}})e \neq \alpha_{g_j}(t1_{g_j^{-1}})e = f_j(\eta(1\otimes t))e,$$

mostrando que $f_1, \cdots, f_k$ são dois a dois α-fortemente distintos.

Como T é uma A^α-álgebra separável então $\eta(A\otimes T)$ é A-separável. De fato, se $e_T = \sum_{i=1}^{n} t_i \otimes u_i \in T\otimes T$ é o idempotente de separabilidade de T sobre A^α, então $\sum_{i=1}^{n} \eta(1_A\otimes t_i)\otimes_A \eta(1_A\otimes u_i) \in \eta(A\otimes T)\otimes_A \eta(A\otimes T)$ é o idempotente de separabilidade de $\eta(A\otimes T)$ sobre A.

Aplicando os Lemas 2.1.12 e 2.1.13, obtemos idempotentes dois a dois ortogonais $w_1, \cdots, w_k \in \eta(A\otimes T)$ tais que $f_i(z)w_i = zw_i$, para todo $z \in \eta(A\otimes T)$, e $f_i(w_j) = \delta_{ij}$, para $i, j = 1, \cdots, k$. Notemos que $w_1, \cdots, w_k \in \eta(A\otimes T) \subseteq \mathcal{F}^{\alpha'_H}$. Logo, para mostrar que $\mathcal{F}^{\alpha'_H} \subseteq \eta(A\otimes T)$ resta mostrar que $\{w_1, \cdots, w_k\}$ geram $\mathcal{F}^{\alpha'_H}$ como A-módulo.

Tomemos $v \in \mathcal{F}^{\alpha'_H}$. Então existe $\sum_{j=1}^{n} x_j \otimes y_j \in A\otimes A$ tal que $v = \eta(\sum_{j=1}^{n} x_j \otimes y_j)$. Assim, para todo $i \in \{1, \cdots, k\}$, temos

$$\begin{aligned}
v(g_i)1_{g_ih} &= \eta(\sum_{j=1}^{n} x_j\otimes y_j)(g_i)1_{g_ih} \\
&= \sum_{j=1}^{n} x_j\alpha_{g_i}(y_j 1_{g_i^{-1}})1_{g_ih} \\
&= \sum_{j=1}^{n} x_j\alpha_{g_i}(y_j 1_{g_i^{-1}})1_{g_i}1_{g_ih} \\
&= \sum_{j=1}^{n} x_j\alpha_{g_i}(y_j 1_{g_i^{-1}})f_i(w_i)1_{g_i}1_{g_ih} \\
&= \sum_{j=1}^{n}\sum_{l=1}^{k} x_j\alpha_{g_l}(y_j 1_{g_l^{-1}})f_i(w_l)1_{g_i}1_{g_ih} \\
&= \underbrace{\sum_{j=1}^{n}\sum_{l=1}^{k} x_j\alpha_{g_l}(y_j 1_{g_l^{-1}})}_{\in A} w_l(g_i)1_{g_i}1_{g_ih}.
\end{aligned}$$

Como $G = \cup_{i=1}^{r} g_iH$ e esta união é disjunta, então todo elemento de G se escreve de maneira única como g_ih, para algum $h \in H$. Pelo Lema 2.2.2, temos que $v \in \mathcal{F}^{\alpha'_H}$

se e somente se $v(g_i)1_{g_ih} = v(g_ih)1_{g_i}$, para quaisquer $h \in H$ e $g_i \in G$. Assim,

$$v(g_ih)1_{g_i} = v(g_i)1_{g_ih} = \begin{cases} 0, se\ g_i \notin G_0 \\ \sum_{l=1}^{k} a_l w_l(g_i)1_{g_i}1_{g_ih}, se\ g_i \in G_0, \end{cases}$$

com $a_l = \sum_{j=1}^{n} x_j \alpha_{g_l}(y_j 1_{g_l^{-1}})$. Desta forma, é suficiente aplicar v nos g_i's $\in \{g_1, \cdots, g_k\}$. Portanto concluímos que $\{w_1, \cdots, w_k\}$ geram $\mathcal{F}^{\alpha'_H}$ sobre A. $\square$

Capítulo 3

Teoria de Galois e semirreticulados

Este capítulo é baseado em [9]. Aqui serão discutidos alguns aspectos da estrutura de uma extensão de Galois parcial. Para isso, vamos supor que A é um anel unitário, $\alpha = (\{D_g\}, \{\alpha_g\})_{g\in G}$ é uma ação parcial de um grupo finito G sobre A e cada D_g é um ideal unitário gerado por um idempotente central 1_g.

3.1 Ações parciais e semirreticulados

Começamos por considerar o seguinte conjunto:

$$I_G = \{1_g \mid g \in G\}.$$

Um semigrupo booleano B é um semigrupo no qual $b^2 = b$, para todo $b \in B$. Desta forma, consideremos o semigrupo Booleano gerado pelo produto dos elementos de I_G, com a multiplicação de A, denotado por $B(I_G)$. Em $B(I_G)$ existe uma relação de ordem natural dada por $e \leq f$ se, e somente se, $ef = e$, para todo

$e, f \in B(I_G)$. Um elemento $0 \neq e \in B(I_G)$ é dito minimal se satisfaz $ef = e$ ou $ef = 0$, para todo $f \in B(I_G)$. A cada elemento minimal $e \in B(I_G)$ associamos um subconjunto de G, definido por

$$G(e) = \{g \in G \mid e1_g \neq 0\} = \{g \in G \mid e1_g = e\}.$$

Observemos que $1 \in G(e)$, para todo $e \in B(I_G)$.

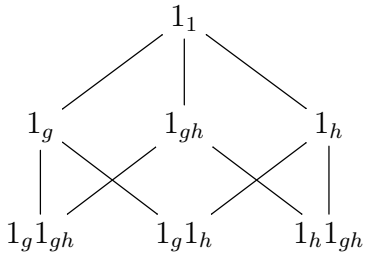
Os seguintes exemplos ilustram como podemos construir semirreticulados a partir de ações parciais.

Exemplo 3.1.1. *Considere a ação parcial do Grupo de Klein sobre o anel $A = R \times R \times R$, onde R é um anel com unidade, definida no Exemplo 1.2.6. Neste caso,*

$I_G = \{1_1 = 1_A, 1_g, 1_h, 1_{gh}\} = \{(1,1,1), (1,0,1), (1,1,0), (0,1,1)\}$,

$B(I_G) = \{1_1, 1_g, 1_h, 1_{gh}, 1_g1_h, 1_g1_{gh}, 1_h1_{gh}, (0,0,0)\}$.

O semirreticulado associado a esta ação parcial é o seguinte:



Neste exemplo os elementos minimais e os subconjuntos de G associados a eles são dados por:

1) $e_1 = 1_g1_{gh} \rightsquigarrow G(e_1) = \{1, g, gh\}$,

2) $e_2 = 1_g1_h \rightsquigarrow G(e_2) = \{1, g, h\}$ e

3) $e_3 = 1_h1_{gh} \rightsquigarrow G(e_3) = \{1, h, gh\}$.

Observe que nenhum $G(e_i), i \in \{1,2,3\}$, é subgrupo do Grupo de Klein.

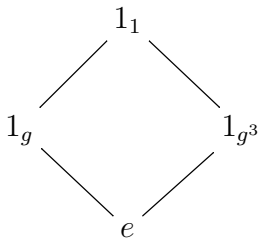
Exemplo 3.1.2. *Considere a ação parcial de C_4, o grupo cíclico de ordem 4, sobre o anel $A = R \times R \times R$, onde R é um anel com unidade, definida no Exemplo 1.2.7. Neste caso,*

$I_G = \{1_1 = 1_A, 1_g, 1_{g^2}, 1_{g^3}\} = \{(1,1,1), (0,1,1), (0,1,0), (1,1,0)\}$,

$B(I_G) = \{1_1, 1_g, 1_{g^2}, 1_{g^3}\}$.

Observe que $1_{g^2} = 1_g 1_{g^2} = 1_{g^2} 1_{g^3} = 1_g 1_{g^2} 1_{g^3}$. Denotaremos 1_{g^2} por e.

O semirreticulado associado a esta ação parcial é o seguinte:



Neste exemplo temos apenas o elemento minimal em $e \in B(I_G)$ e $G(e) = \{1, g, g^2, g^3\} = C_4$ (que trivialmente é um subgrupo de C_4).

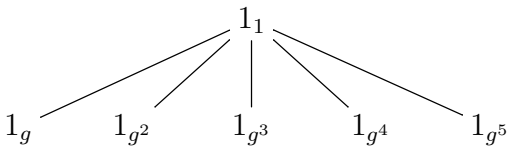
Exemplo 3.1.3. *Agora vamos considerar o exemplo 6.3 de [5], que foi transcrito no exemplo 2.2.4 do capítulo anterior. O grupo considerado é cíclico de ordem 6 gerado por g, denotado por C_6, e o anel é $S = \sum_{1 \leq i \leq 5} \oplus Ae_i$, onde $\{e_i \mid 1 \leq i \leq 5\}$ é um conjunto de idempotentes ortogonais não nulos cuja soma é 1 e A é uma extensão de Galois (global) cíclica de um anel comutativo R com grupo de Galois C_6. Os ideais desta ação parcial são definidos como $A_{g^i} = Ae_{6-i}$. Dessa maneira,*

$I_G = \{1_1 = 1_S, 1_g, 1_{g^2}, 1_{g^3}, 1_{g^4}, 1_{g^5}\}$, *tal que* $1_g = 1_A e_5$, $1_{g^2} = 1_A e_4$, $1_{g^3} = 1_A e_3$, $1_{g^4} = 1_A e_2$, $1_{g^5} = 1_A e_1$, $1_1 = 1_S = 1_A e_1 \oplus 1_A e_2 \oplus 1_A e_3 \oplus 1_A e_4 \oplus 1_A e_5$, *e*

$B(I_G) = \{1_1, 1_g, 1_{g^2}, 1_{g^3}, 1_{g^4}, 1_{g^5}, 0_S\}$.

À ação parcial definida por esta construção relacionamos o semirreticulado

abaixo:



Os elementos minimais de $B(I_G)$ e os subconjuntos de C_6 relacionados a eles são:

1) $1_g \rightsquigarrow G(1_g) = \{1, g\}$,

2) $1_{g^2} \rightsquigarrow G(1_{g^2}) = \{1, g^2\}$,

3) $1_{g^3} \rightsquigarrow G(1_{g^3}) = \{1, g^3\}$,

4) $1_{g^4} \rightsquigarrow G(1_{g^4}) = \{1, g^4\}$,

5) $1_{g^5} \rightsquigarrow G(1_{g^5}) = \{1, g^5\}$.

Observe que $G(1_{g^3})$ é subgrupo de C_6.

Como visto nos exemplos acima, dado um elemento minimal $e \in B(I_G)$, o subconjunto de G associado a e, denotado por $G(e)$, pode não ser um subgrupo de G. Suponhamos que H é um subconjunto de G tal que $1 \in H$. Definimos:

$$e_H = \prod_{h \in H} 1_h, \text{ e } I_H = \{1_h \mid h \in H\},$$

e $B(I_H)$ o semigrupo booleano gerado pelos elementos de I_H com a multiplicação de A. Observemos que e_H pode ser zero. Na próxima seção vamos mostrar alguns resultados que valem quando H é subgrupo de G.

3.2 Teoria de Galois e uma aplicação para os semirreticulados

Aqui apresentaremos resultados envolvendo os conceitos da seção anterior para o caso em que H é um subgrupo de G. Ao final desta seção relacionaremos os semirreticulados com os resultados desenvolvidos.

Lema 3.2.1. *Seja H um subgrupo de G. Então, para cada $h \in H$, temos:*

(i) $\alpha_h(e_H 1_{h^{-1}}) = e_H$;

(ii) $\alpha_h(B(I_H)1_{h^{-1}}) \subset B(I_H)$.

Demonstração.

(i) Seja $h \in H$, então
$\alpha_h(e_H 1_{h^{-1}}) = \alpha_h((\prod_{h' \in H} 1_{h'})1_{h^{-1}}) = \prod_{h' \in H} \alpha_h(1_{h'}1_{h^{-1}}) = \prod_{h' \in H} 1_h 1_{hh'} = 1_h e_H = e_H$.

(ii) Sejam $h_1, \cdots, h_n \in H$ e $x = 1_{h_1} \cdots 1_{h_n} \in B(I_H)$. Temos que $\alpha_h(x1_{h^{-1}}) = \alpha_h(1_{h_1}1_{h^{-1}}) \cdots \alpha_h(1_{h_n}1_{h^{-1}}) = 1_h 1_{hh_1} \cdots 1_h 1_{hh_n} = 1_{hh_1} \cdots 1_{hh_n} 1_h \in B(I_H)$ pois $hh_i \in H$, para todo $i = 1, \cdots, n$. □

Lema 3.2.2. *Seja H um subgrupo de G, tal que $e_H \neq 0$. Então α induz uma ação global de H em Ae_H. Além disso, se A é uma extensão de Galois α-parcial de A^α, então Ae_H é uma extensão de Galois de $(Ae_H)^H$ com grupo de Galois H.*

Demonstração. Para cada $h \in H$, temos que $\alpha_h(Ae_H 1_{h^{-1}}) = \alpha_h(A1_{h^{-1}})\alpha_h(e_H 1_{h^{-1}})$ $= A1_h e_H = Ae_H 1_h$. Então α induz uma ação parcial de H em Ae_H que denotaremos por $\alpha' = (\{Ae_H 1_h\}, \{\alpha'_h = \alpha_h|_{Ae_H 1_{h^{-1}}}\})_{h \in H}$. Observemos que $Ae_H 1_h = Ae_H$, para todo $h \in H$, consequentemente α' é uma ação global de H em Ae_H. Suponhamos que A é uma extensão de Galois α-parcial de A^α. Seja $\{x_i, y_i\}_{1 \leq i \leq n}$ um sistema de

coordenadas de Galois α-parciais de A sobre A^{α}. Então, $\sum_{i=1}^{n} x_i\alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g}1_A$, para cada $g \in G$. Em particular esta igualdade vale para cada $h \in H$. Para cada $i = 1, \cdots, n$, sejam $x_i' = x_i e_H$ e $y_i' = y_i e_H$. Então, para cada $h \in H$, temos

$$\begin{aligned}\sum_{i=1}^{n} x_i'\alpha_h(y_i' 1_{h^{-1}}) &= \sum_{i=1}^{n} x_i e_H \alpha_h(y_i e_H 1_{h^{-1}}) = \sum_{i=1}^{n} x_i e_H \alpha_h(y_i 1_{h^{-1}})\alpha_h(e_H 1_{h^{-1}}) \\ &= \sum_{i=1}^{n} x_i e_H \alpha_h(y_i 1_{h^{-1}}) = e_H \sum_{i=1}^{n} x_i \alpha_h(y_i 1_{h^{-1}}) = e_H \delta_{1,h} 1_A = \delta_{1,h} e_H.\end{aligned}$$

Como α' é uma ação global de H em Ae_H então $\{x_i', y_i'\}_{1\leq i\leq n}$ é um sistema de coordenadas de Galois (globais) para Ae_H e portanto Ae_H é uma extensão de Galois (global) de $(Ae_H)^H$ com grupo de Galois H. □

Relembramos, como exposto na seção 2.2, que se H é um subgrupo de G, então α induz uma ação parcial de H, denotada por α_H, em A. Pelo Teorema 2.2.5 temos que A é uma extensão de Galois α_H-parcial de A^{α_H}. Com as mesmas hipóteses do Lema anterior decorre que α_H quando restrito a Ae_H está bem definida (coincide com α') e torna Ae_H uma extensão de Galois de $A^{\alpha_H}e_H$ com grupo de Galois H. Para vermos isto basta observar que $(Ae_H)^H = A^{\alpha_H}e_H$:

$$\begin{aligned} xe_H \in (Ae_H)^H &\Leftrightarrow h(xe_H) = xe_H, \text{ para todo } h \in H \\ &\Leftrightarrow h(xe_H 1_{h^{-1}}) = xe_H 1_h, \text{ para todo } h \in H \\ &\Leftrightarrow \alpha_h(xe_H 1_{h^{-1}}) = xe_H 1_h, \text{ para todo } h \in H \\ &\Leftrightarrow \alpha_h(x1_{h^{-1}})\alpha_h(e_H 1_{h^{-1}}) = xe_H 1_h, \text{ para todo } h \in H \\ &\Leftrightarrow \alpha_h(x1_{h^{-1}})e_H = xe_H 1_h, \text{ para todo } h \in H \\ &\Leftrightarrow xe_H \in A^{\alpha_H}e_H. \end{aligned}$$

Seja A uma extensão de Galois α-parcial de A^{α}. Sejam S o conjunto dos ideais unitários D de A contendo $(Ae_H)^H$ tal que D é extensão de Galois de D^H com grupo de Galois H induzida por α e $E = \{e_H \neq 0 \mid H \text{ subgrupo de } G\}$.

Lema 3.2.3. *Seja A uma extensão de Galois α-parcial de A^{α}. Seja H um subgrupo de G e D um ideal de A, com identidade, contendo $(Ae_H)^H$. Suponhamos que D*

é uma extensão de Galois de D^H com grupo de Galois H, induzida por α. Então $e_H \neq 0$ e $D = Ae_H$.

Demonstração. Denotemos por 1_D a identidade de D e α^* a ação parcial de H em D induzida por α, ou seja, $\alpha^* = (\{D1_h\}, \{\alpha_h^* = \alpha_h|_{D1_{h^{-1}}}\})_{h\in H}$. Por hipótese temos que α^* é uma ação global de H em D. Consequentemente, $D1_h = D$, para todo $h \in H$. Então, $1_D 1_h = 1_D$, para todo $h \in H$. Em particular, $e_H^* = \prod_{h\in H} 1_D 1_h = 1_D \neq 0$. Por outro lado, $e_H^* = \prod_{h\in H} 1_D 1_h = 1_D e_H$. Portanto, $e_H \neq 0$.

Como $e_H \neq 0$, pelo Lema 3.2.2, Ae_H é uma extensão de Galois de $(Ae_H)^H$ com grupo de Galois H induzido por α. Por outro lado, $D = D1_D = De_H^* = De_H \subseteq Ae_H$ e, consequentemente, $D^H \subseteq (Ae_H)^H$. Como D contém $(Ae_H)^H$, segue que $D^H = (Ae_H)^H$. Então D também é uma extensão de Galois de $(Ae_H)^H$ com grupo de Galois H induzida por α. Uma vez que D está contido em Ae_H, decorre que $D = Ae_H$. □

Proposição 3.2.4. *Se A uma extensão de Galois α-parcial de A^α, então existe uma correspondência biunívoca entre E e S.*

Demonstração. Considere a aplicação

$$\begin{array}{rccc} \varphi & : & E & \longrightarrow & S \\ & & e_H & \longmapsto & Ae_H \end{array}$$

Pelo Lema 3.2.2 temos que φ está bem definida e é injetora. Além disso, utilizando o Lema 3.2.3 temos que φ é sobrejetora. □

Para calcularmos a quantidade de extensões de Galois dadas na Proposição 3.2.4, podemos encontrar os subgrupos H de G e determinar quantos e_H são diferentes de zero. Alternativamente, podemos utilizar o semirreticulado associado à α, onde ficam explicitados os elementos do $B(I_G)$ que são diferentes de zero. Uma vez

feito isso, contamos quantos subconjuntos $G(e)$ são subgrupos de G, onde e é um elemento do semirreticulado.

3.3 Quando $G(e)$ é um subgrupo de G

Com a mesma notação das seções anteriores, vamos apresentar alguns resultados para determinar quando o subconjunto $G(e)$ de G é um subgrupo de G, tal que $e \in B(I_G)$ é um elemento minimal. Observemos que $e_{G(e)} = \prod_{g \in G(e)} 1_g = e$.

Proposição 3.3.1. *Seja e um elemento minimal no $B(I_G)$. Então as seguintes afirmações são equivalentes:*

(*i*) *$G(e)$ é um subgrupo de G;*

(*ii*) $e \in A^\alpha$;

(*iii*) $\alpha_g(B(I_{G(e)})1_{g^{-1}}) \subset B(I_{G(e)})$, *para cada* $g \in G(e)$.

Demonstração.

$(i) \Rightarrow (ii)$ Pelo Lema 3.2.1, se $g \in G(e)$, então $e \in A^\alpha$. Suponhamos que $g \notin G(e)$, então $g^{-1} \notin G(e)$, logo $e1_g = e1_{g^{-1}} = 0$ e, consequentemente, $\alpha_g(e1_{g^{-1}}) = \alpha_g(0) = 0 = e1_g$.

$(ii) \Rightarrow (i)$ Note que $1 \in G(e)$, pois $e1_1 = e1_A = e$. Sejam $g, h \in G(e)$ então $e1_{gh} = e1_g1_{gh} = e\alpha_g(1_{g^{-1}}1_h) = e1_g\alpha_g(1_{g^{-1}}1_h) = \alpha_g(e1_{g^{-1}})\alpha_g(1_{g^{-1}}1_h) = \alpha_g(e1_{g^{-1}}1_h) = \alpha_g(e1_{g^{-1}}) = e1_g = e$. Portanto $gh \in G(e)$.

$(i) \Rightarrow (iii)$ Segue diretamente do Lema 3.2.1 (ii) para $H = G(e)$.

$(iii) \Rightarrow (i)$ Resta mostrar que se $g, h \in G(e)$, então $gh \in G(e)$. Note que $1_g1_{gh} = \alpha_g(1_h1_{g^{-1}}) \in \alpha_g(B(I_{G(e)})1_{g^{-1}}) \subset B(I_{G(e)})$. Portanto, $1_g1_{gh} \in B(I_{G(e)})$. Então,

$e1_{gh} = e1_g1_{gh} = e$ e, consequentemente, $gh \in G(e)$. □

Proposição 3.3.2. *Seja A uma extensão de Galois α-parcial de A^α e $e \in B(I_G)$ um elemento minimal. Suponhamos que $e \in A^\alpha$. Então Ae é uma extensão (global) de $A^\alpha e$ com grupo de Galois $G(e)$ induzida por α.*

Demonstração. Se $e \in A^\alpha$ então, pela Proposição 3.3.2, $G(e)$ é subgrupo de G. Lembremos que $e_{G(e)} = e$. Pelo Lema 3.2.2, temos que Ae é uma extensão de Galois de $(Ae)^{G(e)}$, com grupo de Galois $G(e)$, induzida por α. Resta mostrar que $(Ae)^{G(e)} = A^\alpha e$. Como $e \in A^\alpha$, então $A^\alpha e \subseteq (Ae)^{G(e)}$. Reciprocamente, tome $xe \in (Ae)^{G(e)}$. Então, $\alpha_g(xe1_{g^{-1}}) = xe1_g$, para todo $g \in G(e)$. Se $g \notin G(e)$, então $e1_g = 0 = 1_{g^{-1}}$, logo $\alpha_g(xe1_{g^{-1}}) = \alpha_g(0) = 0 = xe1_g$. Portanto $\alpha_g(xe1_{g^{-1}}) = xe1_g$, para todo $g \in G$. Então, $\alpha_g(x1_{g^{-1}})e = x1_ge$, para todo $g \in G$. Consequentemente, $xe \in A^\alpha e$. □

Teorema 3.3.3. *Considere A uma extensão de Galois α-parcial de A^α. Sejam $k \in \mathbb{Z}$ e que $\{e_1, e_2, \cdots, e_k\}$, um conjunto de elementos minimais em $B(I_G)$, tal que cada $e_i \in A^\alpha$, para todo $i = 1, \cdots, k$. Então $A = (\oplus_{i=1}^k Ae_i) \oplus Ae'$, onde $e' = 1_A - \sum_{i=1}^{k} e_i$, tal que Ae_i é uma extensão de Galois de $A^\alpha e_i$ com grupo de Galois $G(e_i)$ induzida por α, para todo $i = 1, \cdots, k$. Além disso, se $e' \neq 0$, então Ae' é uma extensão de Galois α'-parcial de $A^\alpha e'$ pela ação parcial α' de G induzida por α.*

Demonstração. Para todo $i = 1, \cdots, k$, e_i é idempotente em A. Além disso, se $i \neq j$, $e_ie_j = 0$, pois são elementos minimais em $B(I_G)$. Portanto $A = (\oplus_{i=1}^k Ae_i) \oplus Ae'$. Pela Proposição 3.3.2, para todo $i = 1, \cdots, k$, cada Ae_i é uma extensão de Galois de $A^\alpha e_i$, com grupo de Galois $G(e_i)$, induzida por α.

Observemos que $e' \in A^{\alpha}$, pois

$$\begin{aligned}\alpha_g(e'1_{g^{-1}}) &= \alpha_g(1_A 1_{g^{-1}}) - \sum_{i=1}^{k} \alpha_g(e_i 1_{g^{-1}}) \\ &= 1_A 1_g - \sum_{i=1}^{k} e_i 1_g \\ &= (1_A - \sum_{i=1}^{k} e_i)1_g = e'1_g,\end{aligned}$$

para todo $g \in G$. Agora suponhamos que $e' \neq 0$. Para cada $g \in G$, temos que

$$\alpha_g(D_{g^{-1}}e') = \alpha_g(D_{g^{-1}})\alpha_g(e'1_{g^{-1}}) = D_g e'.$$

Então α induz uma ação parcial α' de G em Ae' dada por $\alpha' = (\{D_g e'\}, \{\alpha'_g = \alpha_g|_{D_{g^{-1}}e'}\})_{g\in G}$.

Seja $\{x_i, y_i\}_{1\leq 1\leq n}$ um sistema de coordenadas de Galois α-parciais de A sobre A^{α}. Então $\{x_i e', y_i e'\}_{1\leq i\leq n}$ é um sistema de coordenadas de Galois α'-parciais de Ae' sobre $(Ae')^{\alpha'}$. De fato,

$$\begin{aligned}\sum_{i=1}^{n} x_i e' \alpha_g(y_i e' 1_{g^{-1}}) &= \sum_{i=1}^{n} x_i e' \alpha_g(y_i 1_{g^{-1}}) e' 1_g \\ &= \sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) e' \\ &= \delta_{1,g} 1_A e' = \delta_{1,g} e'.\end{aligned}$$

Portanto, Ae' é uma extensão de Galois α'-parcial de $(Ae')^{\alpha'}$. Resta notar que $(Ae')^{\alpha'} = A^{\alpha}e'$. □

A seguir daremos um exemplo que ilustra os últimos resultados apresentados.

Exemplo 3.3.4 ([9],exemplo 12, adaptado)**.** *Sejam R e T anéis, R uma extensão de Galois de R^H com grupo de Galois H e T uma extensão de Galois de T^K com grupo de Galois K. Definiremos uma ação parcial α de $G = H \times K$ em $A = R \oplus T$, tal que A é uma extensão de Galois α-parcial de $R^H \oplus T^K$.*

Fixemos $g = (h, k)$, considere

$$1_g = \begin{cases} (0,0), se\ g = (h,k), h \neq 1, k \neq 1, \\ (1,0), se\ g = (h,1), h \neq 1, \\ (0,1), se\ g = (1,k), k \neq 1, \\ (1,1), se\ g = (1,1). \end{cases}$$

Seja

$$D_g = A1_g = \begin{cases} 0 \oplus 0, se\ g = (h,k), h \neq 1, k \neq 1, \\ R \oplus 0, se\ g = (h,1), h \neq 1, \\ 0 \oplus T, se\ g = (1,k), k \neq 1, \\ R \oplus T, se\ g = (1,1). \end{cases}$$

Observando que $D_{g^{-1}} = D_g$, definimos os isomorfismos da seguinte maneira

$$\begin{array}{rccll} \alpha_g & : & D_g & \longrightarrow & D_g \\ & & (0,0) & \longmapsto & (0,0), \quad se\ g = (h,k), h \neq 1, k \neq 1, \\ & & (r,0) & \longmapsto & (h(r),0), \quad se\ g = (h,1), h \neq 1, \\ & & (0,t) & \longmapsto & (0,k(t)), \quad se\ g = (1,k), k \neq 1, \\ & & (r,t) & \longmapsto & (r,t), \quad se\ g = (1,1). \end{array}$$

Temos que $\alpha = (\{D_g\}, \{\alpha_g\})_{g \in G}$ é uma ação parcial de G em A. A condição (i) da definição de ação parcial é verificada: $D_1 = D_{(1,1)} = R \oplus T = A$ e $\alpha_1 = \alpha_{(1,1)} = Id_A$. Vamos mostrar que a segunda condição vale, analisando casos. Precisamos verificar que $\alpha_g(D_g \cap D_{g'}) = \alpha_g(D_{g^{-1}} \cap D_{g'}) = D_g \cap D_{gg'}$. É fácil ver que esta condição vale se $g = (1,1)$ ou $g = (h,k)$ com $h \neq 1$ e $k \neq 1$. Se $g = (h,1), h \neq 0$, então $D_g = R \oplus 0$ e temos que analisar as possibilidades de g':

- $g' = (h', k')$, com $h' \neq 1$ e $k' \neq 1 \Rightarrow D_{g'} = 0 \oplus 0 \Rightarrow \alpha_g(D_g \cap D_{g'}) = 0 \oplus 0$

$$gg' = \begin{cases} (1,k'), se\ h^{-1} = h' \Rightarrow D_{gg'} = 0 \oplus T \Rightarrow D_g \cap D_{gg'} = 0 \oplus 0 \\ (hh',k'), se\ h^{-1} \neq h' \Rightarrow D_{gg'} = 0 \oplus 0 \Rightarrow D_g \cap D_{gg'} = 0 \oplus 0 \end{cases}$$

- $g' = (h', 1)$, com $h' \neq 0 \Rightarrow D_{g'} = R \oplus 0 \Rightarrow \alpha_g(D_g \cap D_{g'}) = R \oplus 0$

  $$gg' = \begin{cases} (1,1), se\ h^{-1} = h' \Rightarrow D_{gg'} = R \oplus T \Rightarrow D_g \cap D_{gg'} = R \oplus 0 \\ (hh', 1), se\ h^{-1} \neq h' \Rightarrow D_{gg'} = R \oplus 0 \Rightarrow D_g \cap D_{gg'} = R \oplus 0 \end{cases}$$

- $g' = (1, k')$, com $k' \neq 0 \Rightarrow D_{g'} = 0 \oplus T \Rightarrow \alpha_g(D_g \cap D_{g'}) = 0 \oplus 0$

  $gg' = (h, k') \Rightarrow D_{gg'} = 0 \oplus 0 \Rightarrow D_g \cap D_{gg'} = 0 \oplus 0$

- $g' = (1, 1) \Rightarrow D_{g'} = R \oplus T \Rightarrow \alpha_g(D_g \cap D_{g'}) = R \oplus 0$

  $gg' = (h, 1) \Rightarrow D_{gg'} = R \oplus 0 \Rightarrow D_g \cap D_{gg'} = R \oplus 0$

O caso em que $g = (1, k)$ é análogo ao descrito acima. A terceira condição de ação parcial também é satisfeita e pode ser verificada analisando os casos possíveis, como feito acima.

Sendo assim, temos que $R^H = \{r \in R \mid h(r) = r, \text{ para todo } h \in H\}$ e $T^K = \{t \in T \mid k(t) = t, \text{ para todo } k \in K\}$. Então $A^\alpha = \{(r,t) \in R \oplus T \mid \alpha_g((r,t)1_{g^{-1}}) = (r,t)1_g, \text{ para todo } g \in H \times K\} = R^H \oplus T^K$.

Agora, considere $\{r_i, r_i' \in R\}, i = 1, \cdots, m$ e $\{t_j, t_j' \in T\}, j = 1, \cdots, n$ sistemas de coordenadas de Galois para R e T. Sejam $x_1 = (r_1, 0), \cdots, x_m = (r_m, 0), x_{m+1} = (0, t_1), \cdots, x_{m+n} = (0, t_n)$ e $y_1 = (r_1', 0), \cdots, y_m = (r_m', 0), y_{m+1} = (0, t_1'), \cdots, y_{m+n} = (0, t_n')$. E assim, temos:

- $g = (1, 1)$:
  $\sum_{l=1}^{m+n} x_l \alpha_g(y_l 1_{g^{-1}}) = \sum_{l=1}^{m+n} x_l y_l = (\sum_{i=1}^{m} r_i r_i', \sum_{j=1}^{n} t_j t_j') = (1, 1)$

- $g = (h, k)$, com $h, k \neq 1$:
  $\sum_{l=1}^{m+n} x_l \alpha_g(y_l 1_{g^{-1}}) = \sum_{l=1}^{m+n} x_l \alpha_g(0, 0) = (0, 0)$

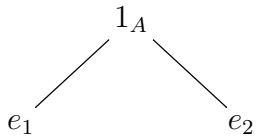
- $g = (h, 1)$, com $h \neq 1$:
  $\sum_{l=1}^{m+n} x_l \alpha_g(y_l 1_{g^{-1}}) = (\sum_{i=1}^{m} r_i h(r_i'), 0) = (0, 0)$

- $g = (1, k)$, com $k \neq 1$:

  $\sum_{l=1}^{m+n} x_l \alpha_g(y_l 1_{g^{-1}}) = (0, \sum_{j=1}^{n} t_j k(t'_j)) = (0, 0).$

Portanto $\{x_l, y_l \in A\}, talquel = 1, \cdots, m+n$, é um sistema de coordenadas de Galois α-parcial para A. Assim, A é uma extensão de Galois α-parcial de $R^H \oplus T^K$. Neste caso, $e_1 = (1, 0)$ e $e_2 = (0, 1)$ são os únicos elementos minimais no $B(I_G)$ e $e_1 + e_2 = (1, 1) = 1_A$. Além disso, $e_1, e_2 \in A^\alpha$. De fato, $G(e_1) = H \times 1$ e $G(e_2) = 1 \times K$ são subgrupos de G. Portanto, pelo Teorema 3.3.3, $A = Ae_1 \oplus Ae_2$, onde $Ae_i, i = 1, 2$, é uma extensão de Galois de $(Ae_i)^{G(e_i)} = A^\alpha e_i$ com grupo de Galois $G(e_i)$. Esta conclusão é natural uma vez que $Ae_1 \simeq R$, $G(e_1) \simeq H$ e R é uma extensão de Galois de R^H. Analogamente $Ae_2 \simeq T$, $G(e_2) \simeq K$ e T é uma extensão de Galois de T^K com grupo de Galois K.

O semirreticulado associado a este exemplo é:



Referências

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, Massachusetts (1969).

[2] S.U. Chase, D.K. Harrison, and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. **52** (1965), 1-19.

[3] F. DeMeyer and E. Ingraham, *Separable Algebras Over Commutative Rings*, Springer-Verlag Berlin·Heidelberg (1971).

[4] M. Dokuchaev and R. Exel, *Associativity of crossed products by partial actions, enveloping actions and partial representations*, Trans. Amer. Math. Soc. **357** (2005), 1931-1952.

[5] M. Dokuchaev, M. Ferrero, and A. Paques, *Partial actions and Galois theory*, Journal of Pure and Applied Algebra **208** (2007), 77-87.

[6] R. Exel, *Circle actions on C*-algebras, partial automorphisms and a generalized Pimsner-Voiculescu exact sequence*, J. Funct. Anal. 122 (1994), 361-401.

[7] D. A. S. Flôres, *Ação de Grupóides sobre Álgebras: Teoremas de Estrutura*, Tese de Doutorado (2011).

[8] J. Á. Guzmán and J. Lazzarin, *A Morita context related to finite groups acting partially on a ring*, Algebra and Discrete Mathematics **3** (2009), 49-60.

[9] K. Jung-Miao and G. Szeto, *The structure of a partial Galois extension*, Monatshefte fur Mathematik, Springer-Verlag Wien (2013).

[10] B. R. McDonald, *Linear Algebra over Commutative Rings*, Marcel Dekker (1984).

[11] A. Paques, *Ações Parciais de Grupos sobre Álgebras*, Notas de curso, redigido por D. S. Azevedo, UFRGS (2013).

[12] ———, *Teoría de Galois sobre anillos conmutativos*, Univ. de Los Andes, Mérida, Venezuela (1999).

[13] T. R. Tamusiunas, *Teorias de Galois para Ação de Grupóides*, Tese de Doutorado (2012).