Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

TEORIAS DE GALOIS PARA AÇÃO DE GRUPÓIDES

Tese de Doutorado

THAÍSA RAUPP TAMUSIUNAS

Porto Alegre, 05 de julho de 2012

Tese submetida por Thaísa Raupp Tamusiunas[1], como requisito parcial para a obtenção do grau de Doutora em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Professor Dr. Antonio Paques

Banca examinadora:
Professor Dr. Antonio Paques (UFRGS, Orientador)
Professor Dr. Alveri Alves Sant'Ana (UFRGS)
Professora Dra. Daiana Aparecida Flôres (UFSM)
Professor Dr. Dirceu Bagio(UFSM)
Professor Dr. Miguel Angel Alberto Ferrero (UFRGS)

[1]Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)

Agradecimentos

Aos meus familiares, especialmente aos meus pais Sérgio e Marli. Ao meu amado namorado, Jonathan. Aos colegas de pós-graduação da UFRGS. À secretária da pós-graduação, Rosane. Ao meu querido orientador, Paques.

À vocês, muito obrigada.

Resumo

Este trabalho de pesquisa tem por objetivo tratar de teorias de Galois para o caso de ação de grupóides sobre anéis, focalizando especialmente em construir e analisar teoremas de correspondência, tendo como ponto de partida a teoria desenvolvida por Chase, Harrison e Rosenberg em [8].

Abstract

This research aims to address theories of Galois for the case of groupoids action over rings, focusing especially on building and analyzing correspondence's theorems, taking as its starting point the theory developed by Chase, Harrison and Rosenberg in [8].

Índice

Introdução

Grupóides foram originalmente introduzidos por Brandt, em sua publicação [5] de 1926. Sucintamente, dizemos que um grupóide G é uma categoria pequena (isto é, uma categoria cujos objetos e morfismos formam conjuntos) onde cada morfismo é um isomorfismo. Esta definição categórica pode ser encontrada em [6], onde são ilustrados diversos exemplos e aplicações de grupóides. Um grupóide com um objeto é precisamente um grupo, portanto a noção de grupóide é uma extensão natural da noção de grupos. Nesta tese, não adotaremos a versão categórica, mas sim uma versão axiomática de grupóides, dada em [19], que será introduzida já no início do primeiro capítulo.

A noção de ação parcial de grupóide foi introduzida por D. Bagio e A. Paques em [4], onde interpreta-se esta como uma generalização de ação parcial de grupos (veja [11] e [13]), assim como de ação parcial de grupóide ordenado (veja [3]).

Na teoria de Galois, diversos autores deixaram sua marca. Em 1965, S. U. Chase, D. K. Harrison e A. Rosenberg publicaram em [8] uma teoria de Galois para anéis comutativos, na qual apresentam, dentre outros resultados, uma lista de novas definições equivalentes de extensão de Galois e um teorema fundamental, o qual referenciaremos por 'Teorema de Correspondêcia CHR'. Este teorema de correspondência relaciona bijetivamente subgrupos do grupo de Galois G e subálgebras separáveis que são G-fortes dessa extensão. Em [4], D. Bagio e A. Paques generalizaram estas equivalentes definições para o contexto de ação de grupóides, e esta generalização foi um recurso bastante utilizado neste trabalho, visto que traz importantes caracterizações para extensões de Galois.

Em 1995, A. W. Dress mostrou em [12] que uma simplificação da teoria de Galois para corpos é possível combinando o Lema de Dedekind com alguns fatos elementares sobre G-conjuntos. M. Ferrero e A. Paques mostraram em [14] que esta simplificação é possível ser usada na teoria de Galois para ação de grupos sobre anéis comutativos e, consequentemente, obtiveram novos resultados. Além disso, A. Paques, utilizando-se dos trabalhos recém citados, generalizou em [21] um outro teorema de correspondência - a chamada Correspondência de Galois-Grothendieck - igualmente para o caso de ação de grupos sobre anéis, e mostrou o Teorema de Correspondência CHR como uma simples consequência da Correspondência de Galois-Grothendieck.

Com estas informações, elaboramos no primeiro capítulo desta tese uma base teórica e consistente sobre grupóides, objetivando chegar a uma generalização do Teorema de Correspondência CHR. No segundo capítulo, introduzimos uma nova teoria, mais ampla, sobre G-conjuntos, e contruímos uma versão do Lema de Dedekind, tendo como finalidade a demonstração da Correspondência de Galois-Grothendieck para o caso de ação de grupóides. Nestes dois capítulos iniciais, trabalhamos num enredo onde assume-se de partida a comutatividade dos anéis envolvidos.

Entretanto, quando descarta-se a comutatividade do anel, ainda é possível obter resultados sobre o teorema fundamental. Não temos a correspondência em si, todavia temos caracterizações sobre álgebras que satisfazem o teorema. Em [23] e [24], G. Szeto e L. Xue mostraram situações onde a correspondência de Galois é injetiva, mas não necessariamente sobrejetiva, e deram caracterizações de álgebras de

Galois que satisfazem o teorema fundamental. Tendo em vista este fato, trazemos no terceiro capítulo desta tese generalizações destes resultados para o contexto de ações de grupóides.

Em uma abordagem geral, podemos notar que a teoria de Galois desenvolvida por Chase, Harrison e Rosenberg é sem dúvida a que mais se aproxima da teoria de Galois clássica, no sentido de que hoje podemos dizer tratar-se de uma "generalização natural" da mesma. No contexto de anéis comutativos cujos únicos idempotentes são 0 e 1, vê-se claramente o quanto esta generalização é natural, pois nesse caso a condição "G-forte" pode ser omitida, recaindo-se na correspondência clássica do caso de ação de grupos sobre corpos. Contudo, não é uma generalização absoluta para anéis quaisquer. A abordagem para anéis comutativos quaisquer é devida a O. E. Villamayor e D. Zelinsky, conhecida na literatura como teoria de Galois fraca. Em [25], esses autores desenvolveram uma teoria de Galois para anéis comutativos com um número finito de idempotentes, a qual resultou em uma correspondência bijetiva entre todas as subálgebras separáveis e determinados subgrupos (denominados subgrupos "gordos") do grupo de automorfismos. Já em [26], Villamayor e Zelinsky construiram uma teoria que se aplica a qualquer anel comutativo, sem qualquer restrição relativa a seus idempotentes. Nesta publicação, a correspondência de Galois estabelece uma bijeção entre todas as subálgebras separáveis da extensão e os subgrupos do grupo de automorfismos que satisfazem determinada "condição de fecho".

Como nota de curiosidade, nos bastidores deste trabalho de pesquisa conseguimos mostrar que toda extensão de Galois fraca para ação de grupóides (cuja definição é completamente natural em relação àquela dada para ação de grupos) é na verdade uma extensão de Galois fraca para ação de grupos, utilizando uma associação intermediária entre grupóides e semigrupos inversos, e semigrupos inversos com grupos, baseados nos resultados publicados em [2]. Com isso, acreditamos que a teoria de Galois fraca para ação de grupóides coincide com a teoria de Galois fraca para ação de grupos. Complementando esta informação, tentamos relacionar bijetivamente grupos satisfazendo determinada condição de fecho com grupóides satisfazendo semelhante condição, porém o caminho adotado não foi eficiente para obtermos tal propósito. Com isso, não conseguimos que o trabalho de Villamayor e Zelinsky fosse completamente generalizado, ficando este tópico ainda em aberto.

Por todo este trabalho, anel significa anel associativo unitário. Quando for necessário assumir a comutatividade do anel, será mencionado explicitamente.

Capítulo 1

Teorema de Correspondência de Galois

O Teorema de Correspondência de Galois para anéis comutativos devido a S. Chase, D. K. Harrison e A. Rosenberg ([8]) relaciona bijetivamente os subgrupos de um grupo finito G de automorfismos de uma dada álgebra R (chamado grupo de Galois) e as subálgebras separáveis que são G-fortes de R. O objetivo deste capítulo é relacionar as subálgebras de uma extensão de Galois (que satisfazem as propriedades do caso de grupos, porém generalizadas) com subestruturas de uma classe de elementos que generaliza grupos - os chamados grupóides.

Começaremos este trabalho com algumas definições e notações básicas, a fim de que o leitor se familiarize com a noção de grupóide. Neste capítulo, assume-se de partida a comutatividade de todos os anéis envolvidos.

1.1 Pré-requisitos

1.1.1 Grupóides

Grupóides são usualmente apresentados como categorias pequenas nas quais cada morfismo é invertível. Todavia, grupóides também podem ser vistos como estruturas algébricas, como uma generalização natural de grupos. Adotaremos aqui a versão axiomática dada em [19], como pode ser visto na definição que sucede.

Definição 1.1.1. *Um grupóide é um conjunto não vazio G, equipado com uma operação binária definida parcialmente (que será denotada por concatenação), onde os axiomas usuais de grupo ocorrem sempre que fizerem sentido, isto é:*
(i) Para todo $g, h, l \in G$, $g(hl)$ existe se, e somente se, $(gh)l$ existe, e neste caso são iguais.
(ii) Para todo $g, h, l \in G$, $g(hl)$ existe se, e somente se, gh e hl existem.
(iii) Para cada $g \in G$, existem (únicos) elementos $d(g), r(g) \in G$ tais que $gd(g)$ e $r(g)g$ existem e $gd(g) = g = r(g)g$.
(iv) Para cada $g \in G$, existe um elemento $g^{-1} \in G$ tal que $d(g) = g^{-1}g$ e $r(g) = gg^{-1}$.

Notação: Para todo $g, h \in G$, escreveremos $\exists gh$ sempre que o produto gh estiver definido.

Observação 1.1.2. *(a) Segue da definição que o elemento g^{-1} é único com a propriedade descrita em (iv), bem como $(g^{-1})^{-1} = g$, para todo $g \in G$.*
(b) Para todo $g, h \in G$, temos que $\exists gh$ se, e somente se, $d(g) = r(h)$, e neste caso, $d(gh) = d(h)$ e $r(gh) = r(g)$. Denotaremos por G^2 o subconjunto dos pares $(g, h) \in G \times G$ tais que $d(g) = r(h)$.
(c) Para todo $g, h \in G$, temos que $\exists gh$ se, e somente se, $\exists h^{-1}g^{-1}$, e neste caso, $(gh)^{-1} = h^{-1}g^{-1}$.

(d) Um elemento $e \in G$ é chamado identidade de G se $e = d(g) = r(g^{-1})$, para algum $g \in G$. Neste caso, e é chamado identidade domínio de g e identidade imagem de g^{-1}. O conjunto das identidades de G será denotado por G_0.
(e) Para qualquer $e \in G_0$, temos $d(e) = r(e) = e$, $e^{-1} = e$ e denotaremos por G_e o conjunto de todos elementos $g \in G$ tais que $d(g) = r(g) = e$.

Observe que, claramente, G_e é grupo, cujo elemento identidade é e. Este grupo é chamado *grupo principal associado a e*.

Vejamos alguns exemplos de grupóides.

Exemplo 1.1.3. *Todo grupo G é um grupóide, onde o produto gh está definido para todo $g, h \in G$ e $r(g) = d(g) = 1_G$ para todo $g \in G$.*

Exemplo 1.1.4. *A união disjunta $G = \dot{\bigcup\limits_{\lambda\in\Lambda}} G_\lambda$, onde cada G_λ ($\lambda \in \Lambda$) é um grupo, é um grupóide. O produto gh está definido se, e somente se, g e h pertencem a um mesmo G_λ e, neste caso, gh é exatamente o produto no grupo G_λ.*

Exemplo 1.1.5. *Seja G um grupo agindo por bijeções num conjunto X. Em $X \times G$ definimos a seguinte operação parcial:*

$$\exists (x, g)(y, h) \Leftrightarrow x = g.y \text{ e, neste caso, } (x, g)(y, h) = (x, gh).$$

O conjunto $X \times G$ com esta multiplicação parcial será denotado por $P(X, G)$. É fácil verificar que $P(X, G)$ é um grupóide, onde $(x, g)^{-1} = (g^{-1}.x, g^{-1})$, $d((x, g)) = (g^{-1}.x, 1_G)$ e $r((x, g)) = (x, 1_G)$, para todo $(x, g) \in X \times G$.

Exemplo 1.1.6. *Seja I um conjunto não vazio. Considere em $I \times I$ a seguinte operação binária parcial:*

$$\exists (i, j)(l, k) \Leftrightarrow j = l \text{ e, neste caso, } (i, j)(l, k) = (i, k).$$

Este conjunto com a operação definida acima é um grupóide, que denotaremos por $\widehat{I}$. *Note que* $(i,j)^{-1} = (j,i)$, $d((i,j)) = (j,j)$ *e* $r((i,j)) = (i,i)$. *Aqui,* $G_0 = \{(i,j) \in I \times I \mid i = j\}$.

Exemplo 1.1.7. *Considere* R *um anel e* G *o conjunto de todos os isomorfismos parciais entre ideais de* R. *Então* G *é um grupóide com multiplicação parcial dada pela composição e, dado* $g : I \longrightarrow J$ *em* G, $d(g) = Id_I$ *e* $r(g) = Id_J$. *Note que para* $g : I \longrightarrow J$ *e* $h : K \longrightarrow L$ *em* G, $\exists gh \Leftrightarrow I = L \Leftrightarrow Id_I = Id_L \Leftrightarrow d(g) = r(h)$.

Exemplo 1.1.8. *Sejam* R *uma extensão de corpos finita e separável de* K, N *o fecho normal desta extensão e* G *o grupo de Galois da extensão* N *sobre* K. *Se* $L = L_1, ..., L_n$ *denotam os diferentes conjugados de* L *em* N *sob a ação de* G *e* G_{ij} *denota o conjunto de isomorfismos de* L_i *em* L_j, $1 \leq i,j \leq n$, *então* $\overline{G} = \bigcup_{i,j} G_{ij}$ *é um grupóide, onde a operação parcial é definida por:*

$$\exists g_{ij} g_{lk} \Leftrightarrow j = l,$$

para todo $1 \leq i,j,k,l \leq n$. *Neste caso,* $g_{ij} g_{lk} = g_{ij} \circ g_{lk} \in G_{li}$.

Introduziremos agora a noção de ação de grupóide.

Definição 1.1.9. [4] *Sejam* G *um grupóide,* K *um anel comutativo e* R *uma* K-*álgebra unitária. Uma ação de* G *sobre* R *é um par*

$$\beta = (\{E_g\}_{g \in G}, \{\beta_g\}_{g \in G})$$

onde, para cada $g \in G$, $E_g = E_{r(g)}$ *é um ideal de* R *e* $\beta_g : E_{g^{-1}} \longrightarrow E_g$ *é um isomorfismo de* K-*álgebras satisfazendo as seguintes condições:*

(i) β_e *é a aplicação identidade* Id_{E_e} *de* E_e, *para todo* $e \in G_0$;

(ii) $\beta_g(\beta_h(r)) = \beta_{gh}(r)$, *para todo* $(g,h) \in G^2$ *e para todo* $r \in E_{h^{-1}} = E_{(gh)^{-1}}$.

É imediato ver que se $\beta = (\{E_g\}_{g\in G}, \{\beta_g\}_{g\in G})$ é uma ação de G sobre R, então $\beta_{(e)} = (\{E_g\}_{g\in G_e}, \{\beta_g\}_{g\in G_e})$ é uma ação do grupo G_e sobre o anel E_e, para todo $e \in G_0$. Em particular, $E_g = E_{r(g)} = E_e$, para todo $g \in G_e$.

Exemplo 1.1.10. *Considere* $G = \{d(g), r(g), g, g^{-1}\}$ *e* $R = Ke_1 \oplus Ke_2 \oplus Ke_3 \oplus Ke_4$, *onde* K *é um anel comutativo unitário e* e_1, e_2, e_3 *e* e_4 *são idempotentes dois a dois ortogonais cuja soma é* 1_R. *Tome* $E_{d(g)} = E_{g^{-1}} = Ke_1 \oplus Ke_2$ *e* $E_{r(g)} = E_g = Ke_3 \oplus Ke_4$. *Defina* $\beta_{d(g)} = Id_{E_{d(g)}}$, $\beta_{r(g)} = Id_{E_{r(g)}}$, $\beta_g(ae_1 + be_2) = ae_3 + be_4$ *e* $\beta_{g^{-1}}(ae_3 + be_4) = ae_1 + be_2$, *para todo* $a, b \in K$. *Então* $\beta = (\{E_g\}_{g\in G}, \{\beta_g\}_{g\in G})$ *é uma ação do grupóide* G *sobre* R.

Ao trabalhamos com grupóides, podemos introduzir a noção subestruturas fechadas para a operação parcial em questão, como veremos a seguir.

Definição 1.1.11. *Seja* G *um grupóide e* H *um subconjunto não vazio de* G. *Dizemos que* H *é um subgrupóide de* G *se satisfaz as seguintes condições:*
(i) Para todo $g, h \in H$, *se* $\exists gh$ *então* $gh \in H$;
(ii) Se $g \in H$, *então* $g^{-1} \in H$, *para todo* $g \in H$.

Lema 1.1.12. *Considere* $\beta = (\{E_g\}_{g\in G}, \{\beta_g\}_{g\in G})$ *uma ação do grupóide* G *sobre a álgebra* R, *onde cada* E_g *é uma álgebra unitária. Denote por* 1_e *a unidade de* E_e. *Para uma subálgebra* T *de* R, *seja* $H_T = \{g \in G \mid \beta_g(t1_{g^{-1}}) = t1_g$, *para todo* $t \in T\}$. *Então* H_T *é um subgrupóide.*

Demonstração: (i) Para $g, h \in H_T$ tal que $\exists gh$ temos:

$$\begin{aligned}
\beta_{gh}(t1_{h^{-1}g^{-1}}) &= \beta_g(\beta_h(t1_{h^{-1}})1_{g^{-1}}) = \beta_g(t1_h 1_{g^{-1}}) \\
&= \beta_g(t1_{r(h)}1_{g^{-1}}) = \beta_g(t1_{d(g)}1_{g^{-1}}) \\
&= \beta_g(t1_{g^{-1}}1_{g^{-1}}) = \beta_g(t1_{g^{-1}}) \\
&= t1_g = t1_{r(g)} = t1_{r(gh)} = t1_{gh},
\end{aligned}$$

para todo $t \in T$. Logo $gh \in H_T$;

(ii) Considere $g \in H_T$. Assim,

$$\begin{aligned}\beta_{g^{-1}}(t1_g) &= \beta_{g^{-1}}(\beta_g(t1_{g^{-1}})) = \beta_{g^{-1}g}(t1_{g^{-1}}) \\ &= \beta_{d(g)}(t1_{g^{-1}}) = t1_{g^{-1}},\end{aligned}$$

para todo $t \in T$. Desta forma $g^{-1} \in H_T$. ■

1.1.2 Subgrupóide Normal e Grupóide Quociente

Considere G um grupóide e H um subgrupóide de G. Para $g \in G$, tome o subconjunto de G definido por:

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H \quad e \quad r(h) = d(h) = r(g)\}$$

$$= \{g^{-1}hg \mid h \in H \cap G_{r(g)}\}.$$

Definição 1.1.13. *Dizemos que H é normal se $g^{-1}Hg \neq \emptyset$ e $g^{-1}Hg \subseteq H$ para todo $g \in G$.*

Note que esta definição, quando restrita a grupos, coincide exatamente com a definição de subgrupo normal.

Em [7], R. Brown fornece uma outra definição para subgrupóide normal. Entretanto, mostraremos que estas definições são equivalentes.

Definição 1.1.14. [7] *O subgrupóide H é dito normal se $G_0 = H_0$ e $g^{-1}H_{r(g)}g = H_{d(g)}$ para todo $g \in G$.*

Para verificar que a definição dada por Brown é equivalente à introduzida nesta tese, começaremos provando que $g^{-1}Hg \neq \emptyset$ se, e somente se, $G_0 = H_0$. De fato, se $g^{-1}Hg \neq \emptyset$ para todo $g \in G$, então dado $g \in G$, existe $h \in H$ tal que $r(g) = r(h) = d(h)$. Assim $r(g) \in H$ para todo $g \in G$. Logo $G_0 \subseteq H$ e consequentemente

$G_0 = H_0$. Reciprocamente, se $G_0 = H_0$, então dado $g \in G$, $r(g) \in H_0 \subseteq H$. Portanto $g^{-1}r(g)g = g^{-1}g = d(g) \in g^{-1}Hg$, desta maneira $g^{-1}Hg \neq \emptyset$.

Agora mostraremos que $g^{-1}Hg \subseteq H$ para todo $g \in G$ se, e somente se, $g^{-1}H_{r(g)}g = H_{d(g)}$ para todo $g \in G$. Com efeito, suponha que $g^{-1}Hg \subseteq H$ para todo $g \in G$. Observe que $H_{r(g)} = \{h \in H|\ r(g) = r(h) = d(h)\}$. Então temos que $g^{-1}Hg = \{g^{-1}hg \mid h \in H \text{ e } r(h) = d(h) = r(g)\} = g^{-1}H_{r(g)}g \subseteq H$, por hipótese. Logo dado $h \in H_{r(g)}$, existe $l \in H$ tal que $g^{-1}hg = l$. Isto implica que $d(l) = d(g^{-1}hg) = d(g)$ e $r(l) = r(g^{-1}hg) = r(g^{-1}) = d(g)$, portanto $l \in H_{d(g)}$. Desta maneira, temos que $g^{-1}H_{r(g)}g \subseteq H_{d(g)}$. Agora tome $h \in H_{d(g)}$. Note que $ghg^{-1} \in H_{r(g)}$, pois $d(ghg^{-1}) = d(g^{-1}) = r(g)$ e $r(ghg^{-1}) = r(g)$. Assim $h = g^{-1}(ghg^{-1})g \in g^{-1}H_{r(g)}g$, concluindo que $g^{-1}H_{r(g)}g = H_{d(g)}$. Reciprocamente, suponha $g^{-1}H_{r(g)}g = H_{d(g)}$. Então $g^{-1}Hg = g^{-1}H_{r(g)}g = H_{d(g)} \subseteq H$.

Vejamos exemplos de subgrupóides normais.

Exemplo 1.1.15. *Seja G um grupóide. Então $G_0 = \{e \in G \mid e = d(g) = r(g^{-1})$, para algum $g \in G\}$ é um subgrupóide normal de G. De fato, basta notar que $g^{-1}G_0g = \{r(g)\}$ para todo $g \in G$.*

Exemplo 1.1.16. *Como já vimos no Exemplo 1.1.4, $G = \dot{\bigcup\limits_{\lambda \in \Lambda}} G_\lambda$, onde cada G_λ ($\lambda \in \Lambda$) é um grupo, é um grupóide. Tomando H_λ um subgrupo normal de G_λ, para todo $\lambda \in \Lambda$, então $H = \dot{\bigcup\limits_{\lambda \in \Lambda}} H_\lambda$ é um subgrupóide normal de G.*

Com efeito, é fácil ver que H é um subgrupóide de G. Para mostrar que é normal, tome $g^{-1}Hg = \{g^{-1}hg|\ h \in G_{r(g)} \cap H\}$ e suponha $g \in G_\lambda$, para algum $\lambda \in \Lambda$. Então $g^{-1}Hg = g^{-1}H_\lambda g \subseteq H_\lambda$, pois cada H_λ é normal. Logo $g^{-1}Hg \subseteq \dot{\bigcup\limits_{\lambda \in \Lambda}} H_\lambda = H$ para todo $g \in G$. Mais ainda, $1_{G_\lambda} \in g^{-1}Hg$, para todo $g \in G_\lambda$, mostrando que $g^{-1}Hg \neq \emptyset$, para todo $g \in G$.

Exemplo 1.1.17. *Seja $P(X, G)$ como no Exemplo 1.1.5 e considere H um subgrupo normal de G. Então $X \times H$ é um subgrupóide normal de $P(X, G)$.*

De fato, seja $N = X \times H$ e considere $(x,g) \in P(X,G)$. Então:

$$(x,g)^{-1}N(x,g) = (g^{-1}x, g^{-1})N(x,g) =$$

$$\{(g^{-1}x, g^{-1})(y,h)(x,g) |\ (y,h) \in N \cap (X \times G)_{r((x,g))}\} =$$

$$\{(g^{-1}x, g^{-1})(y,h)(x,g) |\ (y,h) \in N \cap (X \times G)_{(x,1_G)}\}.\ (*)$$

Neste ponto, observe que $(X \times G)_{(x,1_G)} = \{(w,l) \in X \times G |\ (l^{-1}w, 1_G) = (w, 1_G) = (x, 1_G)\} = \{(x,l) \in X \times G |\ lx = x\}$. Desta maneira,

$$(*) = \{(g^{-1}x, g^{-1}h)(x,g) |\ hx = x\} = \{(g^{-1}x, g^{-1}hg) |\ hx = x\} \in X \times H = N.$$

Por conseguinte, segue também que $(x,g)^{-1}N(x,g) \neq \emptyset$, já que para todo $(x,g) \in P(X,G)$ e $(x,1_G) \in X \times H$, $(g^{-1}x, 1_G) = (g^{-1}x, g^{-1}1_G g) \in \{(g^{-1}x, g^{-1}hg) |\ hx = x\} = (x,g)^{-1}N(x,g)$.

Exemplo 1.1.18. *Seja G um grupóide e considere o subconjunto de G definido por $H = \{g \in G |\ d(g) = r(g)\}$. Não é difícil verificar que H é um subgrupóide, portanto mostraremos que H é de fato um subgrupóide normal.*

Observe que $g^{-1}Hg \neq \emptyset$, pois $r(g) \in H$, logo $g^{-1}r(g)g = g^{-1}g = d(g) \in H$.

Além disso, para $h \in H$ e $g \in G$ com $d(h) = r(h) = r(g)$, temos que $d(g^{-1}hg) = d(g)$ e $r(g^{-1}hg) = r(g^{-1}) = d(g)$, o que implica que $g^{-1}hg \in H$, concluindo que H é normal.

Definição 1.1.19. *Dizemos que um grupóide G é abeliano se satisfaz as seguintes condições:*
(i) Para cada $g \in G$, $d(g) = r(g)$;
(ii) Para todo $g, h \in G$ com $d(g) = r(h)$, $gh = hg$.

Exemplo 1.1.20. *Todo subgrupóide H de um grupóide abeliano G é normal. De fato, para todo $g \in G$, $g^{-1}Hg = \{g^{-1}hg|\ h \in H$ e $r(h) = d(h) = r(g)\} = \{g^{-1}gh|\ h \in H$ e $r(h) = d(h) = r(g)\} = \{d(g)h|\ h \in H$ e $r(h) = d(h) = r(g)\} = \{r(h)h|\ h \in H$ e $r(h) = d(h)\} = \{h|\ h \in H$ e $r(h) = d(h)\} = H$.*

Um exemplo natural de grupóide abeliano pode ser visualizado a seguir.

Exemplo 1.1.21. *Considere o grupóide G como no Exemplo 1.1.4, ou seja, $G = \dot{\bigcup\limits_{\lambda \in \Lambda}} G_\lambda$, onde cada G_λ $(\lambda \in \Lambda)$ é um grupo. Se, para cada $\lambda \in \Lambda$, G_λ for um grupo abeliano, então G é abeliano.*

Definição 1.1.22. [19] *Seja G um grupóide e $\equiv$ uma relação de equivalência em G. Suponha que $\overline{a}$ denote a classe de equivalência de a. Se para quaisquer $a, b, x, y \in G$ tais que $\exists ab$, $\exists xy$, $\overline{a} = \overline{x}$ e $\overline{b} = \overline{y}$ tivermos que $\overline{xy} = \overline{ab}$, então dizemos que $\equiv$ é uma congruência.*

Definição 1.1.23. *Seja G um grupóide e H um subgrupóide de G. Dizemos que H é amplo se $H_0 = G_0$.*

Lema 1.1.24. *Seja G um grupóide e H um subgrupóide amplo de G. Defina em G a seguinte relação $\equiv_H$: para todo $a, b \in G$, $a \equiv_H b \Leftrightarrow \exists b^{-1}a$ e $b^{-1}a \in H \Leftrightarrow \exists h \in H$ tal que $a = bh$. Então $\equiv_H$ é uma relação de equivalência. Mais ainda, H é um subgrupóide normal se, e somente se, $\equiv_H$ é uma congruência.*

Demonstração: Primeiramente vamos mostrar que $\equiv_H$ é uma relação de equivalência:

(i) $a \equiv_H a$, para todo $a \in G$, pois $a^{-1}a = d(a) \in G_0 \cap H$.

(ii) Suponha $a \equiv_H b$, para $a, b \in G$. Então $\exists b^{-1}a$ e existe $h \in H$ tal que $b^{-1}a = h$. Mas como H é subgrupóide, $a^{-1}b = h^{-1} \in H$. Note que $\exists a^{-1}b$, pois $r(b) = r(a)$. Logo $b \equiv_H a$.

(iii) Assuma $a \equiv_H b$ e $b \equiv_H c$, para $a, b, c \in G$. Isto implica que $\exists b^{-1}a$ e $\exists c^{-1}b$, isto é, $r(a) = r(b) = r(c)$, e existem $h, l \in H$ tais que $b^{-1}a = h$ e $c^{-1}b = l$. Mais ainda, como $d(l) = d(b) = r(h)$, temos que $\exists lh$ e $lh \in H$, utilizando novamente que H é subgrupóide. Mas $lh = c^{-1}a$, logo $a \equiv_H c$.

Agora suponha que H é um subgrupóide normal e tome $a, b, x, y \in G$ tais que $\exists ab$, $\exists xy$, $a \equiv_H x$ e $b \equiv_H y$. Vamos verificar que $xy \equiv_H ab$. Temos que

$$xy \equiv_H ab \Leftrightarrow b^{-1}a^{-1}xy \in H.$$

Como $a \equiv_H x$ e $b \equiv_H y$, isto implica que $\exists a^{-1}x$, $\exists b^{-1}y$, $a^{-1}x \in H$ e $b^{-1}y \in H$. Em particular, $r(a) = r(x)$ e $r(b) = r(y)$. Como $\exists ab$ e $\exists xy$, temos que $d(a) = r(b)$ e $d(x) = r(y)$. Logo o produto $b^{-1}a^{-1}xbb^{-1}y$ existe, e portanto $b^{-1}a^{-1}xy = b^{-1}a^{-1}xbb^{-1}y \in H$ já que $a^{-1}x \in H$, $b^{-1}y \in H$ e H é normal.

Reciprocamente, assuma que a relação $\equiv_H$ é uma congruência. Observe que $r(h) \equiv_H r(h)h$ para todo $h \in H$ e $g \equiv_H gl$ para todo $g \in G$ e $l \in H$ tal que $d(g) = r(l)$. Como $\equiv_H$ é uma congruência, isto implica que se $\exists r(h)g$ e $\exists r(h)hgl$ (ou seja, $r(h) = r(g)$ e $d(h) = r(g)$, ou ainda, $h \in H \cap G_{r(g)}$), então $r(h)g \equiv_H r(h)hgl$. Mas

$$r(h)g \equiv_H r(h)hgl \Leftrightarrow g^{-1}r(h)hgl = k, \text{ para algum } k \in H \Leftrightarrow g^{-1}hg = kl^{-1} \in H,$$
$$\text{com } d(k) = d(l),$$

para todo $g \in G$ e $h \in H \cap G_{r(g)}$.

Portanto $g^{-1}Hg = \{g^{-1}hg \mid h \in H \cap G_{r(g)}\} \subseteq H$, para todo $g \in G$, concluindo que H é normal. ■

Por definição, a classe de equivalência de $\equiv_H$ que contém x é o conjunto $xH = \{xh \mid h \in H \text{ e } d(x) = r(h)\}$. Chamaremos este conjunto de classe lateral à esquerda de H em G que contém x.

Definição 1.1.25. *A cardinalidade do conjunto das classes laterais à esquerda é o índice de H em G, e será denotado por $(G{:}H)$.*

Analogamente, podemos definir em G a seguinte relação de equivalência $\equiv'_H$: Para $a, b \in G$,

$$a \equiv'_H b \Leftrightarrow \exists ba^{-1} \quad e \quad ba^{-1} \in H \Leftrightarrow \exists h \in H \quad tal \quad que \quad b = ha.$$

Esta relação define a classe lateral à direita, que fica denotada por $Hx = \{hx | h \in H \text{ e } d(h) = r(x)\}$.

Observação 1.1.26. *O índice de H em G é também a cardinalidade do conjunto das classes laterais à direita de H em G. Com efeito, o leitor verifica facilmente que a aplicação abaixo é uma bijeção.*

$$\begin{array}{rccc} \phi : & \{classes \quad à \quad esquerda\} & \longrightarrow & \{classes \quad à \quad direita\} \\ & xH & \longmapsto & Hx^{-1} \end{array}$$

Observação 1.1.27. *Note que: (1) H normal $\Rightarrow$ H é amplo, pela definição.*
(2) H normal $\Leftrightarrow gH = Hg$ para todo $g \in G$. De fato, considere $gH = Hg$ e tome $h \in H$ com $d(h) = r(h) = r(g)$ (o que implica que o produto $g^{-1}hg$ está definido). Como $gH = Hg$, existe $l \in H$ com $r(l) = d(g)$ tal que $gl = hg$, ou seja, $g^{-1}hg = l \in H$, mostrando que H é normal.

Reciprocamente, suponha que H é normal. Dados $g \in G$ e $h \in H$ com $r(g) = r(h) = d(h)$, temos que $g^{-1}hg \in H$, ou seja, $g^{-1}hg = l$ para algum $l \in H$. Logo $hg = gl$, mostrando que $Hg = gH$.

Portanto, concluímos que quando H é normal, temos que $\equiv_H = \equiv'_H$, uma vez que suas classes de equivalência são iguais.

Porém, observe que $g^{-1}Hg \subseteq H \nRightarrow g^{-1}Hg = H$. Basta visualizar o Exemplo 1.1.15, onde $H = G_0$.

Considere H um subgrupóide do grupóide G tal que $G_0 \subseteq H$. Para $x, y \in G$, tome as classes laterais à esquerda xH e yH. Suponha $xH \cap yH \neq \emptyset$ e pegue

$z \in xH \cap yH$. Isto acarreta que $z = xh = yl$, para determinados $h, l \in H$. Logo $ylh^{-1} = xhh^{-1} = xr(h) = xd(x) = x$ (note que $d(l) = d(h) = r(h^{-1})$, por isso o produto ylh^{-1} está definido). Analogamente, $y = xhl^{-1}$, concluindo que $xH = yH$. Portanto temos $xH \cap yH = \emptyset$ ou $xH = yH$, para todo $x, y \in G$. Mais ainda, todo elemento está contido em sua classe de equivalência, desta maneira $G = \dot{\bigcup\limits_{x\in G}} xH$. Entretanto, é importante salientar que as classes laterais não possuem a mesma cardinalidade, como ocorre no caso de grupos. Veja o seguinte exemplo:

Exemplo 1.1.28. *Considere o grupóide definido por $G = \mathbb{Z} \cup S_3$, onde S_3 é o grupo das permutações de três elementos (já vimos no Exemplo 1.1.4 que a união disjunta de grupos é um grupóide). Tome o subgrupóide $H = 2\mathbb{Z} \cup S_3$ e a relação $\equiv_H$ definida no Lema 1.1.24. Então $0H = \{0 + 2z \mid z \in \mathbb{Z}\} = 2\mathbb{Z}$ e $Id_{S_3}H = \{Id_{S_3}s \mid s \in S_3\} = S_3$, concluindo que $\#(0H) = \infty$ e $\#(Id_{S_3}H) = 6$.*

Com este exemplo visualizamos claramente que o Teorema de Lagrange não se aplica no caso de grupóides.

Definição 1.1.29. *Dada uma partição de um conjunto, um sistema de representantes é um conjunto $\{x_i\}_{i\in I}$ que tem exatamente um elemento em cada subconjunto da partição. Em particular, a cardinalidade de qualquer sistema de representantes das classes laterais à esquerda de H em G é igual a $(G : H)$.*

O conjunto das classes laterais à esquerda é denotado por $\frac{G}{H}$.

Lema 1.1.30. *Considere G um grupóide, H um subgrupóide normal de G e $\equiv_H$ a relação de equivalência em G definida no Lema 1.1.24. Então $\frac{G}{H}$ é um grupóide, chamado grupóide quociente.*

Demonstração: Como já foi mostrado no Lema 1.1.24, $\equiv_H$ é uma congruência. Defina:

$$aH.bH = abH \quad se \quad \exists ab.$$

Como $\equiv_H$ é uma congruência, esta operação está bem definida. Vamos verificar as propriedades de grupóide:

(i) Como G é um grupóide, sabemos que $\exists a(bc) \Leftrightarrow \exists (ab)c$ para todo $a, b, c \in G$, o que implica que $\exists a(bc)H \Leftrightarrow \exists (ab)cH$, consequentemente $\exists aH(bHcH)) \Leftrightarrow \exists (aHbH)cH$, e neste caso são iguais;

(ii) Diretamente de G ser um grupóide, também temos que $\exists aH(bHcH) \Leftrightarrow \exists aHbH$ e $\exists bHcH$;

(iii) Para cada $a, b \in G$ tal que $d(a) = r(b)$, temos: $aHbH = aH \Leftrightarrow abH = aH \Leftrightarrow \exists a^{-1}ab$ e $a^{-1}ab \in H$, ou seja, $b = r(b)b = d(a)b = a^{-1}ab \in H$. Mas $b \in H \Rightarrow bH = r(b)H$, pois $b^{-1}r(b) = b^{-1}d(b^{-1}) = b^{-1} \in H$, logo $bH = r(b)H = d(a)H$, o que significa que $d(aH) = d(a)H$. Analogamente, $r(aH) = r(a)H$;

(iv) $(aH)^{-1} = a^{-1}H$, pois $aHa^{-1}H = aa^{-1}H = r(a)H$ e $a^{-1}HaH = a^{-1}aH = d(a)H$.

Assim, $\frac{G}{H}$ é um subgrupóide. ■

1.2 Teoria de Galois

Para o que segue neste capítulo, sejam:

- K um anel;
- R uma K-álgebra;
- G um grupóide finito;
- $\beta = (\{E_g\}_{g \in G}, \{\beta_g\}_{g \in G})$ uma ação de G sobre R tal que cada E_g é uma K-álgebra unitária e $R = \bigoplus_{e \in G_0} E_e$.

Denotemos por 1_e a unidade de E_e. Neste caso, $1_R = \sum_{e \in G_0} 1_e$.

Considere o conjunto dos elementos invariantes sobre a ação de β definido por:

$$R^\beta = \{r \in R \mid \beta_g(r1_{g^{-1}}) = r1_g \text{ para todo } g \in G\}.$$

Observe que este subconjunto de R é, de fato, uma K-subálgebra de R. Com efeito, para $r, s \in R^\beta$, $\lambda \in K$ e $g \in G$, temos:

(i) $\beta_g(\lambda r1_{g^{-1}}) = \lambda\beta_g(r1_{g^{-1}}) = \lambda r1_g$;

(ii) $\beta_g((r-s)1_{g^{-1}}) = \beta_g(r1_{g^{-1}} - s1_{g^{-1}}) = \beta_g(r1_{g^{-1}}) - \beta_g(s1_{g^{-1}}) = r1_g - s1_g = (r-s)1_g$; e

(iii) $\beta_g(rs1_{g^{-1}}) = \beta_g(r1_{g^{-1}}s1_{g^{-1}}) = \beta_g(r1_{g^{-1}})\beta_g(s1_{g^{-1}}) = r1_g s1_g = rs1_g$.

Definição 1.2.1. [4] *Dizemos que R é uma extensão β-Galois de R^β se existem elementos $x_i, y_i \in R$, $1 \leq i \leq m$, tais que $\sum_{1\leq i\leq m} x_i\beta_g(y_i 1_{g^{-1}}) = \delta_{e,g}1_e$ para todo $e \in G_0$ e $g \in G$. O conjunto $\{x_i, y_i\}_{1\leq i\leq m}$ é chamado sistema de coordenadas de Galois de R sobre R^β.*

Definição 1.2.2. [4] *O skew anel de grupóide $R\star_\beta G$ correspondente à β é definido como a soma direta*

$$R \star_\beta G = \bigoplus_{g\in G} E_g u_g,$$

onde os u_g's são símbolos, com a adição usual, e multiplicação determinada por

$$(xu_g)(yu_h) = \begin{cases} x\beta_g(y1_{g^{-1}})u_{gh}, & \textit{se} \quad (g,h) \in G^2 \\ 0, & \textit{caso contrário,} \end{cases}$$

para todo $g, h \in G, x \in E_g$ e $y \in E_h$.

O próximo teorema, encontrado em [4], fornece equivalências para a definição de extensão β-Galois, e será usado frequentemente na demonstração do Teorema Fundamental.

Teorema 1.2.3. [[4], Theorem 5.3] *As seguintes condições são equivalentes:*

(i) R é uma extensão β-Galois de R^β.

(ii) R é um R^β-módulo projetivo finitamente gerado e a aplicação $j : R \star_\beta G \longrightarrow$

$End_{R^\beta}(R)$ dada por $j(\sum_{g\in G} a_g u_g)(x) = \sum_{g\in G} a_g\beta_g(x1_{g^{-1}})$ é um isomorfismo de R^β-álgebras e de R-módulos.

(iii) Para todo $R\star_\beta G$ - módulo à esquerda M, a aplicação $\mu : R\otimes_{R^\beta} M^G \longrightarrow M$ dada por $\mu(x\otimes m) = xm$ é um isomorfismo de R-módulos.

(iv) A aplicação $\phi : R\otimes_{R^\beta} R \longrightarrow \prod_{g\in G} E_g$ dada por $\phi(x\otimes y) = (x\beta_g(y1_{g^{-1}}))_{g\in G}$ é um isomorfismo de R-módulos.

(v) $RtR = R\star_\beta G$, onde $t = \sum_{g\in G} 1_g u_g$.

(vi) A aplicação $\tau' : R\otimes_{R^\beta} R \longrightarrow R\star_\beta G$ dada por $\tau'(x\otimes y) = \sum_{g\in G} x\beta_g(y1_{g^{-1}})\delta_g$ é sobrejetiva.

(vii) R é um gerador para a categoria dos $R\star_\beta G$-módulos à esquerda.

Definição 1.2.4. *Seja A uma R-álgebra unitária. Dizemos que A é R-separável se existe um elemento $e = \sum_{i=1}^{n} x_i\otimes_R y_i \in A\otimes_R A$ tal que $\sum_{i=1}^{n} x_i y_i = 1_A$ e $ae = ea$ para todo $a\in A$. Este elemento e é chamado idempotente de separabilidade de A sobre R e é de fato um idempotente, pois R é comutativo.*

D. Flôres mostrou em [15] o seguinte lema, que será útil na demonstração do Teorema Fundamental.

Lema 1.2.5. *Se R é uma extensão β-Galois de R^β, então R é uma extensão separável de R^β.*

Definição 1.2.6. *Sejam $f, g : S \longrightarrow T$ homomorfismos de anéis comutativos. Dizemos que f e g são fortemente distintos se, para todo idempotente não nulo $e\in T$, existe $s\in S$ tal que $f(s)e \neq g(s)e$.*

Lema 1.2.7. [[8], Lema 1.2] *Seja S uma R-álgebra separável comutativa e $f : S \longrightarrow R$ um homomorfismo de R-ágebras. Então existe um único idempotente $e\in S$ tal que $f(e) = 1$ e $se = f(s)e$, para todo $s\in S$. Mais ainda, se $f_1, ..., f_n$ são* *homomorfismos de R-álgebras de S em R dois a dois fortemente distintos, então os correspondentes idempotentes $e_1, ..., e_n$ são dois a dois ortogonais e $f_i(e_j) = \delta_{ij}$.*

Seja $tr_\beta : R \longrightarrow R$ a aplicação definida por $tr_\beta(x) = \sum_{g \in G} \beta_g(x1_{g^{-1}})$, chamada aplicação *traço.* Não é difícil verificar que tr_β é uma aplicação R^β-linear. Por [4], Lemma 4.2, temos que se $\beta = (\{E_g\}_{g\in G}, \{\beta_g\}_{g\in G})$ é uma ação de um grupóide finito G sobre uma K-álgebra unitária R tal que cada E_e é unitário para cada $e \in G_0$ e $R = \bigoplus_{e \in G_0} E_e$, então $tr_\beta(R) \subseteq R^\beta$. Mais ainda, se R, em adição, for um anel comutativo, [4], Corollary 5.4, garante que $tr_\beta(R) = R^\beta$. A hipótese de $R = \bigoplus_{e \in G_0} E_e$ é de fundamental importância para a validade deste resultado. Em [4], é mostrado um exemplo onde esta hipótese não é admitida e a condição $tr_\beta(R) \subseteq R^\beta$ não se verifica.

Observação 1.2.8. *Como estamos considerando R um anel comutativo, temos $tr_\beta(R) = R^\beta$. Agora observe que:*

(1) Como $1_R \in R^\beta$, existe $c \in R$ tal que $tr_\beta(c) = 1_R$.

(2) R^β é isomorfo a um somando direto de R como R^β-módulo. De fato, tr_β é uma aplicação sobrejetiva, logo $R \simeq R^\beta \oplus ker(tr_\beta)$.

Lembrando que $H_T = \{g \in G \mid \beta_g(t1_{g^{-1}}) = t1_g$, para todo $t \in T\}$, temos a seguinte definição:

Definição 1.2.9. *Dizemos que um subanel T de R é β-forte se para todo $g, h \in G$ com $r(g) = r(h)$, $g^{-1}h \notin H_T$ e para qualquer idempotente não nulo $e \in E_g = E_h$, existe um elemento $t \in T$ tal que $\beta_g(t1_{g^{-1}})e \neq \beta_h(t1_{h^{-1}})e$.*

1.3 Teorema Fundamental

Frisamos neste instante que o contexto trabalhado é precisamente o que foi abordado na seção anterior, isto é, K é um anel, R é uma K-álgebra, G é um grupóide finito e $\beta = (\{E_g\}_{g\in G}, \{\beta_g\}_{g\in G})$ é uma ação de G sobre R tal que cada E_g é uma álgebra unitária, e $R = \bigoplus_{e\in G_0} E_e$. Adicionalmente, vamos supor $E_g = E_{r(g)} \neq 0$ para cada $g \in G$. Este fato será utilizado na demonstração do item (iv) do próximo teorema.

Teorema 1.3.1. *Suponha que R é uma extensão β-Galois de R^β. Sejam H um subgrupóide de G e $R_H = \bigoplus_{e\in H_0} E_e$. Então:*
(i) $\beta_H = \{\beta_h : E_{h^{-1}} \longrightarrow E_h \mid h \in H\}$ é uma ação de H sobre R_H e R_H é uma extensão β_H-Galois de $T = (R_H)^{\beta_H}$.
(ii) T é R^β-separável.
Além disso, se H é amplo, então:
(iii) $R_H = R$ e T é β-forte.
(iv) $H = H_T$.
(v) Se H é normal e $\equiv_H$ é a congruência definida no Lema 1.1.24, então $\frac{G}{H}$ age sobre T via uma ação $\overline{\beta}$ e T é uma extensão $\overline{\beta}$-Galois de R^β.

Demonstração: (i) O fato de β_H ser uma ação de H sobre R_H é uma consequência imediata de β ser uma ação de G sobre R. Sejam $x_i, y_i \in R, 1 \leq i \leq m$, tais que $\sum_{1\leq i\leq m} x_i\beta_g(y_i 1_{g^{-1}}) = \delta_{e,g}1_e$, para todo $e \in G_0, g \in G$. Considere $1_{R_H} = \sum_{e\in H_0} 1_e$ e tome $\widetilde{x}_i = x_i 1_{R_H}$ e $\widetilde{y}_i = y_i 1_{R_H}$. Note que R_H é ideal de R, pois é uma soma de ideais de R, logo $\widetilde{x}_i, \widetilde{y}_i \in R_H$. Então, para cada $h \in H$, $\sum_{1\leq i\leq m} \widetilde{x}_i\beta_h(\widetilde{y}_i 1_{h^{-1}}) = \sum_{1\leq i\leq m} x_i 1_{R_H}\beta_h(y_i 1_{R_H} 1_{h^{-1}}) = \sum_{1\leq i\leq m} x_i\beta_h(y_i 1_{h^{-1}}) = \delta_{e,h}1_e$, para todo $e \in G_0$ e $h \in H$. Observando que $\delta_{e,h}1_e \neq 0$ somente quando $h = e$ para algum $e \in H \cap G_0 = H_0$, temos que $\sum_{1\leq i\leq m} \widetilde{x}_i\beta_h(\widetilde{y}_i 1_{h^{-1}}) = \delta_{e,h}1_e$, para todo $e \in H_0$ e $h \in H$, mostrando que R_H é uma extensão β_H-Galois de T.

(ii) Pelo item (i), R_H é uma extensão β_H-Galois de T. Logo pelo Teorema 1.2.3, item (ii), R_H é um T-módulo projetivo finitamente gerado. Desta maneira, existe $r \in \mathbb{Z}^+$ tal que $T^r = R_H \oplus L$, onde L é um T-módulo. Observe que R_H e T são R^β-módulos via a multiplicação em R. De fato, R_H é ideal de R e para $x \in R^\beta$ e $t \in T$, $\beta_h(xt1_{h^{-1}}) = \beta_h(x1_{h^{-1}})\beta_h(t1_{h^{-1}}) = xt1_h, \forall h \in H$, concluindo que $xt \in T$. Mais ainda, $R_H \otimes_{R^\beta} R_H$ é um $T \otimes_{R^\beta} T$-módulo projetivo, pois

$$(T \otimes_{R^\beta} T)^{r^2} = T^r \otimes_{R^\beta} T^r = (R_H \oplus L) \otimes_{R^\beta} (R_H \oplus L) = (R_H \otimes_{R^\beta} R_H) \oplus M,$$

onde $M = (R_H \otimes_{R^\beta} L) \oplus (L \otimes_{R^\beta} R_H) \oplus (L \otimes_{R^\beta} L)$. Além disso, utilizando que R_H é uma R^β-álgebra, R_H é um somando direto de R e R é uma álgebra R^β-separável, por [17], Proposition III.1.7, temos que R_H é uma R^β-álgebra separável, ou seja, R_H é projetivo sobre $R_H \otimes_{R^\beta} R_H$. Assim existem $s \in \mathbb{Z}^+$ e N um $(R_H \otimes_{R^\beta} R_H)$-módulo tais que $(R_H \otimes_{R^\beta} R_H)^s = R_H \oplus N$. Portanto

$$(T \otimes_{R^\beta} T)^{r^2 s} = (R_H \otimes_{R^\beta} R_H)^s \oplus M^s = R_H \oplus N \oplus M^s,$$

concluindo que R_H é um $(T \otimes_{R^\beta} T)$-módulo projetivo.

Pela Observação 1.2.8, T é um T-módulo somando direto de R_H e consequentemente um R^β-módulo somando direto de R_H. Então

$$(T \otimes_{R^\beta} T)^{r^2 s} = R_H \oplus N \oplus M^s = T \oplus ker(tr_{\beta_H}) \oplus N \oplus M^s,$$

mostrando que T é $(T \otimes_{R^\beta} T)$-projetivo. Logo T é uma R^β-álgebra separável.

(iii) Como H é amplo, é imediato ver que $R_H = R$. Desde que R é uma extensão β_H-Galois de T, segue da Observação 1.2.8 que existe $c \in R$ tal que $tr_{\beta_H}(c) = 1_R$, isto é, $\sum\limits_{h \in H} \beta_h(c1_{h^{-1}}) = 1_R$.

Dados $x_i, y_i \in R$ tais que $\sum\limits_{1 \leq i \leq m} x_i \beta_h(y_i 1_{h^{-1}}) = \delta_{e,h} 1_e$, para todo $e \in H_0$ e $h \in H$, tome $x_i' = \sum\limits_{h \in H} \beta_h(cx_i 1_{h^{-1}})$ e $y_i' = \sum\limits_{h \in H} \beta_h(y_i 1_{h^{-1}})$, para todo $1 \leq i \leq m$. Note que

$x_i' = tr_{\beta_H}(cx_i)$ e $y_i' = tr_{\beta_H}(y_i)$, logo segue da Observação 1.2.8 que $x_i', y_i' \in T$.

Afirmação 1: $\sum\limits_{i=1}^{m} x_i' y_i' = 1_R$.

$$
\begin{aligned}
\sum_{i=1}^{m} x_i' y_i' &= \sum_{i=1}^{m} \Big(\sum_{h\in H} \beta_h(cx_i 1_{h^{-1}}) \sum_{l\in H} \beta_l(y_i 1_{l^{-1}})\Big)\\
&= \sum_{i=1}^{m} \sum_{h,l\in H} \beta_h(cx_i \beta_{h^{-1}}(\beta_l(y_i 1_{l^{-1}}) 1_h))\\
&= \sum_{i=1}^{m} \sum_{r(h)=r(l)} \beta_h(cx_i \beta_{h^{-1}l}(y_i 1_{l^{-1}h}))\\
&= \sum_{r(h)=r(l)} \beta_h(c \sum_{i=1}^{m} x_i \beta_{h^{-1}l}(y_i 1_{l^{-1}h}))\\
&= \sum_{r(h)=r(l)} \beta_h(c\delta_{e,h^{-1}l} 1_e)
\end{aligned}
$$

Mas se $e = h^{-1}l$ para algum $e \in H_0$, então $e = r(e) = r(h^{-1}l) = r(h^{-1}) = d(h)$. Logo $h = he = hh^{-1}l = r(h)l = r(l)l = l$. Portanto,

$$
\begin{aligned}
\sum_{i=1}^{m} x_i' y_i' &= \sum_{r(h)=r(l)} \beta_h(c\delta_{e,h^{-1}l} 1_e) = \sum_{h\in H} \beta_h(c1_{d(h)})\\
&= \sum_{h\in H} \beta_h(c1_{r(h^{-1})}) = \sum_{h\in H} \beta_h(c1_{h^{-1}}) = 1_R.
\end{aligned}
$$

Afirmação 2:

$$
\sum_{i=1}^{m} x_i' \beta_g(y_i' 1_{g^{-1}}) = \begin{cases} 1_g, & \text{se} \quad g \in H \\ 0, & \text{caso contrário.} \end{cases}
$$

Desde que $x_i', y_i' \in T = R^{\beta_H}$, $\sum\limits_{i=1}^{m} x_i' \beta_g(y_i' 1_{g^{-1}}) = \sum\limits_{i=1}^{m} x_i' y_i' 1_g = 1_g$, para todo $g \in G$.

Se $g \notin H$, então

$$
\begin{aligned}
\sum_{i=1}^{m} x_i'\beta_g(y_i'1_{g^{-1}}) &= \sum_{i=1}^{m}\sum_{h\in H}\beta_h(cx_i1_{h^{-1}})\beta_g(\sum_{l\in H}\beta_l(y_i1_{l^{-1}})1_{g^{-1}}) \\
&= \sum_{i=1}^{m}\sum_{h\in H}\beta_h(cx_i1_{h^{-1}})\sum_{d(g)=r(l)}\beta_{gl}(y_i1_{l^{-1}g^{-1}}) \\
&= \sum_{i=1}^{m}\sum_{\substack{r(h)=r(g)\\ d(g)=r(l)}}\beta_h(cx_i\beta_{h^{-1}gl}(y_i1_{l^{-1}g^{-1}h})) \\
&= \sum_{\substack{r(h)=r(g)\\ d(g)=r(l)}}\beta_h(c\delta_{e,h^{-1}gl}1_e).
\end{aligned}
$$

Se $h^{-1}gl = e$ para algum $e \in G_0$, então $e = r(e) = r(h^{-1}gl) = r(h^{-1}) = d(h)$. Desta forma,

$$gl = r(h)gl = hh^{-1}gl = hd(h) = h \Rightarrow gll^{-1} = hl^{-1}$$

$$\Rightarrow gr(l) = hl^{-1} \Rightarrow gd(g) = hl^{-1} \Rightarrow g = hl^{-1} \in H.$$

Mas isso é um absurdo. Logo $h^{-1}gl \neq e$ para todo $e \in G_0$, e portanto

$$\sum_{\substack{r(h)=r(g)\\ d(g)=r(l)}}\beta_h(c\delta_{e,h^{-1}gl}1_e) = 0,$$

o que completa a afirmação.

Suponha que g, h são elementos em G com $r(g) = r(h) \in H_0$, tais que $g^{-1}h \notin H$. Seja $e \in E_g$ um idempotente não nulo tal que $\beta_g(t1_{g^{-1}})e = \beta_h(t1_{h^{-1}})e$ para todo $t \in T$. Isto implica que $t\beta_{g^{-1}}(e) = \beta_{g^{-1}h}(t1_{h^{-1}g})\beta_{g^{-1}}(e)$ para todo $t \in T$. Seja $e' = \beta_{g^{-1}}(e)$. Como $y_i' \in T$ e $\sum_{i=1}^{m} x_i'y_i' = 1_R$, temos

$$e' = 1_Re' = (\sum_{i=1}^{m} x_i'y_i')e' = \sum_{i=1}^{m} x_i'\beta_{g^{-1}h}(y_i'1_{h^{-1}g})e' = 0.$$

A última igualdade segue da Afirmação 2 e do fato que $g^{-1}h \notin H$. Como $0 = e' = \beta_{g^{-1}}(e)$, segue que $e = 0$, o que é um absurdo. Portanto T é β-forte.

(iv) Considere H amplo e lembre que $H_T = \{g \in G \mid \beta_g(t1_{g^{-1}}) = t1_g$, para todo $t \in T\}$. Note que igualmente temos $R_H = R$. Como já vimos no Lema 1.1.12, H_T é um subgrupóide de G, e claramente contém H, já que $T = R^{\beta_H}$.

Observe que $R^{\beta_{H_T}} = R^{\beta_H} = T$. De fato, como $H \subseteq H_T$, então $R^{\beta_{H_T}} \subseteq R^{\beta_H}$. A inclusão contrária segue da definição de H_T. Portanto, de (i) segue que R é uma extensão β_H-Galois de $R^{\beta_{H_T}} = R^{\beta_H}$.

Sejam n, n' as ordens de H e H_T, respectivamente. Pelo Teorema 1.2.3, item (iv), as aplicações

$$\begin{array}{rcl} \phi \ : \ R \otimes_T R & \longrightarrow & \displaystyle\prod_{h \in H} E_h \\ x \otimes y & \longmapsto & (x\beta_h(y1_{h^{-1}}))_{h \in H} \end{array}$$

e

$$\begin{array}{rcl} \widetilde{\phi} \ : \ R \otimes_T R & \longrightarrow & \displaystyle\prod_{h \in H_T} E_h \\ x \otimes y & \longmapsto & (x\beta_h(y1_{h^{-1}}))_{h \in H_T} \end{array}$$

são isomorfismos de R-módulos.

Portanto, $\displaystyle\prod_{h \in H} E_h \simeq \prod_{h \in H_T} E_h$. Agora suponha que existe $g \in H_T - H$ e tome $z = (0, ..., 0, 1_g, 0, ..., 0) \in \displaystyle\prod_{h \in H_T} E_h$. Note que $z \neq 0$, pois $E_g \neq 0$, para todo $g \in G$. Como $\widetilde{\phi}$ é um isomorfismo, existe $0 \neq x = \displaystyle\sum_{i=1}^{m} r_i \otimes_T s_i \in R \otimes_T R$ tal que $\widetilde{\phi}(x) = z$, ou seja, $(\displaystyle\sum_{i=1}^{m} r_i\beta_h(s_i1_{h^{-1}}))_{h \in H_T} = z = (\delta_{g,h}1_g)_{h \in H_T}$. Isto implica que $\displaystyle\sum_{i=1}^{m} r_i\beta_h(s_i1_{h^{-1}}) = \delta_{g,h}1_g$, para cada $h \in H_T$. Então temos que $\phi(x) = (\displaystyle\sum_{i=1}^{m} r_i\beta_h(s_i1_{h^{-1}}))_{h \in H} = (\delta_{g,h}1_g)_{h \in H} = 0$ e isto gera um absurdo, pois ϕ é um isomorfismo. Portanto $H = H_T$.

(v) Finalmente, suponha que H é um subgrupóide normal de G. Então, pelos Lemas 1.1.24 e 1.1.30, temos que a relação de equivalência $\equiv_H$ dada por

$$a \equiv_H b \Leftrightarrow \exists b^{-1}a \quad e \quad b^{-1}a \in H$$

é uma congruência e $\frac{G}{H}$ é um grupóide. Considere $\{g_i\}_{1 \leq i \leq n}$ um sistema de representantes das classes de equivalência de $\equiv_H$. Então $g \equiv_H g_i \Leftrightarrow$ existe $h \in H$ tal que $\exists g_ih$ e $g = g_ih$. Para facilitar a notação, considere $gH = \overline{g}$.

Considere $e_{g_i} = tr_{\beta_H}(1_{g_i}) = e_g$, para $g \in G$ tal que $g = g_i h$ para algum $h \in H$. Note que este elemento é um idempotente de R, pois

$$tr_{\beta_H}(1_{g_i}) = \sum_{h \in H} \beta_H(1_{g_i} 1_{h^{-1}}) = \sum_{r(g_i)=d(h)} \beta_H(1_{g_i} 1_{h^{-1}}) = \sum_{r(g_i)=r(h)} 1_h.$$

Tome os ideais de T dados por $E_{\overline{g}} = Te_{g_i} = Te_g$, onde $g = g_i h$ para algum $h \in H$. Note que $E_{\overline{g}}$ é de fato um ideal de T, visto que $e_{g_i} \in T$. Defina uma ação $\overline{\beta}$ de $\frac{G}{H}$ sobre $T = R^{\beta_H}$ por:

$$\overline{\beta}_{\overline{g}}(te_{g^{-1}}) = \beta_{g_i}(te_{g_i^{-1}}),$$

onde $g = g_i h$, para algum $h \in H$. Note que esta aplicação está bem definida de $E_{\overline{g}^{-1}}$ em $E_{\overline{g}}$, pois

$$\beta_{g_i}(e_{g_i^{-1}}) = \beta_{g_i}(\sum_{d(g_i)=r(h)} 1_h) = \sum_{d(g_i)=r(h)} \beta_{g_i}(1_h) = \sum_{r(g_i)=r(h)} 1_h = e_{g_i}.$$

Observe que $(\frac{G}{H})_0 = \{d(gH) | gH \in \frac{G}{H}\} = \{d(g)H | g \in G\} = \frac{G_0}{H} = \overline{G_0}$. Assim, não é difícil ver que $\bigoplus_{\overline{e} \in (\overline{G})_0} E_{\overline{e}} = T$.

Afirmação: $T^{\overline{\beta}} = R^{\beta}$.

($\subseteq$) Seja $t \in T^{\overline{\beta}}$. Note que, para cada $g \in G$, existe $i \in \{1, ..., n\}$ e $h \in H$ tal que $d(g_i) = r(h)$ e $g = g_i h$. Assim:

$$\begin{aligned}
\beta_g(t1_{g^{-1}}) &= \beta_{g_i h}(t1_{h^{-1}g_i^{-1}}) = \beta_{g_i}(\beta_h(t1_{h^{-1}})1_{g_i^{-1}}) \\
&= \beta_{g_i}(t1_h 1_{g_i^{-1}}) = \beta_{g_i}(t1_{g_i^{-1}}) \\
&= t1_{g_i} = t1_g,
\end{aligned}$$

portanto $t \in R^{\beta}$.

($\supseteq$) Seja $t \in R^{\beta}$. Logo temos:

$$\begin{aligned}
\overline{\beta}_{\overline{g}}(te_{g_i^{-1}}) &= \beta_{g_i}(te_{g_i^{-1}}) = \beta_{g_i}(t \sum_{d(g_i)=r(h)} 1_h) \\
&= t \sum_{d(g_i)=r(h)} \beta_{g_i}(1_h) = t \sum_{r(g_i)=r(h)} 1_h \\
&= te_{g_i},
\end{aligned}$$

concluindo que $t \in T^{\overline{\beta}}$.

Já sabemos que $x'_i, y'_i \in T$. Por um raciocínio semelhante ao que foi feito na Afirmação 2 temos que:

$$\sum_{i=1}^{m} x'_i \beta_g(y'_i 1_{g^{-1}}) = \begin{cases} 1_g, & \text{se} \quad g \in G_0 \\ 0, & \text{caso contrário.} \end{cases}$$

Mas $\sum_{i=1}^{m} x'_i \beta_g(y'_i 1_{g^{-1}}) = \sum_{i=1}^{m} x'_i \beta_{g_j h}(y'_i 1_{h^{-1} g_j^{-1}}) = \sum_{i=1}^{m} x'_i \beta_{g_j}(y'_i 1_{g_j^{-1}})$. Consequentemente, $\sum_{i=1}^{m} x'_i \beta_{\overline{g}}(y'_i e_{g^{-1}}) = \delta_{e,g} e_g$.

Desta forma, T é uma extensão $\overline{\beta}$-Galois de R^{β}. ■

Lema 1.3.2. *Suponha que R é uma extensão β-Galois de R^{β} e seja A uma R^{β}-álgebra comutativa. Seja $\gamma = (\{A \otimes_{R^{\beta}} E_g\}_{g \in G}, \{\gamma_g\}_{g \in G})$ uma ação de G sobre $A \otimes_{R^{\beta}} R$ induzida por β via $\gamma_g((a \otimes_{R^{\beta}} r)(1_A \otimes_{R^{\beta}} 1_{g^{-1}})) = \gamma_g((a \otimes_{R^{\beta}} r1_{g^{-1}})) = a \otimes_{R^{\beta}} \beta_g(r1_{g^{-1}})$ para $r \in R, g \in G, a \in A$. Então $A \otimes_{R^{\beta}} R$ é uma extensão γ-Galois de A.*

Demonstração: Pela Observação 1.2.8, segue que $R \simeq R^{\beta} \oplus ker(tr_{\beta})$. Logo $A \otimes_{R^{\beta}} R \simeq (A \otimes_{R^{\beta}} R^{\beta}) \oplus (A \otimes_{R^{\beta}} ker(tr_{\beta}))$. Assim, vamos identificar A com sua imagem isomórfica $A \otimes_{R^{\beta}} R^{\beta}$.

Observe que $\bigoplus_{e \in G_0} (A \otimes_{R^{\beta}} E_e) = A \otimes_{R^{\beta}} (\bigoplus_{e \in G_0} E_e) = A \otimes_{R^{\beta}} R$.

Agora se $x_i, y_i \in R$, $1 \leq i \leq m$, são tais que $\sum_{1 \leq i \leq m} x_i \beta_g(y_i 1_{g^{-1}}) = \delta_{e,g} 1_e$ para todo $e \in G_0$ e $g \in G$, então claramente $1 \otimes_{R^{\beta}} x_i$ e $1 \otimes_{R^{\beta}} y_i$ satisfazem a mesma condição em $A \otimes_{R^{\beta}} R$, isto é, $\sum_{1 \leq i \leq m} (1_A \otimes_{R^{\beta}} x_i) \gamma_g(1_A \otimes_{R^{\beta}} y_i 1_{g^{-1}}) = 1_A \otimes_{R^{\beta}} \delta_{e,g} 1_e$ para todo $e \in G_0$ e $g \in G$. Sendo assim, para concluir que $A \otimes_{R^{\beta}} R$ é uma extensão γ-Galois de A, resta mostrar que $(A \otimes_{R^{\beta}} R)^{\gamma} = A$.

($\subseteq$) Seja $u = \sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i \in (A \otimes_{R^\beta} R)^\gamma$ e $c \in R$ tal que $tr_\beta(c) = 1_R$. Então:

$$u = u(Id_A \otimes_{R^\beta} tr_\beta)(1_A \otimes_{R^\beta} c) = (\sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i)(1_A \otimes_{R^\beta} tr_\beta(c)) = \sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i tr_\beta(c) =$$

$$\sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i \sum_{g\in G} \beta_g(c1_{g^{-1}}) = \sum_{i=1}^{m} a_i \otimes_{R^\beta} \sum_{g\in G} \beta_g(r_i 1_{g^{-1}})\beta_g(c1_{g^{-1}}) =$$

$$\sum_{i=1}^{m} a_i \otimes_{R^\beta} \sum_{g\in G} \beta_g(r_i c 1_{g^{-1}}) = \sum_{i=1}^{m} a_i \otimes_{R^\beta} tr_\beta(r_i c) \in A \otimes_{R^\beta} R^\beta = A.$$

($\supseteq$) Obviamente, $A = A \otimes_{R^\beta} R^\beta \subseteq (A \otimes_{R^\beta} R)^\gamma$, pois se $\sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i \in A \otimes_{R^\beta} R^\beta$, temos que $\gamma_g(\sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i 1_{g^{-1}}) = \sum_{i=1}^{m} a_i \otimes_{R^\beta} \beta_g(r_i 1_{g^{-1}}) = \sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i 1_g = (\sum_{i=1}^{m} a_i \otimes_{R^\beta} r_i)(1_A \otimes_{R^\beta} 1_g)$. ■

Seja $E = \{f : G \longrightarrow R \mid f$ é função e $f(g) \in E_g$ para todo $g \in G\}$. Note que E é uma R^β-álgebra com adição e multiplicação pontuais.

Lema 1.3.3. *Suponha que R é uma extensão β-Galois de R^β. Então existe uma ação β' de G sobre a álgebra E e E é uma extensão β'-Galois de R.*

Demonstração: Pelo Lema 1.3.2, $R \otimes_{R^\beta} R$ é uma extensão γ-Galois de R com grupóide de Galois G, onde $\gamma_g((s \otimes_{R^\beta} r1_g)) = s \otimes_{R^\beta} \beta_g(r1_{g^{-1}})$, para $s, r \in R$. Mas temos que $E \simeq \prod_{g\in G} E_g$ como R^β-álgebras, via:

$$\begin{array}{rccc} \phi : & E & \longrightarrow & \prod_{g\in G} E_g \\ & f & \longmapsto & (f(g))_{g\in G} \end{array}$$

e inversa dada por:

$$\begin{array}{rccc} \phi^{-1} : & \prod_{g\in G} E_g & \longrightarrow & E \\ & (a_g)_{g\in G} & \longmapsto & f : G \longrightarrow R, \quad f(g) = a_g, \forall g \in G. \end{array}$$

Pelo Teorema 1.2.3, item (iv), a aplicação

$$\begin{array}{rcl} \psi \ : \ R \otimes_{R^\beta} R & \longrightarrow & \prod_{g \in G} E_g \\ x \otimes_{R^\beta} y & \longmapsto & (x\beta_g(y1_{g^{-1}}))_{g \in G} \end{array}$$

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

$$\begin{array}{rcl} \eta \ : \ R \otimes_{R^\beta} R & \longrightarrow & E \\ x \otimes_{R^\beta} y & \longmapsto & \eta(x \otimes_{R^\beta} y) : G \longrightarrow R, \quad \textit{onde} \quad \eta(x \otimes_{R^\beta} y)(g) = x\beta_g(y1_{g^{-1}}) \end{array}$$

é um isomorfismo de R^β-álgebras.

Este isomorfismo induz uma ação $\beta' = (\{E'_g\}_{g \in G}, \{\beta'_g\}_{g \in G})$ de G sobre $E = \eta(R \otimes_{R^\beta} R)$ dada por:

$$\begin{array}{rcl} \beta'_g(\eta(s \otimes_{R^\beta} r)\eta(1_S \otimes_{R^\beta} 1_{g^{-1}}))(l) & = & \beta'_g(\eta(s \otimes_{R^\beta} r1_{g^{-1}}))(l) \\ & = & \eta(\gamma_g(s \otimes_{R^\beta} r1_{g^{-1}}))(l) \\ & = & \eta(s \otimes_{R^\beta} \beta_g(r1_{g^{-1}}))(l) \\ & = & s\beta_l(\beta_g(r1_{g^{-1}})1_{l^{-1}}), \end{array}$$

para todo $l \in G$, onde os ideais são dados por $E'_g = \eta(R \otimes_{R^\beta} E_g)$. De fato, esta aplicação está bem definida, visto que $\beta'_g(\eta(s \otimes_{R^\beta} r1_{g^{-1}}))(l) = s\beta_l(\beta_g(r1_{g^{-1}})1_{l^{-1}}) \in R\beta_l(E_g1_{l^{-1}}) = \eta(R \otimes_{R^\beta} E_g)(l)$, para todo $l \in G$, e portanto $\beta'_g(\eta(s \otimes_{R^\beta} r1_{g^{-1}})) \in \eta(R \otimes_{R^\beta} E_g) = E'_g$. Observe que $E = \eta(R \otimes_{R^\beta} R) = \eta(R \otimes_{R^\beta} \bigoplus_{e \in G_0} E_e) = \bigoplus_{e \in G_0} \eta(R \otimes_{R^\beta} E_e) = \bigoplus_{e \in G_0} E'_e$. Desta forma, E é um extensão β'-Galois de R. ■

Lema 1.3.4. *Suponha que R é uma extensão β-Galois de R^β e seja H um subgrupóide de G. Então $f \in E^{\beta'_H}$ se, e somente se, $f(lh) = f(l)$ para $h \in H$ e $l \in G$ tal que $d(l) = r(h)$.*

Demonstração: Considere $f \in E^{\beta'_H}$. Como foi visto no Lema 1.3.3, a aplicação $\eta : R \otimes_{R^\beta} R \longrightarrow E$, onde $\eta(x \otimes_{R^\beta} y) : G \longrightarrow R$ é dada por $\eta(x \otimes_{R^\beta} y)(g) = x\beta_g(y1_{g^{-1}})$, é um isomorfismo de R^β-álgebras. Logo existe $s \otimes_{R^\beta} r \in R \otimes_{R^\beta} R$ tal que $f = \eta(s \otimes_{R^\beta} r)$. Assim,

$$\begin{aligned}
\eta(s \otimes_{R^\beta} r) \in E^{\beta'_H} &\Leftrightarrow \beta'_h(\eta(s \otimes_{R^\beta} r1_{h^{-1}})) = \eta(s \otimes_{R^\beta} r1_h) \quad \forall h \in H \\
&\Leftrightarrow \eta(s \otimes_{R^\beta} \beta_h(r1_{h-1})) = \eta(s \otimes_{R^\beta} r1_h) \quad \forall h \in H \\
&\Leftrightarrow \eta(s \otimes_{R^\beta} \beta_h(r1_{h^{-1}}))(l) = \eta(s \otimes_{R^\beta} r1_h)(l) \quad \forall h \in H, l \in G \\
&\Leftrightarrow s\beta_l(\beta_h(r1_{h^{-1}})1_{l^{-1}}) = s\beta_l(r1_{l^{-1}}) \quad \forall h \in H, l \in G \\
&\Leftrightarrow s\beta_{lh}(r1_{h^{-1}l^{-1}}) = s\beta_l(r1_{l^{-1}}) \quad \forall h \in H, l \in G \quad tal \quad que \\
& d(l) = r(h) \\
&\Leftrightarrow \eta(s \otimes_{R^\beta} r)(lh) = \eta(s \otimes_{R^\beta} r)(l) \quad \forall h \in H, l \in G \quad tal \quad que \\
& d(l) = r(h) \\
&\Leftrightarrow f(lh) = f(l) \quad \forall h \in H, l \in G \quad tal \quad que \quad d(l) = r(h).
\end{aligned}$$

■

Teorema 1.3.5. *Suponha que R é uma extensão β-Galois de R^β e seja T uma R^β-subálgebra separável e β-forte de R. Então $R^{\beta_H} = T$ para $H = H_T$, onde β_H é a ação de H sobre R definida no Teorema 1.3.1.*

Demonstração: ($\supseteq$) Claramente $R^{\beta_H} \supseteq T$, pois $R^{\beta_H} = \{r \in R \mid \beta_h(r1_{h^{-1}}) = r1_h \text{ para todo } h \in H\}$ e $H = H_T = \{g \in G \mid \beta_g(t1_{g^{-1}}) = t1_g \text{ para todo } t \in T\}$, logo todo elemento de T fica fixo por β_H.
($\subseteq$) Vamos mostrar que $R^{\beta_H} \subseteq T$.

Pelo Lema 1.3.3, $E = \{f : G \longrightarrow R \mid f \text{ é função e } f(g) \in E_g \text{ para todo } g \in G\}$ é um extensão β'-Galois de R, onde a ação β' de G sobre E é dada por

$$\begin{aligned}
\beta'_g(\eta(s \otimes_{R^\beta} r1_{g^{-1}}))(l) = \eta(\gamma_g(s \otimes_{R^\beta} r1_{g^{-1}}))(l) &= \eta(s \otimes_{R^\beta} \beta_g(r1_{g^{-1}}))(l) \\
&= s\beta_l(\beta_g(r1_{g^{-1}})1_{l^{-1}}),
\end{aligned}$$

para todo $s, r \in R$, $g, l \in G$.

Mais ainda, como R é R^β-projetivo (pelo Teorema 1.2.3, item (ii)), então R é R^β-plano, e a sequência exata

$$0 \to T \hookrightarrow R$$

permanece exata quando tensorizada por R, ou seja,

$$0 \to R \otimes_{R^\beta} T \hookrightarrow R \otimes_{R^\beta} R$$

é exata. Logo podemos identificar $R \otimes_{R^\beta} T$ com sua imagem em $R \otimes_{R^\beta} R$.

Vamos mostrar que $E^{\beta'_H} \subseteq \eta(R \otimes T)$.

Considere então a relação de equivalência definida no Lema 1.1.24 por:

$$a \equiv_H b \Leftrightarrow \exists b^{-1}a \quad e \quad b^{-1}a \in H.$$

Note que é possível definir esta relação, pois $G_0 \subseteq H$. Seja $\{g_i\}_{1 \leq i \leq n}$ um sistema de representantes das classes de equivalência dessa relação. Seja $f_i : E \longrightarrow R$ o homomorfismo de R-álgebras definido por $f_i(v) = v(g_i)$. Vamos mostrar que $f_1, ..., f_n$ são fortemente distintos como homomorfismos de $\eta(R \otimes_{R^\beta} T)$ em R. Para ver isso, observe que se $i \neq j$, então a definição de H garante que as restrições de β_{g_i}, β_{g_j} em T não coincidem. De fato, se $\beta_{g_i}(t1_{g_i^{-1}}) = \beta_{g_j}(t1_{g_j^{-1}})$ para todo $t \in T$ com $r(g_i) = r(g_j)$, então $\beta_{g_j^{-1}}(\beta_{g_i}(t1_{g_i^{-1}})1_{g_j}) = t1_{g_j^{-1}}$ e desta forma

$$\beta_{g_j^{-1}g_i}(t1_{g_i^{-1}g_j}) = t1_{g_j^{-1}} = t1_{r(g_j^{-1})} = t1_{r(g_j^{-1}g_i)} = t1_{g_j^{-1}g_i},$$

para todo $t \in T$, o que implica que $g_j^{-1}g_i \in H$ e desta maneira $g_iH = g_jH$, uma contradição. Note que se $r(g_i) \neq r(g_j)$, então $g_iH \neq g_jH$ pela definição das classes laterais.

Se e é qualquer idempotente não nulo de R, então como T é β-forte, existe $t \in T$ tal que $\beta_{g_i}(t1_{g_i^{-1}})e \neq \beta_{g_j}(t1_{g_j^{-1}})e$, logo

$$f_i(\eta(1 \otimes_{R^\beta} t))e = (\eta(1 \otimes_{R^\beta} t)(g_i))e = \beta_{g_i}(t1_{g_i^{-1}})e \neq \beta_{g_j}(t1_{g_j^{-1}})e = f_j(\eta(1 \otimes_{R^\beta} t))e.$$

Assim $f_1, ..., f_n$ são, de fato, fortemente distintos.

Como T é R^β-separável, temos que $\eta(R \otimes_{R^\beta} T)$ é R-separável. De fato, se $e = \sum_{i=1}^{n} a_i \otimes_{R^\beta} b_i \in T \otimes_{R^\beta} T$ é o idempotente de separabilidade de T, então $\sum_{i=1}^{n} \eta(1_R \otimes_{R^\beta}$

$a_i) \otimes_R \eta(1_R \otimes_{R^\beta} b_i) \in \eta(R \otimes_{R^\beta} T) \otimes_R \eta(R \otimes_{R^\beta} T)$ é o idempotente de separabilidade de $\eta(R \otimes_{R^\beta} T)$.

Aplicando o Lema 1.2.7, obtemos idempotentes dois a dois ortogonais $w_1, ..., w_n$ em $\eta(R \otimes_{R^\beta} T)$ com $f_i(x)w_i = xw_i$ para todo $x \in \eta(R \otimes_{R^\beta} T)$ e $w_j(g_i) = f_i(w_j) = \delta_{ij}$ para $i, j \leq n$.

Vamos verificar que $w_1, ..., w_n$ geram $E^{\beta'_H}$ sobre R.

Primeiro mostraremos que $\{w_i\}_{1 \leq i \leq n} \subseteq E^{\beta'_H}$. Como $w_i \in \eta(R \otimes_{R^\beta} T)$, existem $u_{ij} \in R$ e $t_{ij} \in T$ tais que $w_i = \eta(\sum_j u_{ij} \otimes_{R^\beta} t_{ij})$, para $1 \leq i \leq n$. Pelo Lema 1.3.4, é suficiente mostrar que $w_i(lh) = w_i(l)$ para $h \in H$ e $l \in G$ tal que $d(l) = r(h)$. Desta forma,

$$w_i(lh) = \eta(\sum_j u_{ij} \otimes_{R^\beta} t_{ij})(lh) = \sum_j u_{ij}\beta_{lh}(t_{ij}1_{h^{-1}l^{-1}}) =$$
$$\sum_j u_{ij}\beta_l(\beta_h(t_{ij}1_{h^{-1}})1_{l^{-1}}) = \sum_j u_{ij}\beta_l(t_{ij}1_h1_{l^{-1}}) = \eta(\sum_j u_{ij} \otimes_{R^\beta} t_{ij})(l) = w_i(l),$$

e portanto $w_i \in E^{\beta'_H}$ para todo $1 \leq i \leq n$.

Agora seja $f \in E^{\beta'_H}$. Então existem $s_j, r_j \in R$ tais que $f = \eta(\sum_j s_j \otimes_{R^\beta} r_j)$. Assim,

$$\begin{aligned} f(g_i) &= \eta(\sum_j s_j \otimes_{R^\beta} r_j)(g_i) = \sum_j s_j\beta_{g_i}(r_j1_{g_i^{-1}}) \\ &= \sum_j s_j\beta_{g_i}(r_j1_{g_i^{-1}})w_i(g_i) = \sum_{j,k} s_j\beta_{g_k}(r_j1_{g_k^{-1}})w_k(g_i). \end{aligned}$$

Como $f \in E^{\beta'_H}$, é suficiente aplicá-la apenas nos g_i's, pois $f(g_i) = f(g_ih)$ para toda $f \in E^{\beta'_H}$ e para todo $h \in H$ tal que $d(g_i) = r(h)$, pelo Lema 1.3.4. Desta forma, concluímos que $w_1, ..., w_n$ geram $E^{\beta'_H}$ sobre R.

Temos, então, que $E^{\beta'_H} \subseteq \eta(R \otimes_{R^\beta} T)$. Aplicando η^{-1}, temos que $\eta^{-1}(E^{\beta'_H}) \subseteq R \otimes_{R^\beta} T$.

Afirmação: $E^{\beta'_H} = \eta((R \otimes_{R^\beta} R)^{\gamma_H})$.

Esta afirmação segue direto do fato que $\beta'_g \circ \eta = \eta \circ \gamma_g$, para todo $g \in G$.

Então, pela afirmação, $(R \otimes_{R^\beta} R)^{\gamma_H} = \eta^{-1}(E^{\beta'_H}) \subseteq R \otimes_{R^\beta} T$. Desta maneira,

$$R \otimes_{R^\beta} R^{\beta_H} \subseteq (R \otimes_{R^\beta} R)^{\gamma_H} \subseteq R \otimes_{R^\beta} T.$$

Aplicando $tr_\beta \otimes_{R^\beta} Id_R$ e usando que o traço é sobrejetivo, temos:

$$tr_\beta(R) \otimes_{R^\beta} R^{\beta_H} \subseteq tr_\beta(R) \otimes_{R^\beta} T,$$

o que implica que

$$R^\beta \otimes_{R^\beta} R^{\beta_H} \subseteq R^\beta \otimes_{R^\beta} T.$$

Logo segue que $R^{\beta_H} \subseteq T$, como queríamos demonstrar. ■

Os Teoremas 1.3.1 e 1.3.5 nos fornecem a seguinte generalização do Teorema Fundamental da Teoria de Galois:

Teorema 1.3.6. ***Teorema de Correspondência de Galois***. *Suponha que R é uma extensão β-Galois de R^β. Então existe uma correspondência um-a-um entre os subgrupóides amplos de G e as subálgebras separáveis T de R que são β-fortes. Se T é uma R^β-subálgebra β-forte de R, então o correspondente subgrupóide é H_T. Mais ainda, se H é um subgrupóide normal de G e $\equiv_H$ é a congruência definida no Lema 1.1.24, então $\frac{G}{H}$ age sobre R^{β_H} via uma ação $\overline{\beta}$ e R^{β_H} é um extensão $\overline{\beta}$-Galois de R^β.*

Este teorema nos diz que a aplicação $\theta : H \mapsto R^{\beta_H}$ dos subgrupóides amplos de G nas subálgebras separáveis de R que são β-fortes é bijetiva. Podemos ilustrar este fato no seguinte diagrama:

$$
\begin{tikzcd}
 & & R \arrow[dll, dash] \arrow[d, dash] \arrow[dr, dash] & \\
G_0 \arrow[d, dash] \arrow[dr, dash] & & R^{\beta_H} \arrow[dr, dash] & T \arrow[d, dash] \arrow[dll, dashed] \\
H \arrow[dr, dash] \arrow[urr, dashed] & H_T \arrow[d, dash] & & R^{\beta} \arrow[dll, dash] \\
 & G & &
\end{tikzcd}
$$

Capítulo 2

Correspondência de Galois-Grothendieck

O Lema de Dedekind diz que, dados um corpo L extensão de um corpo K e A uma K-álgebra, o conjunto $Alg_K(A, L)$ de todos os homomorfismos de K-álgebras de A em L é um subconjunto linearmente independente do L-espaço vetorial $Hom_K(A, L)$. Em [14], M. Ferrero e A. Paques, entre outros resultados da teoria de Galois para anéis comutativos, simplificaram a demonstração do Teorema de Correspondência combinando uma versão do Lema de Dedekind para extensões de anéis com resultados básicos de G-conjuntos, no caso em que G é um grupo. Mais tarde, baseado nos resultados desta publicação e motivado pelo trabalho de A. Dress em [12], A. Paques mostrou em [21] a correspondência de Galois-Grothendieck no contexto de anéis comutativos, a qual associa bijetivamente G-conjuntos e K-álgebras R-decomponíveis, onde K e R são anéis comutativos, R é uma extensão de Galois de K e G é um subgrupo finito de K-automorfismos de R. Tendo em vista estas informações, o objetivo deste capítulo é desenvolver uma generalização do Lema de Dedekind e, dado um grupóide G, combiná-la com resultados de G-conjuntos, para então generalizar a correspondência de Galois-Grothendiek para o caso de ação de grupóides e mostrar o Teorema de Correspondência de Galois como um caso particular do anterior.

Neste capítulo, todos os anéis (ou álgebras) são assumidos comutativos.

2.1 Preliminares

Antes de introduzirmos a noção de G-conjuntos para um grupóide G, trabalharemos nesta primeira seção com alguns resultados que serão utilizados no decorrer do capítulo.

Seja R um anel.

Lema 2.1.1. [[14], Lemma 1.1] *Suponha que $A \subset B$ são R-álgebras finitamente geradas e projetivas como R-módulos e que A é separável sobre R. Se $rank_{R_\mathfrak{p}} A_\mathfrak{p} = rank_{R_\mathfrak{p}} B_\mathfrak{p}$, para todo ideal primo $\mathfrak{p}$ de R, então $A = B$.*

Definição 2.1.2. *Dizemos que uma R-álgebra A é fortemente separável sobre R se é separável sobre R e, em acréscimo, é finitamente gerada e projetiva como R-módulo.*

O próximo resultado generaliza a versão do Lema de Dedekind dada em [14].

Proposição 2.1.3. *Seja K um anel. Suponha que T e R são K-álgebras com T separável sobre K e V é um conjunto não vazio de homomorfismos de K-álgebras $v : T \longrightarrow E_v$, onde $E_v = R1_v$ e $\{1_v\}_{v \in V}$ são idempotentes centrais em R. Então as seguintes condições são equivalentes:*
(i) Para cada $v \in V$, os elementos de $V_v = \{u \in V \mid 1_u = 1_v\}$ são dois a dois

fortemente distintos.

(ii) Para todo $v \in V$ existem $x_{iv} \in E_v$, $y_{iv} \in T$, $1 \leq i \leq m_v$, tais que $\sum_{i=1}^{m_v} x_{iv}u(y_{iv}) = \delta_{u,v}1_u$, para todo $u \in V_v$.

(iii) Para cada $u \in V$, V_u é linearmente independente sobre E_u em $Hom_K(T, E_u)$.

Demonstração: $(i) \Rightarrow (ii)$ Como T é separável sobre K, $E_v \otimes_K T$ é separável sobre E_v. De fato, se $e = \sum_{i=1}^{n} a_i \otimes_K b_i \in T \otimes_K T$ é o idempotente de separabilidade de T sobre K, então $\sum_{i=1}^{n}(1_v \otimes_K a_i) \otimes_{E_v} (1_v \otimes_K b_i) \in (E_v \otimes_K T) \otimes_{E_v} (E_v \otimes_K T)$ é o idempotente de separabilidade de $E_v \otimes_K T$ sobre E_v.

Mais ainda, as aplicações

$$\begin{array}{rrcl} f_v : & E_v \otimes_K T & \longrightarrow & E_v \\ & x \otimes_K y & \longmapsto & xv(y) \end{array}$$

são duas a duas fortemente distintas sempre que os contradomínios (consequentemente, os domínios) coincidirem, pois os elementos de V_v são fortemente distintos. De fato, para $l, u \in V_v$, dado um idempotente não nulo $e \in E_v$, existe $t \in T$ tal que $el(t) \neq eu(t)$. Logo

$$ef_l(1_v \otimes_K t) = el(t) \neq eu(t) = ef_u(1_v \otimes_K t).$$

Assim, pelo Lema 1.2.7, existe $e_v = \sum_{i=1}^{m_v} x_{iv} \otimes_K y_{iv} \in E_v \otimes_K T$ tal que $f_u(e_v) = \delta_{u,v}1_u$, para todo $u \in V_v$.

$(ii) \Rightarrow (iii)$ Considere V'_u um subconjunto finito de V_u e $\sum_{l \in V'_u} r_l l = 0$ em $Hom_K(T, E_u)$, onde $r_l \in E_l = E_u$. Para $v \in V'_u$, temos

$$r_v = \sum_{l \in V'_u} \delta_{l,v} 1_l r_l = \sum_{l \in V'_u} (\sum_{i=1}^{m_v} x_{iv} l(y_{iv})) r_l = \sum_{i=1}^{m_v} x_{iv} (\sum_{l \in V'_u} l(y_{iv}) r_l) = 0,$$

mostrando que V_u é livre sobre E_u.

$(iii) \Rightarrow (i)$ Seja $v \in V$. Para $l, u \in V_v$, dado um idempotente $e \in E_v$, suponha que $el(x) = eu(x)$, para todo $x \in T$. Logo $e(l-u)(x) = 0$, para todo $x \in T$, e desta maneira $e(l-u)=0$. Como V_v é linearmente independente sobre E_v, segue que $e=0$. ∎

Corolário 2.1.4. *Assuma que T é uma extensão fortemente separável de K, R é uma K-álgebra e V é um conjunto não vazio de homomorfismos de K-álgebras $v : T \longrightarrow E_v$, onde $E_v = R1_v$ e $\{1_v\}_{v\in V}$ são idempotentes centrais em R. Suponha que para cada $v \in V$, os elementos de $V_v = \{u \in V|\ 1_u = 1_v\}$ são dois a dois fortemente distintos. Então para cada $v \in V$, $\#V_v \leq rank_{K_\mathfrak{p}} T_\mathfrak{p}$, para todo ideal primo $\mathfrak{p}$ de K.*

Demonstração: Como, para cada $v \in V$, os elementos de $V_v = \{u \in V|\ 1_u = 1_v\}$ são dois a dois fortemente distintos, segue pelo Lema 2.1.3 que V_v é linearmente independente sobre E_v em $Hom_K(T, E_v)$. Então, via localização, $(V_v)_\mathfrak{p}$ é linearmente independente sobre $(E_v)_\mathfrak{p}$ em $Hom_{K_\mathfrak{p}}(T_\mathfrak{p}, (E_v)_\mathfrak{p})$, para todo ideal primo $\mathfrak{p}$ de K.

Por outro lado, como T é finitamente gerado e projetivo sobre K, por [20], Theorem IV.25, $T_\mathfrak{p}$ é $K_\mathfrak{p}$-livre de dimensão finita, para todo ideal primo $\mathfrak{p}$ de K. Logo podemos assumir $T_\mathfrak{p} \simeq (K_\mathfrak{p})^s$, onde $s = rank_{K_\mathfrak{p}} T_\mathfrak{p}$. Desta forma,

$$Hom_{K_\mathfrak{p}}(T_\mathfrak{p}, (E_v)_\mathfrak{p}) \simeq Hom_{K_\mathfrak{p}}(K_\mathfrak{p}^s, (E_v)_\mathfrak{p}) \simeq Hom_{K_\mathfrak{p}}(K_\mathfrak{p}, (E_v)_\mathfrak{p})^s \simeq ((E_v)_\mathfrak{p})^s,$$

como $(E_v)_\mathfrak{p}$-módulos.

Então temos que $(V_v)_\mathfrak{p}$ é linearmente independente sobre $(E_v)_\mathfrak{p}$ e, adicionalmente, $(V_v)_\mathfrak{p} \subseteq Hom_{K_\mathfrak{p}}(T_\mathfrak{p}, (E_v)_\mathfrak{p})$, portanto segue que $\#V_v = \#(V_v)_\mathfrak{p} \leq s = rank_{K_\mathfrak{p}} T_\mathfrak{p}$. ∎

Lema 2.1.5. *Sejam T e R K-álgebras e V um conjunto não vazio de homomorfismos de K-álgebras $v : T \longrightarrow E_v$, onde $E_v = R1_v$ e $\{1_v\}_{v\in V}$ são idempotentes centrais em R. Suponha que para cada $v \in V$, E_v é uma K-álgebra fielmente projetiva. Então as seguintes condições são equivalentes:*

(i) T é uma extensão fortemente separável de K, para cada $v \in V$ os elementos de

$V_v = \{u \in V|\ 1_u = 1_v\}$ são dois a dois fortemente distintos e $rank_K T = \#V_v$.

(ii) T é fielmente projetivo sobre K, para todo $v \in V$ existe $x_{iv} \in E_v$, $y_{iv} \in T$, $1 \leq i \leq m_v$, tais que $\sum_{i=1}^{m_v} x_{iv} u(y_{iv}) = \delta_{u,v} 1_u$, para todo $u \in V_v$, e $rank_K T = \#V_v$.

(iii) Para cada $v \in V$, a aplicação $\varphi_v : E_v \otimes_K T \longrightarrow \prod_{u \in V_v} E_u$ dada por $\varphi_v(r \otimes_K t) = (ru(t))_{u \in V_v}$, $r \in E_v, t \in T$, é um isomorfismo de R-álgebras.

Demonstração: $(i) \Rightarrow (ii)$ Direto da Proposição 2.1.3.

$(ii) \Rightarrow (iii)$ Seja $v \in V$. A aplicação φ_v é claramente um homomorfismo de R-álgebras. Vamos mostrar que é um epimorfismo.

Para $r = (r_u)_{u \in V_v} \in \prod_{u \in V_v} E_u$, tome $z = \sum_{u \in V_v} \sum_{i=1}^{m_u} r_u x_{iu} \otimes_K y_{iu} \in E_v \otimes_K T$. Então:

$$\begin{aligned} \varphi_v(z) &= (\sum_{u \in V_v} \sum_{i=1}^{m_u} r_u x_{iu} l(y_{iu}))_{l \in V_v} = (\sum_{u \in V_v} r_u \sum_{i=1}^{m_u} x_{iu} l(y_{iu}))_{l \in V_v} \\ &= (\sum_{u \in V_v} r_u \delta_{l,u} 1_l)_{l \in V_v} = (r_l)_{l \in V_v} = r. \end{aligned}$$

Observe que

$$\prod_{u \in V_v} E_u = E_v^n,$$

onde $n = \#V_v$. Como φ_v é R-epimorfismo e $rank_{E_v}(E_v)^n = n = \#V_v = rank_K T = rank_{E_v} E_v \otimes_K T$, segue por [17], Corollaire 2.4, que φ_v é um isomorfismo de R-álgebras.

$(iii) \Rightarrow (i)$ Como para cada $v \in V$, φ_v é um isomorfismo, temos que

$$rank_K T = rank_{E_v} E_v \otimes_K T = rank_{E_v} \prod_{u \in V_v} E_u = \#V_v.$$

(Observe que este raciocínio vale para todo $v \in V$, logo pela unicidade do *rank* temos que $\#V_v = \#V_u$, para todo $u, v \in V$.)

Agora vamos verificar que T é uma extensão fortemente separável de K. Como para cada $v \in V$, E_v é um K-módulo finitamente gerado e projetivo e T é uma K-álgebra, segue que $E_v \otimes_K T$ é um T-módulo finitamente gerado e projetivo. Então, por [17], Lemma III.1.9, T é um somando direto de $E_v \otimes_K T \simeq \prod_{u\in V_v} E_u = (E_v)^n$, onde $n = \#V_v$, logo T é um E_v-módulo finitamente gerado e projetivo. Mais ainda, temos que para cada $v \in V$, E_v é E_v-separável, assim, por [17], Proposition III.1.7 (c), $(E_v)^n = \prod_{u\in V_v} E_u$ é E_v-separável. Desta forma, novamente por [17], Proposition III.2.2, T é separável sobre K.

Resta mostrar que os elementos de V_v são dois a dois fortemente distintos. Dado $u \in V_v$, considere $s = (\delta_{l,u}1_l)_{l\in V_v} \in \prod_{u\in V_v} E_u$. Então existe $z = \sum_{i=1}^{m_u} r_{iu} \otimes_K t_{iu} \in E_v \otimes_K T$ tal que $\varphi_v(z) = s$, pois φ_v é isomorfismo. Isto implica que $(\sum_{i=1}^{m_u} r_{iu} l(t_{iu}))_{l\in V_v} = (\delta_{l,u}1_l)_{l\in V_v}$, logo $\sum_{i=1}^{m_u} r_{iu} l(t_{iu}) = \delta_{l,u}1_l$ para cada $l \in V_v$. Consequentemente, pela Proposição 2.1.3, os elementos de V_v são dois a dois fortemente distintos. ■

2.2 G-conjuntos

Definição 2.2.1. *Sejam G um grupóide e X um conjunto. Uma ação γ de G sobre X é uma coleção de subconjuntos $X_g \subseteq X$ ($g \in G$) e bijeções $\gamma_g : X_{g^{-1}} \longrightarrow X_g$ com $X_g = X_{r(g)}$ tais que:*

(i) $\gamma_e = Id_{X_e}$ para todo $e \in G_0$;

(ii) $\gamma_g \circ \gamma_h(x) = \gamma_{gh}(x)$ para todo $(g, h) \in G^2$ e $x \in X_{h^{-1}} = X_{(gh)^{-1}}$.

Neste caso, dizemos que X é um G-conjunto.

Exemplo 2.2.2. *Um grupóide G é um G-conjunto. De fato, para $X = G$, defina $X_g = r(g)G = \{r(g)l \mid l \in G \text{ e } r(l) = r(g)\} = X_{r(g)}$. Desta forma, $X_{g^{-1}} = \{d(g)l \mid l \in G \text{ e } r(l) = d(g)\} = X_{d(g)}$, para todo $g \in G$. Tome $\gamma_g : X_{g^{-1}} \longrightarrow X_g$ definida por*

$$\gamma_g(d(g)l) = gd(g)l = gl.$$

Observe que $gl = r(g)gl \in X_g$, logo γ_g está bem definida. Note que $\gamma_g \circ \gamma_{g^{-1}} = Id_{X_g}$

e $\gamma_{g^{-1}} \circ \gamma_g = Id_{X_{g^{-1}}}$. Portanto γ_g é uma bijeção e claramente satisfaz as condições (i) e (ii) da Definição 2.2.1.

Exemplo 2.2.3. *Considere G um grupóide finito e H um subgrupóide amplo de G. Tome a relação de equivalência $\equiv_H$ definida no Lema 1.1.24. Então o conjunto das classes de equivalência $\frac{G}{H} = \{gH \mid g \in G\}$ é um G-conjunto. Com efeito, para $X = \frac{G}{H}$, defina $X_g = \{lH \in \frac{G}{H} \mid r(l) = r(g)\} = X_{r(g)}$. Desta maneira, $X_{g^{-1}} = \{lH \in \frac{G}{H} \mid r(l) = d(g)\} = X_{d(g)}$. Defina $\gamma_g : X_{g^{-1}} \longrightarrow X_g$ por*

$$\gamma_g(lH) = glH.$$

Observe que $r(gl) = r(g)$, logo $glH \in X_g$, portanto γ_g está bem definida. Assim como no exemplo anterior, o leitor pode verificar facilmente que $\gamma_g \circ \gamma_{g^{-1}} = Id_{X_g}$ e $\gamma_{g^{-1}} \circ \gamma_g = Id_{X_{g^{-1}}}$, portanto γ_g é uma bijeção, e claramente satisfaz as condições (i) e (ii) da Definição 2.2.1.

Mais ainda, $X_g \cap X_h = \emptyset$ se $r(g) \neq r(h)$ e $\frac{G}{H} = \dot{\bigcup\limits_{e \in G_0}} X_e$.

Exemplo 2.2.4. *Dado G um grupóide finito, considere X um G-conjunto via a ação $\gamma = (\{X_g\}_{g \in G}, \{\gamma_g\}_{g \in G})$, onde $X = \dot{\bigcup\limits_{e \in G_0}} X_e$. Suponha G agindo sobre uma K-álgebra R via $\beta = (\{E_g\}_{g \in G}, \{\beta_g\}_{g \in G})$, onde E_e é unitário para cada $e \in G_0$ e $R = \bigoplus\limits_{e \in G_0} E_e$. Tome $Map(X, R) = \{f : X \longrightarrow R \mid f$ é aplicação e $f(X_g) \subseteq E_g\}$. Vamos verificar que $Y = Map(X, R)$ é um G-conjunto.*

Considere $Y_g = Map(X, R)_g = \{f \in Map(X, R) \mid f(X_h) = 0, \forall h \neq g\} = Y_{r(g)}$ e tome $\alpha_g : Y_{g^{-1}} \longrightarrow Y_g$ definida por

$$\alpha_g(f1'_{g^{-1}})(x) = \begin{cases} \beta_g \circ f1'_{g^{-1}} \circ \gamma_{g^{-1}}(x), & se \quad x \in X_g \\ 0, & se \quad x \notin X_g, \end{cases}$$

onde $1'_g \in Y_g$ é definido por

$$1'_g(x) = \begin{cases} 1_g, & se \quad x \in X_g \\ 0, & se \quad x \notin X_g. \end{cases}$$

É direto ver que α_g está bem definida e que sua inversa é dada por $\alpha_{g^{-1}} : Y_g \longrightarrow Y_{g^{-1}}$, assim como também é imediato verificar que esta ação satisfaz as condições (i) e (ii) da Definição 2.2.1. Em particular, $A(X) = Map(X,R)^\alpha = \{f \in Map(X,R)| \alpha_g(f1'_{g^{-1}}) = f1'_g \ \forall g \in G\} \subseteq Map(X,R)$ é também um G-conjunto, via a mesma ação α.

Note que $Y = Map(X,R)$ (e portanto $A(X)$) possui uma estrutura de K-álgebra com adição e multiplicação pontuais e ação de K-módulo definida para cada $\lambda \in K$, $f \in Map(X,R)$, $g \in G$, por $(\lambda.f)(x) = \lambda f(x)$, para todo $x \in X$. A unidade neste caso é dada por $1_Y = 1_{A(X)} = \sum_{g \in G} 1'_g$.

Afirmação 1: *Para cada $g \in G$, Y_g é um ideal de Y.*

Sejam $l \in Y$ e $f \in Y_g$. Se $x \notin X_g$, $(l.f)(x) = l(x)f(x) = 0$, concluindo que $l.f \in Y_g$.

Afirmação 2: *$Y = \bigoplus_{g \in G} Y_g$.*

Seja $f \in Y$. Defina $f'_g : X \longrightarrow R$ por $f'_g(X_g) = f(X_g)$ e $f'_g(X_h) = 0$ para todo $h \neq g$. Observe que $f'_g \in Y_g$ para todo $g \in G$. Tome $x \in X$. Então existe $k \in G$ tal que $x \in X_k$. Desta maneira,

$$f(x) = f'_k(x) = \sum_{g \in G} f'_g(x).$$

Agora considere $f \in Y_g \cap (\sum_{h \neq g} Y_h)$. Se $x \notin X_g$, $f(x) = 0$ porque $f \in Y_g$. Se $x \in X_g$, $f(x) = 0$ porque $f \in \sum_{h \neq g} Y_h$. Desta forma temos que $f(x) = 0$ para todo $x \in X$, ou seja, $f = 0$, concluindo a Afirmação 2.

Mais ainda, $Map(X,R)$ (resp., $A(X)$) é um R-módulo (resp., R^β-módulo) via $r.f(x) = rf(x)$, para $r \in R$, $f \in Map(X,R)$ (resp., $A(X)$) e $x \in X$.

Para o restante deste capítulo, fixaremos que:

- K é um anel;

- G é um grupóide finito;

- R é uma K-álgebra;

- $\beta = (\{E_g\}_{g\in G}, \{\beta_g\}_{g\in G})$ é a ação de G sobre R tal que E_e é unitário para cada $e \in G_0$ e $R = \bigoplus_{e\in G_0} E_e$;

- X é um G-conjunto finito via $\gamma = (\{X_g\}_{g\in G}, \{\gamma_g\}_{g\in G})$ tal que $X = \dot{\bigcup_{e\in G_0}} X_e$.

Considere $A(X)$ como definido no Exemplo 2.2.4. Defina $E_x := E_g$ quando $x \in X_g$. Para $x \in X$, denote por ρ_x o homomorfismo de K-álgebras de $A(X)$ em E_x dado por $\rho_x(f) = f(x)$, para todo $f \in A(X)$, e denote por 1_x a unidade de E_x.

Lema 2.2.5. *Seja $V = \{\rho_x |\ x \in X\}$. Suponha que para cada $g \in G$, E_g é uma K-álgebra fielmente projetiva. Então as seguintes condições são equivalentes:*
(i) Para cada $y \in X$, os elementos de $V_y = \{\rho_x |\ 1_x = 1_y\}$ são dois a dois fortemente distintos, $rank_K T = \#V_y$ e $A(X)$ é uma extensão fortemente separável de K.
(ii) Para cada $y \in X$, a aplicação $\varphi_y : E_y \otimes_K A(X) \longrightarrow \prod_{x\in X_y} E_x$ dada por $\varphi_y(r \otimes_K f) = (rf(x))_{x\in X_y}$, para todo $r \in E_y$ e $f \in A(X)$, onde $X_y = \{x \in X |\ 1_x = 1_y\}$, é um isomorfismo de R-álgebras.

Demonstração: $(i) \Rightarrow (ii)$ Decorre do Lema 2.1.5.

$(ii) \Rightarrow (i)$ Mostrando que $\#V_y = \#X_y$ para todo $y \in X$, a demonstração sai como uma aplicação do Lema 2.1.5. Considere a aplicação $\omega_y : X_y \longrightarrow V_y$ dada por $\omega_y(x) = \rho_x$, para todo $x \in X_y$. Esta aplicação é claramente sobrejetiva, logo resta provar sua injetividade. De fato, se $\rho_x = \rho_w$ para $x, w \in X_y$, então $f(x) = f(w)$ para todo $f \in A(X)$. Seja $M_y = \{f : X_y \longrightarrow E_y |\ f \text{ é aplicação}\}$ e considere a aplicação

$$\begin{array}{rcl} \eta : M_y & \longrightarrow & \prod_{x\in X_y} E_x \\ f & \longmapsto & (f(x))_{x\in X_y}. \end{array}$$

Tome também a aplicação

$$\begin{array}{rccc} \eta' : & \prod\limits_{x \in X_y} E_x & \longrightarrow & M_y \\ & r = (r_x)_{x \in X_y} & \longmapsto & \eta'_r, \quad onde \quad \eta'_r(x) = r_x. \end{array}$$

É fácil ver que η e η' são homomorfismos de R-álgebras. Note que

$$\eta \circ \eta'(r) = (\eta'_r(x)) = (r_x)_{x \in X_y} = r \text{ e } \eta' \circ \eta(f) = \eta'((f(x))_{x \in X_y}) = f.$$

Portanto $\prod\limits_{x \in X_y} E_x \simeq M_y$ como R-álgebras, e por conseguinte $E_y \otimes_K A(X) \simeq \prod\limits_{x \in X_y} E_x \simeq M_y$. Tome $p \in M_y$. Então existem $r \in E_y$ e $f \in A(X)$ tais que $p = \eta' \circ \varphi(r \otimes_K f)$, logo

$$p(x) = \eta' \circ \varphi(r \otimes_K f)(x) = \eta'((rf(z))_{z \in X_y})(x) = rf(x) = rf(w) = p(w),$$

para todo $p \in M_y$. Assim, $x = w$. De fato, para visualizar esta igualdade, observe que se $x \neq w$, então podemos definir uma aplicação $p \in M_y$ tal que $p(x) = 1_x$ e $p(z) = 0$ para todo $z \neq x$. Isto implica que $p(x) \neq p(w)$, um absurdo. Desta forma, $x = w$ e ω_y é injetiva, concluindo o lema. ■

Para M um $R \star_\beta G$-módulo qualquer, a parte fixa de M pela ação do skew anel de grupóide $R \star_\beta G$ é definida por

$$M^G = \{m \in M | (1_g u_g)m = 1_g m, \quad \forall g \in G\}.$$

Já foi observado no Exemplo 2.2.4 que $Map(X, R)$ possui uma estrutura de R-módulo; todavia, $Map(X, R)$ possui também uma estrutura de $R \star_\beta G$-módulo à esquerda via

$$r_g u_g . f = r_g \alpha_g (f 1'_{g^{-1}}),$$

para $r_g \in R$ e $g \in G$. Desta maneira, para o caso particular $M = Map(X, R)$, temos

$$Map(X, R)^G = \{f \in Map(X, R) | (1_g u_g) f = 1_g f, \quad \forall g \in G\}$$

$$= \{f \in Map(X,R) | \alpha_g(f1'_{g^{-1}}) = f1'_g, \quad \forall g \in G\} = A(X).$$

Este fato será utilizado no próximo lema.

Lema 2.2.6. *Assuma que R é uma extensão β-Galois de R^β. Então para cada $y \in X$, a aplicação $\varphi_y : E_y \otimes_{R^\beta} A(X) \longrightarrow \prod_{x \in X_y} E_x$ dada por $\varphi_y(r \otimes_{R^\beta} f) = (rf(x))_{x \in X_y}$, $r \in E_y, f \in A(X)$, é um isomorfismo de R-álgebras.*

Demonstração: Pelo Teorema 1.2.3, se R é uma extensão β-Galois de R^β, então a aplicação $\mu : R \otimes_{R^\beta} Map(X,R)^G \longrightarrow Map(X,R)$ dada por $\mu(r \otimes f) = rf$ é um isomorfismo de R-álgebras. Como foi observado acima, $Map(X,R)^G = A(X)$, logo μ é um isomorfismo de $R \otimes_{R^\beta} A(X)$ em $Map(X,R)$. Note que $\mu : R \otimes_{R^\beta} A(X) \longrightarrow Map(X,R)$ induz um isomorfismo $\mu_y : 1_y.(R \otimes_{R^\beta} A(X)) \longrightarrow 1_y.Map(X,R)$ de R-álgebras.

Porém, observe que $1_y.Map(X,R) = \{f \in Map(X,R) |\ f(X_z) = 0$, para todo $z \in X - X_y\}$ e esta álgebra é naturalmente isomorfa a $M_y = \{f : X_y \longrightarrow E_y |\ f$ é aplicação$\}$ via

$$\begin{array}{rcl} \varepsilon_y : 1_y.Map(X,R) & \longrightarrow & M_y \\ f & \longmapsto & f|_{X_y}. \end{array}$$

De fato, é imediato verificar que ε_y é um homomorfismo de R-álgebras, assim como também é direto ver que sua inversa é dada por

$$\begin{array}{rcl} \varepsilon_y^{-1} : M_y & \longrightarrow & 1_y.Map(X,R) \\ f & \longmapsto & f' \quad \textit{onde} \quad f'(X_y) = f \quad \textit{e} \quad f'(X_z) = 0, \quad \forall z \in X - X_y. \end{array}$$

Desta maneira, temos que $E_y \otimes_{R^\beta} A(X) = 1_y.(R \otimes_{R^\beta} A(X)) \simeq M_y$ via $\varepsilon_y \circ \mu_y$. Mas $M_y \simeq \prod_{x \in X_y} E_x$ como R-álgebras via a aplicação η definida no Lema 2.2.5, onde $\eta(f) = (f(x))_{x \in X_y}$. Portanto a aplicação $\varphi_y = \eta \circ \varepsilon_y \circ \mu_y : E_y \otimes_{R^\beta} A(X) \longrightarrow \prod_{x \in X_y} E_x$ é um isomorfismo de R-álgebras. ■

Definição 2.2.7. *Sejam Y e W dois G-conjuntos via as ações $\varepsilon = \{\varepsilon_g : Y_{g^{-1}} \longrightarrow Y_g\}_{g \in G}$ e $\vartheta = \{\vartheta_g : W_{g^{-1}} \longrightarrow W_g\}_{g \in G}$, respectivamente. Dizemos que a aplicação*

$\rho : Y \longrightarrow W$ é um isomorfismo de G-conjuntos se satisfaz as seguintes afirmações:

(i) ρ é uma bijeção;

(ii) $\rho(Y_g) = W_g$ para todo $g \in G$;

(iii) $\rho(\varepsilon_g(y)) = \vartheta_g(\rho(y))$, para todo $y \in Y_{g^{-1}}$ e para todo $g \in G$.

2.3 Correspondência de Galois-Grothendieck

Para o que segue nesta seção, é pertinente neste instante elucidar um novo exemplo de G-conjunto.

Exemplo 2.3.1. *Com as mesmas notações anteriores, para cada $g \in G$, considere o subconjunto $V_g(X) = \{\rho_x : A(X) \longrightarrow E_g |\ x \in X_g$ e $\rho_x(f) = f(x), \forall f \in A(X)\} = V_{r(g)}(X)$ de $Alg_K(A(X), E_g)$. Então $V(X) = \dot{\bigcup\limits_{e \in G_0}} V_e(X)$ é um G-conjunto.*

De fato, tome $\sigma = \{\sigma_g : V_{g^{-1}}(X) \longrightarrow V_g(X)\}_{g \in G}$, onde $\sigma_g(\rho_x)(f) = \beta_g(f(x))$, para todo $x \in X_{g^{-1}}$. Observe que $f \in A(X)$, logo $\sigma_g(\rho_x)(f) = \beta_g(f(x)) = f(\gamma_g(x)) = \rho_{\gamma_g(x)}(f)$, portanto $\sigma_g(\rho_x) \in V_g(X)$, mostrando que a ação está bem definida. Além disso, note que

$$\sigma_g \circ \sigma_{g^{-1}}(\rho_x)(f) = \sigma_g(\rho_{\gamma_{g^{-1}}(x)})(f) = \beta_g(f(\gamma_{g^{-1}}(x))) = f(x) = \rho_x(f),$$

pois $f \in A(X)$. Assim, $\sigma_g \circ \sigma_{g^{-1}} = Id_{V_g(X)}$ e, similarmente, $\sigma_{g^{-1}} \circ \sigma_g = Id_{V_{g^{-1}}(X)}$. Logo σ_g é uma bijeção, e é imediato verificar que satisfaz as condições (i) e (ii) da Definição 2.2.1.

Lema 2.3.2. *Suponha que R é uma extensão β-Galois de R^β e tome $V(X)$ como definido no Exemplo 2.3.1. Então:*

(i) Para cada $g \in G$, os elementos de $V_g(X)$ são dois a dois fortemente distintos.

(ii) A aplicação $\omega : X \longrightarrow V(X)$ dada por $\omega(x) = \rho_x$ é um isomorfismo de G-conjuntos.

Demonstração: (i) Como R é uma extensão β-Galois de R^β, para cada $y \in X$ a aplicação $\varphi_y : E_y \otimes_K A(X) \longrightarrow \prod_{x \in X_y} E_x$ dada por $\varphi(r \otimes_K f) = (rf(x))_{x \in X_y}$, $r \in E_y, f \in A(X)$, é um isomorfismo de R-álgebras, pelo Lema 2.2.6. Note que se $y \in X$, então existe $g \in G$ tal que $y \in X_g$, portanto temos que $E_y = E_g$ e $X_y = X_g$. Logo para cada $x \in X_g$, existem $r_{ix} \in E_g$ e $f_{ix} \in A(X)$, $1 \leq i \leq m_x$, tais que $(\sum_{i=1}^{m_x} r_{ix} f_{ix}(y))_{y \in X_g} = (\delta_{xy} 1_y)_{y \in X_g}$, ou seja, $\sum_{i=1}^{m_x} r_{ix} f_{ix}(y) = \delta_{xy} 1_y$, para todo $y \in X_g$. Porém, $f_{ix}(y) = \rho_y(f_{ix})$, assim temos que $\sum_{i=1}^{m_x} r_{ix} \rho_y(f_{ix}) = \delta_{xy} 1_y$, para todo $\rho_y \in V_g(X)$. Então, pela Proposição 2.1.3, para cada $g \in G$, os elementos de $V_g(X)$ são dois a dois fortemente distintos.

(ii) Já provamos no Lema 2.2.5 que se a aplicação $\varphi_g : E_g \otimes_K A(X) \longrightarrow \prod_{x \in X_g} E_x$ dada por $\varphi_g(r \otimes_K f) = (rf(x))_{x \in X_g}$ é isomorfismo, então a aplicação $\omega_g : X_g \longrightarrow V_g(X)$ dada por $\omega_g(x) = \rho_x$ é uma bijeção, para todo $g \in G$. Por conseguinte, a aplicação $\omega : X = \dot{\bigcup}_{e \in G_0} X_e \longrightarrow V(X) = \dot{\bigcup}_{e \in G_0} V_e(X)$ definida por $\omega(x) = \omega_g(x)$ se $x \in X_g$ é uma bijeção. Resta provar que esta bijeção preserva a ação. Com efeito, para $x \in X_{g^{-1}}$, temos

$$\omega(\gamma_g(x))(f) = \rho_{\gamma_g(x)}(f) = f(\gamma_g(x)) = \beta_g(f(x)) = \sigma_g(\rho_x)(f) = \sigma_g(\omega(x))(f),$$

o que conclui a demonstração. ■

Lema 2.3.3. *Suponha que R é uma extensão β-Galois de R^β e seja B uma K-álgebra. Suponha que para cada $g \in G$, existe um isomorfismo de R-álgebras $\varphi_g : E_g \otimes_K B \longrightarrow (E_g)^n$, $n \geq 1$. Então:*

(i) Para cada $g \in G$, existem $\varphi_{g1}, ..., \varphi_{gn} \in Alg_K(B, E_g)$ tais que $\varphi_g(r \otimes_K b) = (r\varphi_{gi}(b))_{i=1}^n$, para todo $r \in E_g$ e $b \in B$.

(ii) Para cada $g \in G$, os elementos de $V_g(B) = \{\varphi_{gi} | \ 1 \leq i \leq n\}$ são dois a dois fortemente distintos.

(iii) $V_g(B) = Alg_K(B, E_g)$ sempre que os elementos de $Alg_K(B, E_g)$ forem dois a

dois fortemente distintos.

Demonstração: (i) Para cada $g \in G$, denote por $\eta_g : B \longrightarrow E_g \otimes_K B$ a imersão canônica ($b \longmapsto 1_g \otimes_K b$) e $\pi_{gi} : (E_g)^n \longrightarrow E_g$ a i-ésima projeção canônica. Seja $\varphi_{gi} := \pi_{gi}\varphi_g\eta_g : B \longrightarrow E_g$. Desta maneira, para $r \in E_g$ e $b \in B$, temos

$$(r\varphi_{gi}(b))_{i=1}^n = (r\pi_{gi}\varphi_g\eta_g(b))_{i=1}^n = (r\pi_{gi}(\varphi_g(1_g \otimes_K b)))_{i=1}^n = (\pi_{gi}(\varphi_g(r \otimes_K b)))_{i=1}^n$$

$$= \varphi_g(r \otimes_K b).$$

(ii) Como φ_g é isomorfismo, então para cada $1 \leq i \leq n$, existem $r_{il} \in E_g$ e $b_{il} \in B$, $1 \leq l \leq m_g$, tais que $\varphi_g(\sum_{l=1}^{m_g} r_{il} \otimes_K b_{il}) = (\sum_{l=1}^{m_l} r_{il}\varphi_{gj}(b_{il}))_{j=1}^n = (\delta_{ij}1_g)_{j=1}^n$, ou seja, $\sum_{l=1}^{m_l} r_{il}\varphi_{gj}(b_{il}) = \delta_{ij}1_g$ para todo $1 \leq j \leq n$. Por conseguinte, pela Proposição 2.1.3, os elementos de $V_g(B)$ são dois a dois fortemente distintos.

(iii) Vamos supor que os elementos de $Alg_K(B, E_g)$ são dois a dois fortemente distintos. Então, pelo Corolário 2.1.4, $\#Alg_K(B, E_g) \leq rank_{K_\mathfrak{p}} B_\mathfrak{p}$ para todo ideal primo $\mathfrak{p}$ de K. Agora note que, pelo item (ii), os elementos de $V_g(B)$ são dois a dois fortemente distintos, logo pela Proposição 2.1.3 $V_g(B)$ é linearmente independente sobre E_g em $Hom_K(B, E_g)$. Desta maneira, $\#(V_g(B))_\mathfrak{p} = \#V_g(B) = n = rank_K B$. Observe que esta última igualdade é válida porque

$$rank_K B = rank_{E_g} E_g \otimes_K B = rank_{E_g}(E_g)^n = n = \#V_g(B).$$

Mais ainda, $B_\mathfrak{p}$ é um $K_\mathfrak{p}$-módulo livre e $rank_{K_\mathfrak{p}} B_\mathfrak{p} = rank_K B = n$. Desta maneira, temos

$$\#Alg_K(B, E_g) \leq rank_{K_\mathfrak{p}} B_\mathfrak{p} = n = \#V_g(B) \leq \#Alg_K(B, E_g).$$

Como $V_g(B) \subseteq Alg_K(B, E_g)$, concluímos que $V_g(B) = Alg_K(B, E_g)$, para todo $g \in G$. ■

Lema 2.3.4. *Suponha que R é uma extensão β-Galois de R^β e considere B uma K-álgebra. Suponha que para cada $g \in G$, existe um isomorfismo de R-álgebras $\varphi_g : E_g \otimes_K B \longrightarrow (E_g)^n$, e tome $V(B) = \dot{\bigcup\limits_{e \in G_0}} V_e(B)$, onde, para cada $g \in G$, $V_g(B)$ é o conjunto definido no Lema 2.3.3. Então as seguintes afirmações são equivalentes:*

(i) $V(B)$ é um G-conjunto via $\xi = \{\xi_g : V_{g^{-1}}(B) \longrightarrow V_g(B)\}_{g \in G}$, onde $\xi_g(\varphi_{g^{-1}i})(b) = \beta_g(\varphi_{g^{-1}i}(b))$.

(ii) Para todo $g, h \in G$ com $r(g) = r(h)$, dados $\varphi_{g^{-1}i} \in V_{g^{-1}}(B)$ e $\varphi_{h^{-1}j} \in V_{h^{-1}}(B)$, tem-se que $\xi_g(\varphi_{g^{-1}i})$ e $\xi_h(\varphi_{h^{-1}j})$ são fortemente distintos.

Demonstração: $(i) \Rightarrow (ii)$ Se $V(B)$ é um G-conjunto via $\xi = \{\xi_g : V_{g^{-1}}(B) \longrightarrow V_g(B)\}_{g \in G}$, então $\xi_g(\varphi_{g^{-1}i}) \in V_g(B)$. Pelo Lema 2.3.3, os elementos de $V_g(B)$ são dois a dois fortemente distintos, logo segue (ii).

$(ii) \Rightarrow (i)$ Como foi citado na implicação anterior, para cada $g \in G$, os elementos de $V_{g^{-1}}(B)$ são dois a dois fortemente distintos, logo pela Proposição 2.1.3, para cada $1 \leq k \leq n$ existem elementos $r_{ik} \in E_{g^{-1}}$ e $b_{ik} \in B$, $1 \leq i \leq m_{g^{-1}}$, tais que $\sum\limits_{i=1}^{m_{g^{-1}}} r_{ik}\varphi_{g^{-1}j}(b_{ik}) = \delta_{jk}1_{g^{-1}}$, para $1 \leq j \leq n$. Aplicando β_g em ambos os lados da igualdade, tem-se que $\sum\limits_{i=1}^{m_{g^{-1}}} \beta_g(r_{ik})\beta_g(\varphi_{g^{-1}j}(b_{ik})) = \delta_{jk}1_g$, para $1 \leq j \leq n$, ou seja, $\sum\limits_{i=1}^{m_{g^{-1}}} \beta_g(r_{ik})\ \xi_g(\varphi_{g^{-1}j})(b_{ik}) = \delta_{jk}1_g$, para $1 \leq j \leq n$. Pela Proposição 2.1.3, os elementos de $\xi_g(V_{g^{-1}}(B))$ são dois a dois fortemente distintos. Observe que $\xi_g(V_{g^{-1}}(B)) = \xi_g(V_{d(g)}(B)) = \xi_g(\dot{\bigcup\limits_{e \in G_0}} V_e(B)1'_{g^{-1}}) = \xi_g(V(B)1'_{g^{-1}})$, onde $1'_{g^{-1}} : B \longrightarrow E_{g^{-1}}$ é dado por $1'_{g^{-1}}(b) = 1_{g^{-1}}$.

Considere $Y(B) = \bigcup\limits_{g \in G} \xi_g(\dot{\bigcup\limits_{e \in G_0}} V_e(B)1'_{g^{-1}}) = \bigcup\limits_{g \in G} \xi_g(V_{g^{-1}}(B))$. Defina $Y_g(B) = Y_{r(g)}(B) = \{\xi_h(V_{h^{-1}}(B)) |\ r(h) = r(g)\}$. Como os elementos de $\xi_g(V_{g^{-1}}(B))$ são dois a dois fortemente distintos, temos que, utilizando a hipótese, os elementos de $Y_g(B)$

são dois a dois fortemente distintos para cada $g \in G$. Entretanto, note que

$$V_f(B) = \xi_f(V_f(B)) \subseteq Y(B),$$

para todo $f \in G_0$, logo $V(B) = \dot{\bigcup\limits_{e \in G_0}} V_e(B) \subseteq Y(B)$, o que acarreta $V_g(B) \subseteq Y_g(B)$, para todo $g \in G$. Pelo Corolário 2.1.4, $\#Y_g(B) \leq rank_{K_\mathfrak{p}} B_\mathfrak{p}$ para todo ideal primo $\mathfrak{p}$ de K, e pelo Lema 2.1.5, $rank_K B = n$. Assim,

$$\#Y_g(B) \leq rank_{K_\mathfrak{p}} B_\mathfrak{p} = n = \#V_g(B) \leq \#Y_g(B).$$

Deste jeito, $\xi_g(V_{g^{-1}}(B)) \subseteq Y_g(B) = V_g(B)$ para todo $g \in G$. Porém, note que $\#V_g(B) = n = \#\xi_g(V_{g^{-1}}(B))$, logo $\xi_g(V_{g^{-1}}(B)) = V_g(B)$, concluindo que ξ_g é uma bijeção. Não é difícil ver que ξ satisfaz as condições (i) e (ii) da Definição 2.2.1, portanto temos que $V(B)$ é um G-conjunto. ■

Definição 2.3.5. *Seja* $S = \bigoplus\limits_{j=1}^{n} E_j$ *uma* K*-álgebra, onde* $E_j = S1_j$ *e* $\{1_j\}_{1 \leq j \leq n}$ *são idempotentes centrais em* S *dois a dois ortogonais, para algum* $n \geq 1$*. Dizemos que uma* K*-álgebra* T *é* S*-decomponível se:*

(i) Para cada $1 \leq j \leq n$*, existe um isomorfismo de* K*-álgebras* $\phi_j : E_j \otimes_K T \longrightarrow (E_j)^m$*, para algum* $m \geq 1$*;*

(ii) $V(T) = \bigcup\limits_{j=1}^{n} V_j(T)$ *é um* G*-conjunto, onde* $V_j(T)$ *é como definido no Lema 2.3.3.*

Note que $E_j \otimes_K T \simeq (E_j)^m$ implica que $R \otimes_K T = (\bigoplus\limits_{j=1}^{n} E_j) \otimes_K T = \bigoplus\limits_{j=1}^{n} (E_j \otimes_K T) \simeq \bigoplus\limits_{j=1}^{n} (E_j)^m = (\bigoplus\limits_{j=1}^{n} E_j)^m = R^m$.

Lema 2.3.6. *Suponha que* R *é uma extensão* β*-Galois de* R^β *e considere* B *uma* K*-álgebra. Suponha que para cada* $g \in G$*, existe um isomorfismo de* R*-álgebras* $\varphi_g : E_g \otimes_K B \longrightarrow (E_g)^n$*,* $n \geq 1$*, e que* $V(B) = \dot{\bigcup\limits_{e \in G_0}} V_e(B)$*, onde* $V_g(B)$*,* $g \in G$*, é como definido no Lema 2.3.3, é um* G*-conjunto, via* $\xi = \{\xi_g : V_{g^{-1}}(B) \longrightarrow V_g(B)\}_{g \in G}$*.*

Então a aplicação $\nu : B \longrightarrow A(V(B))$ dada por $\nu(b)(\varphi_{gi}) = \varphi_{gi}(b)$, para $b \in B$, $\varphi_{gi} \in V(B)$, é um isomorfismo de K-álgebras.

Demonstração: A aplicação $\nu : B \longrightarrow A(V(B))$ dada por $\nu(b)(\varphi_{gi}) = \varphi_{gi}(b)$, para $b \in B$, $\varphi_{gi} \in V(B)$, claramente é um homomorfismo de K-álgebras. Vejamos que está bem definida. De fato, dados $a, b \in B$, se $a = b$, então $\varphi_{gi}(a) = \varphi_{gi}(b)$ para todo $g \in G$ e para todo $1 \leq i \leq n$, portanto $\nu(a) = \nu(b)$. Mais ainda, para $g \in G$, $b \in B$ e $\varphi_{gi} \in V(B)$,

$$\begin{aligned} \alpha_g(\nu(b)1'_{g^{-1}})(\varphi_{gi}) &= \beta_g \circ \nu(b)1'_{g^{-1}} \circ \xi_{g^{-1}}(\varphi_{gi}) = \beta_g(\nu(b)(\xi_{g^{-1}}(\varphi_{gi}))1_{g^{-1}}) \\ &= \beta_g(\xi_{g^{-1}}(\varphi_{gi})(b)1_{g^{-1}}) = \beta_g(\beta_{g^{-1}}(\varphi_{gi}(b)1_g)1_{g^{-1}}) \\ &= \beta_{r(g)}(\varphi_{gi}(b)1_{r(g)}) = \varphi_{gi}(b)1_{r(g)} \\ &= \varphi_{gi}(b)1_g = \nu(b)(\varphi_{gi})1_g = \nu(b)1'_g(\varphi_{gi}), \end{aligned}$$

mostrando que $\nu(b) \in A(V(B))$. Resta verificar a bijeção.

Dados $a, b \in B$, se $a \neq b$, então $\varphi_g(1 \otimes_K a) \neq \varphi_g(1 \otimes_K b)$, já que, para cada $g \in G$, φ_g é um isomorfismo. Deste modo, existe $i \in \{1, ..., n\}$ tal que $\nu(a)(\varphi_{gi}) = \varphi_{gi}(a) \neq \varphi_{gi}(b) = \nu(b)(\varphi_{gi})$, concluindo que $\nu(a) \neq \nu(b)$, o que prova que ν é injetiva.

Pelo Lema 2.1.5, $rank_K B = \#V_g(B)$ e pelo Lema 2.2.5, $rank_K A(V(B)) = \#V_g(B)$. Ou seja, $\nu(B)$ e $A(V(B))$ tem o mesmo posto sobre K, pois $\nu(B) \simeq B$. Além disso, novamente pelos Lemas 2.1.5 e 2.2.5, temos que tanto B (consequentemente, $\nu(B)$) quanto $A(V(B))$ são K-álgebras fielmente projetivas e separáveis. Logo, pelo Lema 2.1.1, $\nu(b) = A(V(B))$, mostrando que ν é sobrejetora. ■

Teorema 2.3.7. ***Correspondência de Galois-Grothendieck.*** *Suponha que R é uma extensão β-Galois de R^β. Então existe uma correspondência biunívoca entre os G-conjuntos finitos e as R^β-álgebras que são R-decomponíveis.*

Demonstração: Pelo Lema 2.2.6, dado um G-conjunto finito X, $\varphi_g : E_g \otimes_K A(X) \longrightarrow \prod_{x \in X_g} E_x$ definida por $\varphi_g(r \otimes_K f) = (rf(x))_{x \in X_g}$, $g \in G, r \in R, f \in A(X)$, é um isomorfismo de R-álgebras.

Afirmação: $V_g(A(X)) = V_g(X)$, para todo $g \in G$.

Com efeito, $V_g(X) = \{\rho_x : A(X) \longrightarrow E_g |\ x \in X_g \text{ e } \rho_x(f) = f(x), \forall f \in A(X)\}$ e se $B = A(X)$, $V_g(B) = \{\varphi_{gi} |\ \varphi_{gi} = \pi_{gi}\varphi_g\eta_g\}$, onde $\eta_g : B \longrightarrow E_g \otimes_K B$ é a aplicação canônica e $\pi_{gi} : (E_g)^n \longrightarrow E_g$ é a i-ésima projeção em E_x. Logo

$$\begin{aligned}\varphi_{gi}(f)) &= \pi_{gi}\varphi_g\eta_g(f) = \pi_{gi}(\varphi_g(1_g \otimes_K f)) \\ &= \pi_{gi}((f(x))_{x\in X_g}) = f(x_i) = \rho_{x_i}(f).\end{aligned}$$

Por conseguinte, $V_g(A(X)) = V_g(X)$ para todo $g \in G$, isto é, $V(A(X)) = V(X)$.

Considere a aplicação θ dos G-conjuntos finitos nas K-álgebras R-decomponíveis definida por $\theta(X) = A(X)$ e a aplicação θ' das K-álgebras R-decomponíveis nos G-conjuntos finitos dada por $\theta'(B) = V(B)$. Pelo Lema 2.3.2, $X \simeq V(X)$ como G-conjuntos, e pela afirmação anterior, $V(X) = V(A(X))$. Assim, $X \simeq V(A(X)) = \theta'(\theta(X))$. Por outro lado, pelo Lema 2.3.6, $B \simeq A(V(B))$ como K-álgebras, logo $B \simeq A(V(B)) = \theta(\theta'(B))$, o que mostra que θ é uma bijeção, como queríamos. ∎

2.4 Uma nova visão para o Teorema Fundamental

Seja H um subgrupóide amplo de G. Vimos no Exemplo 2.2.3 que, tomando a relação de equivalência $\equiv_H$ definida no Lema 1.1.24, o conjunto das classes laterais $\frac{G}{H} = \{gH\ |g \in G\}$ é um G-conjunto.

Considere $\{g_i\}_{i=1}^n$ um sistema de representantes das classes de equivalência dessa relação. Desta maneira, $E_{g_iH} = E_{r(g_i)} = E_{g_i}$. (Lembre-se que se $X = \dot{\bigcup\limits_{e\in G_0}} X_e$ é um G-conjunto e se $x \in X_g$, então $E_x = E_{r(g)} = E_g$.)

Lema 2.4.1. *$A(\frac{G}{H}) \simeq R^{\beta_H}$ como K-álgebras.*

Demonstração: Já observamos anteriormente que $Map(\frac{G}{H}, R)$ é uma K-álgebra via as operações pontuais e portanto $A(\frac{G}{H}) \subseteq Map(\frac{G}{H}, R)$ é uma K-álgebra.

Considere a aplicação

$$\begin{array}{rcl} \theta \ : \ A(\frac{G}{H}) & \longrightarrow & R^{\beta_H} \\ f & \longmapsto & \sum\limits_{e \in G_0} f(eH). \end{array}$$

Afirmação 1: θ está bem definida.

Para $h \in H$,

$$\beta_h(\sum_{e \in G_0} f(eH)1_{h^{-1}}) = \sum_{e \in G_0} \beta_h(f(eH)1_{h^{-1}}) = \beta_h(f(d(h)H)1_{h^{-1}})$$
$$= \beta_h(\beta_{h^{-1}}(f(hd(h)H)1_h)1_{h^{-1}}) = \beta_{r(h)}(f(hH)1_{r(h)}) = f(hH)1_h$$
$$= f(r(h)H)1_h = \sum_{e \in G_0} f(eH)1_h.$$

Note que $r(h) \equiv_H h$, pois $h^{-1}r(h) = h^{-1}d(h^{-1}) = h^{-1} \in H$.

Agora tome

$$\begin{array}{rcl} \theta' \ : \ R^{\beta_H} & \longrightarrow & A(\frac{G}{H}) \\ r & \longmapsto & \theta'_r, onde \quad \theta'_r(gH) = \beta_g(r1_{g^{-1}}). \end{array}$$

Afirmação 2: θ'_r está bem definida.

Suponha $g_1H = g_2H$. Dado $g_1h_1 \in g_1H$, existe $h_2 \in H$ tal que $g_1h_1 = g_2h_2$. Note que $d(h_1) = d(g_1h_1) = d(g_2h_2) = d(h_2)$, portanto $g_1 = g_2h_2h_1^{-1}$. Desta maneira,

$$\beta_{g_1}(r1_{g_1^{-1}}) = \beta_{g_2h_2h_1^{-1}}(r1_{h_1h_2^{-1}g_2^{-1}}) = \beta_{g_2}(\beta_{h_2h_1^{-1}}(r1_{h_1h_2^{-1}})1_{g_2^{-1}}) = \beta_{g_2}(r1_{g_2^{-1}}),$$

já que $r \in R^{\beta_H}$ e $h_2h_1^{-1} \in H$.

Afirmação 3: θ' está bem definida.

Para $h \in G$ com $r(h) = r(g)$, temos

$$\begin{aligned} h * \theta'_r(gH) &= \beta_h(\theta'_r 1'_{h^{-1}}(\gamma_{h^{-1}}(gH))) = \beta_h(\theta'_r(h^{-1}gH)1_{h^{-1}}) \\ &= \beta_h(\beta_{h^{-1}g}(r1_{g^{-1}h})1_{h^{-1}}) = \beta_h(\beta_{h^{-1}}(\beta_g(r1_{g^{-1}})1_h)1_{h^{-1}}) \\ &= \beta_{r(h)}(\beta_g(r1_{g^{-1}})1_{r(h)}) = \beta_g(r1_{g^{-1}})1_{r(h)} \\ &= \beta_g(r1_{g^{-1}}) = \theta'_r(gH). \end{aligned}$$

Claramente, θ e θ' são homomorfismos de K-álgebras. Ainda:

$$\theta \circ \theta'(r) = \theta(\theta'_r) = \sum_{e \in G_0} \theta_r^{-1}(eH) = \sum_{e \in G_0} \beta_e(r1_e) = \sum_{e \in G_0} r1_e = r$$

e

$$\begin{aligned}
\theta' \circ \theta(f)(gH) &= \theta'(\sum_{e \in G_0} f(eH))(gH) = \beta_g(\sum_{e \in G_0} f(eH)1_{g^{-1}}) \\
&= \beta_g(f(d(g)H)1_{g^{-1}}) = \beta_g(\beta_{g^{-1}}(f(gd(g)H)1_g)1_{g^{-1}}) \\
&= \beta_{r(g)}(f(gd(g)H)1_{r(g)}) = f(gH)1_g = f(gH),
\end{aligned}$$

o que conclui que $\frac{G}{H} \simeq R^{\beta_H}$. ■

Lema 2.4.2. *Para $gH \in \frac{G}{H}$, tome o homomorfismo de K-álgebras ρ_{gH} de $A(\frac{G}{H})$ em $E_{r(g)}$ definido por $\rho_{gH}(f) = f(gH)$, para todo $f \in A(\frac{G}{H})$. Se os elementos de $V_{gH} = \{\rho_{lH} | \quad r(l) = r(g)\}$ são dois a dois fortemente distintos, então R^{β_H} é β-forte.*

Demonstração: Pelo Lema 2.4.1, $A(\frac{G}{H}) \simeq R^{\beta_H}$ via a aplicação θ. Considere $\phi_{gH} := \rho_{gH} \circ \theta^{-1} : R^{\beta_H} \longrightarrow E_{r(g)}$. Como os elementos de V_{gH} são dois a dois fortemente distintos, não é difícil ver que os elementos de $\widetilde{V}_{gH} = \{\phi_{lH} | \quad r(l) = r(g)\}$ também são dois a dois fortemente distintos.

Seja $T = R^{\beta_H}$ e sejam $g, h \in G$ com $r(g) = r(h)$ e $g^{-1}h \notin H_T = \{g \in G | \quad \beta_g(t1_{g^{-1}}) = t1_g \quad \forall t \in T\}$. Dado $e \in E_g = E_{r(g)}$, existe $r \in R^{\beta_H}$ tal que $e\phi_{gH}(r) \neq e\phi_{hH}(r)$. Assim,

$$e\beta_g(r1_{g^{-1}}) = e\theta^{-1}(r)(gH) = e\rho_{gH}(\theta^{-1}(r)) = e\phi_{gH}(r) \neq e\phi_{hH}(r) = e\rho_{hH}(\theta^{-1}(r)) = e\theta^{-1}(r)(gH) = e\beta_h(r1_{h^{-1}}).$$

Logo R^{β_H} é β-forte. ■

Lema 2.4.3. *Suponha que R é uma extensão β-Galois de R^β e que T é uma subálgebra de R que é R^β-separável e β-forte. Então existem elementos $x_i, y_i \in T$,*

$1 \leq i \leq m$, *tais que* $\sum_{i=1}^{m} x_i\beta_g(y_i 1_{g^{-1}}) = 0$ *se* $\beta_g|_{T1_{g^{-1}}} \neq \beta_e|_{T1_e}$, *para* $e \in G_0$, *e* $\sum_{i=1}^{m} x_i\beta_g(y_i 1_{g^{-1}}) = 1_e$ *se* $\beta_g|_{T1_{g^{-1}}} = \beta_e|_{T1_e}$, *para* $e \in G_0$. *Em particular,* T *é finitamente gerado e projetivo como* R^β*-módulo.*

Demonstração: Como T é R^β-separável, seja $e = \sum_{i=1}^{n} x_i \otimes_{R^\beta} y_i \in T \otimes_{R^\beta} T$ o idempotente de separabilidade e seja $\mu : R \otimes_{R^\beta} R$ a aplicação multiplicação.

Para $g \in G$, defina

$$\begin{aligned} \theta \ : \ R \otimes_{R^\beta} R &\longrightarrow R \otimes_{R^\beta} E_g \\ x \otimes_{R^\beta} y &\longmapsto x \otimes_{R^\beta} \beta_g(y1_{g^{-1}}). \end{aligned}$$

Para cada $g \in G$, tome $e_g = \mu(\theta_g(e)) = \sum_{i=1}^{n} x_i\beta_g(y_i 1_{g^{-1}}) \in E_g$. Note que

$e = e^2 \Rightarrow \theta_g(e) = \theta_g(e.e) = \theta_g(e)\theta_g(e) \Rightarrow \mu(\theta_g(e)) = \mu(\theta_g(e)\theta_g(e)) = \mu(\theta_g(e))\mu(\theta_g(e))$,

logo e_g é um idempotente de E_g.

Mais ainda, como T é um $T \otimes_{R^\beta} T$-módulo via

$$(x \otimes_{R^\beta} y).t = xty, \quad para \quad x, y, t \in T,$$

temos que μ é $T \otimes_{R^\beta} T$-linear e θ_g é $T \otimes_{R^\beta} R^\beta$-linear. De fato,

$$\begin{aligned} \mu((x \otimes_{R^\beta} y).(a \otimes_{R^\beta} b)) &= \mu(xa \otimes_{R^\beta} yb) = \mu(xa \otimes_{R^\beta} by) = xaby = (x \otimes_{R^\beta} y).ab \\ &= (x \otimes_{R^\beta} y).\mu(a \otimes_{R^\beta} b), \end{aligned}$$

para $x, y, a, b \in T$ e

$$\begin{aligned} \theta_g((x \otimes_{R^\beta} y)(a \otimes_{R^\beta} b)) &= \theta_g(xa \otimes_{R^\beta} yb) = xa \otimes_{R^\beta} \beta_g(yb1_{g^{-1}}) = xa \otimes_{R^\beta} y\beta_g(yb1_{g^{-1}}) \\ &= (x \otimes_{R^\beta} y)\theta(a \otimes_{R^\beta} b), \end{aligned}$$

para $x, a, b \in T$ e $y \in R^\beta$.

Então, para qualquer $t \in T$,

$$te_g = t\mu(\theta_g(e)) = (t \otimes_{R^\beta} 1).\mu(\theta_g(e)) = \mu(\theta_g((t \otimes_{R^\beta} 1)e)) = \mu(\theta_g((1 \otimes_{R^\beta} t)e)) =$$
$$\mu(\theta_g((1 \otimes_{R^\beta} t))\mu(\theta_g(e)) = \beta_g(t1_{g^{-1}})e_g.$$

Como T é β-forte, se $g \notin G_0$, então $e_g = 0$, ou seja, $\sum_{i=1}^{n} x_i\beta_g(y_i1_{g^{-1}}) = 0$.

Para a segunda parte deste lema, defina

$$\begin{array}{rcl} f_i \ : \ T & \longrightarrow & R^\beta \\ t & \longmapsto & tr_\beta(y_it). \end{array}$$

Pela Observação 1.2.8, as aplicações $\{f_i\}_{i=1}^n$ estão bem definidas e são claramente homomorfismos de R^β-módulos. Desta maneira,

$$\sum_{i=1}^{n} f_i(t)x_i = \sum_{i=1}^{n}\sum_{g\in G} \beta_g(y_it1_{g^{-1}})x_i = \sum_{g\in G} \delta_{g,e}\beta_g(t1_{g^{-1}}) = \sum_{e\in G_0} 1_et = t.$$

Por [20], Theorem II.12, T é finitamente gerado e projetivo. ■

Lema 2.4.4. *Suponha que R é uma extensão β-Galois de R^β e seja T uma R^β-subálgebra de R. Então as seguintes condições são equivalentes:*
(i) T é R^β-separável e β-forte.
(ii) $T = R^{\beta_{H_T}}$.

Demonstração: $(i) \Rightarrow (ii)$ Assuma que T é uma R^β-subálgebra separável de R que é β-forte. Tome $H_T = \{g \in G| \quad \beta_g(t1_{g^{-1}}) = t1_g, \forall t \in T\}$. Pelo Lema 2.4.3, T é finitamente gerado e projetivo como R^β-módulo. Como $T \subseteq R^{\beta_{H_T}}$, $T_\mathfrak{p} \subseteq (R^{\beta_{H_T}})_\mathfrak{p}$, logo temos que $rank_{(R^\beta)_\mathfrak{p}}T_\mathfrak{p} \leq rank_{(R^\beta)_\mathfrak{p}}(R^{\beta_{H_T}})_\mathfrak{p}$, para todo ideal primo $\mathfrak{p}$ de R^β.
Afirmação: $rank_{(R^\beta)_\mathfrak{p}}T_\mathfrak{p} = rank_{(R^\beta)_\mathfrak{p}}(R^{\beta_{H_T}})_\mathfrak{p}$.

Considere a relação de equivalência $\equiv_{H_T}$ em G dada por $a \equiv_{H_T} b \Leftrightarrow \exists b^{-1}a$ e $b^{-1}a \in H_T$. Seja $\{g_i\}_{i=1}^n$ um sistema de representantes das classes. Defina

$$\begin{array}{rcl} f_i \ : \ T & \longrightarrow & E_{g_i} \\ t & \longmapsto & \beta_{g_i}(t1_{g_i^{-1}}). \end{array}$$

Note que os f_i's são claramente homomorfismos de R^β-álgebras e os elementos de $V_{g_i} = \{f_j|\ 1_{g_j} = 1_{g_i}\}$ são dois a dois fortemente distintos, já que T é β-forte. Logo pelo Corolário 2.1.4, $\#V_{g_i} \leq rank_{(R^\beta)_\mathfrak{p}} T_\mathfrak{p}$, para todo ideal primo $\mathfrak{p}$ de R^β.

Pelo Lema 2.2.6, temos que, para cada $g_i \in G$, $1 \leq i \leq n$, $E_{g_i} \otimes_{R^\beta} R^{\beta H_T} \simeq \prod_{x \in (\frac{G}{H_T})_{g_i}} E_x$, logo $(E_{g_i})_\mathfrak{p} \otimes_{(R^\beta)_\mathfrak{p}} R^{\beta H_T} \simeq \prod_{x \in (\frac{G}{H_T})_{g_i}} (E_x)_\mathfrak{p}$. Note que neste caso $(\frac{G}{H_T})_{g_i} = \{lH_T|\ r(l) = r(g_i)\}$, como foi mostrado no Exemplo 2.2.3. Isto nos leva a concluir que $\#V_{g_i} = \#(\frac{G}{H_T})_{g_i}$.

Temos então

$$rank_{(R^\beta)_\mathfrak{p}} (R^{\beta H_T})_\mathfrak{p} = rank_{(E_{g_i})_\mathfrak{p}} ((E_{g_i})_\mathfrak{p} \otimes_{(R^\beta)_\mathfrak{p}} (R^{\beta H_T})_\mathfrak{p}) = rank_{(E_{g_i})_\mathfrak{p}} \prod_{x \in (\frac{G}{H_T})_{g_i}} (E_x)_\mathfrak{p} =$$

$$\#(\frac{G}{H_T})_{g_i} = \#V_{g_i} \leq rank_{(R^\beta)_\mathfrak{p}} T_\mathfrak{p}.$$

Logo $rank_{(R^\beta)_\mathfrak{p}} T_\mathfrak{p} = rank_{(R^\beta)_\mathfrak{p}} (R^{\beta H_T})_\mathfrak{p}$.

Por conseguinte, pelo Lema 2.1.1, $T = R^{\beta H_T}$.

$(ii) \Rightarrow (i)$ Pelo Lema 2.2.6, $T = R^{\beta H_T} \simeq A(\frac{G}{H_T})$ é R-decomponível, logo decorre do Lema 2.1.5 que T é separável. Além disso, pelo Lema 2.3.2 os elementos de $V_g = \{\rho_{hH_T} : A(\frac{G}{H_T}) \longrightarrow E_g|\ hH_T \in (\frac{G}{H_T})_g$ e $\rho_{hH_T}(f) = f(hH_T), \forall f \in A(\frac{G}{H_T})\} = \{\rho_{hH_T}|\ r(h) = r(g)$ e $\rho_{hH_T}(f) = f(hH_T), \forall f \in A(\frac{G}{H_T})\}$ são dois a dois fortemente distintos. Desta forma, pelo Lema 2.4.2, $R^{\beta H_T}$ é β-forte. ■

Estamos aptos a dar uma nova demonstração para o Teorema Fundamental da Teoria de Galois. Note que cada subgrupóide H de G é um G-conjunto, e quando T é uma extensão fortemente separável e β-forte de R^β, segue pelos Lemas 2.4.4 e 2.2.6 que T é R-decomponível, portanto podemos visualizar o Teorema de Correspondência como um caso particular da Correspondência de Galois-Grothendieck.

Teorema 2.4.5. ***Teorema de Correspondência de Galois.*** *Suponha que R é uma extensão β-Galois de R^{β}. Então a correspondência $H \mapsto R^{\beta_H}$ é biunívoca entre o conjunto dos subgrupóides amplos de G e as R^{β}-subálgebras de R que são separáveis e β-fortes.*

Demonstração: Sejam $Subg(G)$ o conjunto dos subgrupóides amplos H de G, $Quoc(G)$ a família dos conjuntos quocientes $\frac{G}{H}$ de G e $sGf(R)$ o conjunto das subálgebras de R que são separáveis e β-fortes. Seja H um subgrupóide amplo de G. Considere a aplicação θ_1 de $Subg(G)$ em $Quoc(G)$ dada por $\theta_1(H) = \frac{G}{H}$, e defina θ_2 de $Quoc(G)$ em $sGf(R)$ por $\theta_2(\frac{G}{H}) = A(\frac{G}{H})$. Observe que θ_1 é, claramente, bijetiva. Tome $\theta := \theta_2 \circ \theta_1 : Subg(G) \longrightarrow sGf(R)$. Queremos mostrar que θ é uma bijeção. Para isto, resta provar que θ_2 é uma bijeção.

Porém, sabemos que, dado $T \in sGf(R)$, $T = R^{\beta_{H_T}}$, pelo Lema 2.4.4. Além disso, $R^{\beta_{H_T}} \simeq A(\frac{G}{H_T})$, pelo Lema 2.4.1, logo a aplicação θ_2 é bijetiva, como pode ser observado no seguinte diagrama:

$$\begin{array}{ccccc}
Subg(G) & & Quoc(G) & & sGf(R) \\
H & \stackrel{\theta_1}{\longrightarrow} & \frac{G}{H} & \stackrel{\theta_2}{\longrightarrow} & A(\frac{G}{H}) \simeq R^{\beta_H} \\
H_T & \stackrel{\theta_1^{-1}}{\longleftarrow} & \frac{G}{H_T} & \stackrel{\theta_2^{-1}}{\longleftarrow} & T = R^{\beta_{H_T}} \simeq A(\frac{G}{H_T}).
\end{array}$$

■

Note que $sGf(R)$ coincide com o conjunto das R^{β}-álgebras do tipo $A(\frac{G}{H})$, o que mostra que a correspondência de Galois é, de fato, uma bijeção entre $Subg(G)$ e o conjunto das R^{β}-álgebras R-decomponíveis do tipo $A(\frac{G}{H})$.

Capítulo 3

Teorema Fundamental no Caso Não-Comutativo

Nos capítulos anteriores estava-se assumindo a comutatividade do anel R. Todavia, neste último capítulo, esta hipótese será omitida, e no que sucede, dado um grupóide finito G agindo sobre R via β, estaremos interessados em analisar sob que condições a aplicação de Galois $\theta : H \mapsto R^{\beta_H}$ é injetiva, mas não necessariamente sobrejetiva, do conjunto dos subgrupóides amplos H de G no conjunto das subextensões separáveis entre R^β e R. Neste tópico, seguiremos baseados no trabalho de G. Szeto e L. Xue ([24]), onde foram publicados resultados em que a aplicação de Galois é injetiva para o caso de ação de grupos.

Ainda no contexto não necessariamente comutativo, mostraremos uma caracterização de álgebras β-Galois centrais (tais que R^{β_H} é uma subálgebra separável de R para cada subgrupóide H de G) que satisfazem o Teorema Fundamental, seguindo outro trabalho de G. Szeto e L. Xue ([23]). Por "satisfazer o Teorema Fundamental" entenderemos que "a aplicação de Galois $\theta : H \mapsto R^{\beta_H}$ é bijetiva do conjunto dos subgrupóides amplos H de G no conjunto das subextensões separáveis entre R^β e R".

3.1 Pré-requisitos

Considere R um anel, S um subanel de R com o mesmo elemento identidade e $\beta = (\{E_g\}_{g\in G}, \{\beta_g\}_{g\in G})$ uma ação de um grupóide finito G sobre R.

Para o caso não-comutativo, a definição de extensão β-Galois é a mesma Definição 1.2.1, extraída de [4]. Já o teorema que fornece equivalências da definição de extensão β-Galois fica enunciado da seguinte maneira:

Teorema 3.1.1. [[4], Theorem 5.3] *As seguintes condições são equivalentes:*
(i) R é uma extensão β-galois de R^β.
(ii) R é um R^β-módulo à direita projetivo finitamente gerado e a aplicação j : $R \star_\beta G \longrightarrow End(R)_{R^\beta}$ dada por $j(\sum_{g\in G} a_g u_g)(x) = \sum_{g\in G} a_g \beta_g(x 1_{g^{-1}})$ é um isomorfismo de anéis e de R-módulos à esquerda.
(iii) R é um R^β-módulo à direita projetivo finitamente gerado e para todo $R \star_\beta G$ -módulo à esquerda M, a aplicação $\mu : R \otimes_{R^\beta} M^G \longrightarrow M$ dada por $\mu(x \otimes m) = xm$ é um isomorfismo de R-módulos à esquerda.
(iv) A aplicação $\phi : R \otimes_{R^\beta} R \longrightarrow \prod_{g\in G} E_g$ dada por $\phi(x \otimes y) = (x\beta_g(y1_{g^{-1}}))_{g\in G}$ é um isomorfismo de R-módulos à esquerda.
(v) $RtR = R \star_\beta G$, onde $t = \sum_{g\in G} 1_g u_g$.
(vi) A aplicação $\tau' : R \otimes_{R^\beta} R \longrightarrow R \star_\beta G$ dada por $\tau'(x \otimes y) = \sum_{g\in G} x\beta_g(y1_{g^{-1}})\delta_g$ é sobrejetiva.
(vii) R é um gerador para a categoria dos $R \star_\beta G$-módulos à esquerda.

Observação 3.1.2. *Observe que uma extensão β-Galois de R^β é uma extensão R^β-separável, conforme foi mostrado em [15].*

No que segue, precisaremos das seguintes definições.

Definição 3.1.3. *R é dito uma álgebra de Galois (ou β-Galois) sobre R^β se R é uma extensão β-Galois de R^β tal que R^β está contido no centro $C(R)$ de R. Mais ainda, R é dito uma álgebra de Galois (ou β-Galois) central se R é uma extensão β-Galois do seu centro $C(R)$ (o que implica $C(R) = R^\beta$).*

Definição 3.1.4. *R é dito uma extensão Hirata-separável de S se $R \otimes_S R$ é isomorfo a um somando direto de uma soma finita de R como R-bimódulos.*

Definição 3.1.5. *R é dito uma extensão de Galois Hirata-separável de R^β se é R é uma extensão Hirata-separável e uma extensão β-Galois de R^β.*

Definição 3.1.6. *Dizemos que R é uma álgebra de Azumaya se é uma extensão separável do seu centro.*

Observação 3.1.7. *Note que, pelo que foi definido acima, toda álgebra de Galois central é uma álgebra de Azumaya. Mais ainda, por [22], uma álgebra de Azumaya é uma extensão Hirata-separável. Logo, toda álgebra de Galois central é uma extensão Hirata-separável.*

3.2 Extensões de Galois com Aplicação de Galois Injetiva

Para o que segue neste capítulo, considere que:

- K é um anel comutativo;

- R é uma K-álgebra;

- G é um grupóide finito;

- $\beta = (\{E_g\}_{g \in G}, \{\beta_g\}_{g \in G})$ é uma ação de G sobre R;

- $R = \bigoplus_{e \in G_0} E_e$, onde cada E_e é uma álgebra unitária;

- R é uma extensão β-Galois de R^β;

- $C(R)$ é o centro de R;

- $J_g = \{r \in E_g \mid r\beta_g(x1_{g^{-1}}) = xr$, para todo $x \in R\}$, $g \in G$ (observe que, claramente, J_g é $C(R)$-módulo);

- Para S_1, S_2 subanéis de R, $V_{S_2}(S_1) = \{r \in S_2 \mid rs = sr$, para todo $s \in S_1\}$ é o comutador de S_1 em S_2.

Seja $\mathcal{S}_G = \{g \in G \mid J_g \neq \{0\}\}$ e $\mathcal{T}_G = \{g \in G \mid J_g = \{0\}\}$. Então $G = \mathcal{S}_G \cup \mathcal{T}_G$. Para um subgrupóide H de G, definimos duas aplicações:

(1) $\sigma : H \longrightarrow \{J_h \mid h \in H\}$, onde $\sigma(h) = J_h$; e

(2) $\gamma : \{H \subseteq G \mid H$ é subgrupóide de $G\} \longrightarrow \{M \mid M$ é $C(R)$-módulo$\}$, onde $\gamma(H) = \bigoplus\limits_{h \in H} J_h$.

Veremos agora algumas propriedades de σ e γ que fornecem condições suficientes para que a aplicação de Galois $\theta : H \mapsto R^{\beta_H}$ seja injetiva. Começaremos com um importante lema:

Lema 3.2.1. $V_R(R^\beta) = \bigoplus\limits_{g \in G} J_g$.

Demonstração: Como R é uma extensão β-Galois de R^β, sabemos pelo Teorema 3.1.1 que a aplicação $j : R \star_\beta G \longrightarrow End(R)_{R^\beta}$ dada por $j(\sum\limits_{g \in G} a_g\delta_g)(x) = \sum\limits_{g \in G} a_g\beta_g(x1_{g^{-1}})$ é um isomorfismo de anéis. Seja $A = R \star_\beta G$.

Afirmação 1: $V_A(R) \simeq V_{End(R)_{R^\beta}}(R_l)$ via j, onde $R_l = \{\lambda_l \in End(R)_{R^\beta} \mid \lambda \in R$ e $\lambda_l(r) = \lambda r$ para todo $r \in R\}$.

Primeiro, observe que a aplicação $\psi : R \longrightarrow R \star_\beta G$ dada por $\psi(r) = \sum\limits_{e \in G_0} r1_e\delta_e$ é injetiva, logo podemos identificar R com sua imagem em $R \star_\beta G$. Assim, dado $x \in R$, temos que $j(r)(x) = j(\sum\limits_{e \in G_0} r1_e\delta_e)(x) = \sum\limits_{e \in G_0} r\beta_e(x1_e) = rx\sum\limits_{e \in G_0} 1_e = rx = r_l(x)$, para todo $r \in R$. Logo $j(R) = R_l$. Identificando $R \star_\beta G$ com sua imagem isomórfica $End(R)_{R^\beta}$, temos que a afirmação é válida.

Afirmação 2: $V_{End(R)_{R^\beta}}(R_l) = End_R(R)_{R^\beta}$

$(\subseteq)$ Seja $f \in V_{End(R)_{R^\beta}}(R_l) = \{f \in End(R)_{R^\beta} |\ f \circ \lambda_l = \lambda_l \circ f, \forall \lambda_l \in R_l\}$. Isto implica que $f(r) = f(r1_R) = f \circ r_l(1_R) = r_l \circ f(1_R) = rf(1_R)$, para todo $r \in R$, mostrando que $f \in End_R(R)_{R^\beta}$.

$(\supseteq)$ Sejam $f \in End_R(R)_{R^\beta}$ e $x \in R$. Logo,

$$(f \circ r_l)(x) = f(rx) = rf(x) = (r_l \circ f)(x),$$

para todo $r \in R$.

Afirmação 3: $End_R(R)_{R^\beta} = (V_R(R^\beta))_r$.

$(\subseteq)$ Sejam $f \in End_R(R)_{R^\beta}$ e $x \in R$. Então:

$$f(x) = f(x1_R) = xf(1_R).$$

Agora observe que $f(1) \in V_R(R^\beta)$, pois $f(1)r = f(r) = rf(1)$, para todo $r \in R^\beta$, utilizando nas igualdades que f é R^β-linear à direita e R-linear à esquerda.

$(\supseteq)$ Seja $f \in (V_R(R^\beta))_r$. Isto implica que existe $a \in V_R(R^\beta)$ tal que $f(y) = ya$, para todo $y \in R$. Mais ainda, $a \in V_R(R^\beta)$ implica que $ax = xa$ para todo $x \in R^\beta$. Sejam então $r \in R$ e $x \in R^\beta$. Assim,

$$f(ryx) = ryxa = ryax = rf(y)x.$$

Desta maneira, $f \in End_R(R)_{R^\beta}$.

Por outro lado,

Afirmação 4: $V_A(R) = \bigoplus_{g\in G} J_g\delta_g$.

$(\subseteq)$ Temos que $J_g = \{r \in E_g | r\beta_g(x1_{g^{-1}}) = xr, \forall x \in R\}$. Seja $\sum_{g\in G} r_g\delta_g \in V_A(R)$. Isto implica que $(\sum_{g\in G} r_g\delta_g)x = x(\sum_{g\in G} r_g\delta_g)$ para todo $x \in R$, isto é, $\sum_{g\in G} r_g\beta_g(x1_{g^{-1}})\delta_g = x\sum_{g\in G} r_g\delta_g$. Mas esta soma é direta, logo $r_g\beta_g(x1_{g^{-1}}) = xr_g$ para cada $g \in G$, ou seja, $r_g \in J_g$ para todo $g \in G$.

$(\supseteq)$ Seja $\sum_{g\in G} r_g\delta_g \in \bigoplus_{g\in G} J_g\delta_g$. Logo $r_g\beta_g(x1_{g^{-1}}) = xr_g$ para todo $g \in G$ e para todo $x \in R$. Assim, $\sum_{g\in G} r_g\beta_g(x1_{g^{-1}})\delta_g = \sum_{g\in G} xr_g\delta_g$, ou seja, $(\sum_{g\in G} r_g\delta_g)x = x(\sum_{g\in G} r_g\delta_g)$ para todo $x \in R$, mostrando que $\sum_{g\in G} r_g\delta_g \in V_A(R)$.

Afirmação 5: $\bigoplus_{g\in G} J_g\delta_g \simeq (\bigoplus_{g\in G} J_g)_r$ via j.

Observe que $j(\sum_{g\in G} r_g\delta_g)(x) = \sum_{g\in G} r_g\beta_g(x1_{g^{-1}})$, para todo $r_g \in J_g$. Como $r_g \in J_g$, isto implica que $\sum_{g\in G} r_g\beta_g(x1_{g^{-1}}) = \sum_{g\in G} xr_g = x\sum_{g\in G} r_g = (\sum_{g\in G} r_g)_r(x)$, mostrando que $j(\sum_{g\in G} r_g\delta_g) = (\sum_{g\in G} r_g)_r$.

Juntando as Afirmações 1, 2 e 3, temos que $V_A(R) \simeq (V_R(R^\beta))_r$ via j e pelas Afirmações 4 e 5 temos $V_A(R) \simeq (\bigoplus_{g\in G} J_g)_r$ via j. Assim, $V_R(R^\beta) = \bigoplus_{g\in G} J_g$, completando a demonstração. ■

Lema 3.2.2. *Para qualquer subgrupóide H de G, $\sigma|_{\mathcal{S}_H} : h \mapsto J_h$ de $\mathcal{S}_H$ em $\{J_h \mid h \in \mathcal{S}_H\}$ é injetiva.*

Demonstração: Seja $J_g = J_h$ para $g, h \in \mathcal{S}_H$. Isto implica que $E_g \cap E_h \neq 0$, portanto $r(g) = r(h)$. Como $J_g = J_h \neq \{0\}$, existe $0 \neq r \in E_g = E_h$ tal que $r \in J_g = J_h$ e $xr = r\beta_g(x1_{g^{-1}}) = r\beta_h(x1_{h^{-1}})$ para todo $x \in R$. Assim, $r(\beta_g(x1_{g^{-1}}) - \beta_h(x1_{h^{-1}})) = 0$, para todo $x \in R$. Colocando β_g em evidência, tem-se

$$r\beta_g(x1_{d(g)} - \beta_{g^{-1}h}(x1_{h^{-1}g})) = 0, \text{ para todo } x \in R.$$

Note que $\exists g^{-1}h$, pois $r(g) = r(h)$. Observe também que como $r \in J_g$, $r\beta_g(x1_{g^{-1}}) = xr$ para todo $x \in R$, logo

$$r\beta_g(x1_{d(g)} - \beta_{g^{-1}h}(x1_{h^{-1}g})) = (x - \beta_{g^{-1}h}(x1_{h^{-1}g}))r = 0. \quad (*)$$

Como R é uma extensão β-Galois de R^β, existem elementos $x_i, y_i \in R$, $1 \leq i \leq m$, tais que $\sum_{1\leq i\leq m} x_i\beta_g(y_i1_{g^{-1}}) = \delta_{e,g}1_e$, para todo $e \in G_0$ e $g \in G$. Tomando x como y_i na equação $(*)$, obtemos $(y_i 1_{d(g)} - \beta_{g^{-1}h}(y_i 1_{h^{-1}g}))r = 0$. Assim, $x_i(y_i - \beta_{g^{-1}h}(y_i 1_{h^{-1}g}))r = 0$, para $1 \leq i \leq m$, logo $\sum_{i=1}^{m} x_i(y_i - \beta_{g^{-1}h}(y_i 1_{h^{-1}g}))r = 0$, concluindo que

$$(\sum_{i=1}^{m} x_i y_i)r = \sum_{i=1}^{m} x_i \beta_{g^{-1}h}(y_i 1_{h^{-1}g})r.$$

Desta forma,

$$\begin{aligned} r &= 1_{r(g)}r = (\sum_{i=1}^{m} x_i \beta_{r(g)}(y_i 1_{r(g)}))r = (\sum_{i=1}^{m} x_i y_i 1_{r(g)})r \\ &= (\sum_{i=1}^{m} x_i y_i)r = \sum_{i=1}^{m} x_i \beta_{g^{-1}h}(y_i 1_{h^{-1}g})r = \delta_{e,g^{-1}h} 1_e r, \end{aligned}$$

para todo $e \in G_0$. Note que $r \neq 0$, portanto $g^{-1}h = r(g^{-1}h) = r(g^{-1}) = d(g)$. Então temos $g^{-1}h = d(g)$, o que implica que $gg^{-1}h = gd(g)$, isto é, $r(g)h = gd(g)$. Utilizando que $r(g) = r(h)$, conclui-se que $h = r(h)h = r(g)h = gd(g) = g$. Isto prova que $\sigma|_{\mathcal{S}_H}$ é injetiva. ■

Para os próximos resultados, precisaremos da seguinte definição.

Definição 3.2.3. *Seja H um subconjunto de G. Definimos o subgrupóide gerado pelos elementos de H como sendo o menor subgrupóide de G que contém H. Usaremos a notação $< H >$ para tal subgrupóide.*

Lema 3.2.4. *Sejam H e L subgrupóides de G tais que $J_h \neq \{0\}$ para cada $h \in H$ e $J_l \neq \{0\}$ para cada $l \in L$. Considere $\theta : H \mapsto R^{\beta_H}$ a aplicação de Galois. Se $\theta(H) = \theta(L)$, então $H = L$.*

Demonstração: Como $\theta(H) = \theta(L)$, $R^{\beta_H} = R^{\beta_L}$. Seja $< H, L >$ o subgrupóide gerado pelos elementos em H e L.

Afirmação: $R^{\beta_{<H,L>}} = R^{\beta_H} = R^{\beta_L}$.

De fato, $R^{\beta_{<H,L>}} \subseteq R^{\beta_H}$ é óbvio, pois $H \subseteq < H, L >$. Vejamos a outra inclusão. Sejam $r \in R^{\beta_H} = R^{\beta_L}$ e $hl \in < H, L >$ tais que $h \in H$, $l \in L$ e $d(h) = r(l)$. Então

$$\beta_{hl}(r 1_{l^{-1}h^{-1}}) = \beta_h(\beta_l(r 1_{l^{-1}}) 1_{h^{-1}}) = \beta_h(r 1_l 1_{h^{-1}}) = r 1_{lh}.$$

Desta maneira, $r \in R^{\beta_{<H,L>}}$.

Portanto temos que R é uma extensão $\beta_{<H,L>}$-Galois de $R^{\beta_{<H,L>}} = R^{\beta_H} = R^{\beta_L}$. Então, pelo Lema 3.2.1, $\bigoplus_{g \in <H,L>} J_g = \bigoplus_{h \in H} J_h = \bigoplus_{l \in L} J_l$, já que $R^{\beta_{<H,L>}} = R^{\beta_H} = R^{\beta_L}$ implica que $V_R(R^{\beta_{<H,L>}}) = V_R(R^{\beta_H}) = V_R(R^{\beta_L})$.

Por hipótese, $J_g \neq \{0\}$ para cada $g \in H \cup L$, logo $\bigoplus_{g \in <H,L>} J_g = \bigoplus_{h \in H} J_h$ implica que $L \subseteq H$, já que são somas diretas e, sendo assim, têm que possuir a mesma quantidade de somandos diretos. Similarmente, $H \subseteq L$. Assim, $H = L$. ■

Lema 3.2.5. *Se R é uma extensão Hirata separável de R^β, então $J_{g^{-1}} J_g = V_{E_g}(R)$ para todo $g \in G$. Mais ainda, para quaisquer $g, h \in G$, $J_h J_g = J_{gh}$ e cada J_g é um $V_{E_g}(R)$-progerador de posto 1.*

Demonstração: Por [22], Definition 1, dizer que R é uma extensão Hirata separável de R^β é equivalente a dizer que, para cada $g \in G$, a aplicação

$$\upsilon_g : V_R(R^\beta) \otimes_{C(R)} M^R \longrightarrow M^{R^\beta}$$

definida por $\upsilon_g(d \otimes m) = dm$, $d \in V_R(R^\beta), m \in M$, onde M é um (R,R)-bimódulo e $M^R = \{m \in M | xm = mx, \quad \forall x \in R\}$, é um isomorfismo de $C(R)$-módulos.

Observe que de R podemos obter um (R,R)-bimódulo R_g de forma que $R_g = R$ como R-módulo à esquerda, mas como R-módulo à direita a ação é dada por:

$$x.y = x\beta_g(y1_{g^{-1}}),$$

para $x, y \in R$. Desta maneira, $J_g = (R_g)^R$ e $V_R(R^\beta) = (R_g)^{R^\beta}$.

Temos então, diretamente da definição de extensão Hirata separável, que a aplicação $\upsilon_g : V_R(R^\beta) \otimes_{C(R)} J_g \longrightarrow V_R(R^\beta)$ definida por $\upsilon_g(d \otimes d_g) = dd_g$, onde $d \in V_R(R^\beta)$ e $d_g \in J_g$, é um isomorfismo de $C(R)$-módulos.

Pelo Lema 3.2.1, $V_R(R^\beta) = \bigoplus_{g \in G} J_g$, então $V_R(R^\beta) J_g \simeq V_R(R^\beta) \otimes_{C(R)} J_g \simeq V_R(R^\beta)$ implica que $V_R(R^\beta) = \bigoplus_{h \in G} J_h J_g \subseteq \bigoplus_{d(h)=r(g)} J_{gh} = \bigoplus_{r(l)=r(h)} J_l 1_h = \bigoplus_{l \in G} J_l 1_h \subseteq \sum_{l \in G} J_l =$

$V_R(R^\beta)$. Note que $J_hJ_g \subseteq J_{gh}$ para $g, h \in G$ tais que $d(g) = r(h)$, pois para $r_h \in J_h$ e $r_g \in J_g$, temos

$$xr_hr_g = r_h\beta_h(x1_{h^{-1}})r_g = r_hr_g\beta_g(\beta_h(x1_{h^{-1}})1_{g^{-1}}) = r_hr_g\beta_{gh}(x1_{h^{-1}g^{-1}}).$$

Concluímos então que $J_hJ_g = J_{gh}$. Em particular, $J_{g^{-1}}J_g = J_{r(g)} = V_{E_g}(R)$.

Como $J_{g^{-1}}J_g = V_{E_g}(R)$, cada elemento de $J_{g^{-1}}$ pode ser pensado como um elemento de $Hom_{V_{E_g}}(J_g,\ V_{E_g}(R))$. Com efeito, podemos visualizar este fato na seguinte afirmação:

Afirmação 1: $J_{g^{-1}} \simeq Hom_{V_{E_g}(R)}(J_g, V_{E_g}(R)) = J_g^*$.

Este isomorfismo é dado pela aplicação

$$\begin{array}{rcl} \varphi \ : \ J_{g^{-1}} & \longrightarrow & Hom_{V_{E_g}(R)}(J_g, V_{E_g}(R)) \\ x & \longmapsto & \varphi_x : J_g \longrightarrow V_{E_g}(R), \quad onde \quad \varphi_x(y) = yx, \end{array}$$

e é fácil verificar que sua inversa é dada por

$$\begin{array}{rcl} \varphi^{-1} \ : \ Hom_{V_{E_g}(R)}(J_g, V_{E_g}(R)) & \longrightarrow & J_{g^{-1}} \\ f & \longmapsto & \displaystyle\sum_{i=1}^{n} f(x_i)y_i. \end{array}$$

Seja $1 = \displaystyle\sum_{i=1}^{n} x_iy_i$ com $x_i \in J_g$ e $y_i \in J_{g^{-1}}$. Então $\{x_i, y_i\}_{1 \leq i \leq n}$ formam uma base dual de J_g sobre $V_{E_g}(R)$, já que $x = \displaystyle\sum_i x_iy_ix$ para todo $x \in J_g$. Desta maneira, J_g é um $V_{E_g}(R)$-módulo projetivo finitamente gerado, ou seja, um $V_{E_g}(R)$-progerador (para mais detalhes, veja as equivalências de módulos projetivos finitamente gerados em [20]).

Afirmação 2: $V_{E_g}(R) \simeq End_{V_{E_g}(R)}(J_g)$.

Neste caso, a aplicação é definida por

$$\begin{array}{rcl} \psi \ : \ V_{E_g}(R) & \longrightarrow & End_{V_{E_g}(R)}(J_g) \\ x & \longmapsto & \psi_x : J_g \longrightarrow J_g, \quad onde \quad \psi_x(y) = yx, \end{array}$$

e a inversa é dada por

$$\begin{array}{rcl} \psi^{-1} \ : \ End_{V_{E_g}(R)}(J_g) & \longrightarrow & V_{E_g}(R) \\ f & \longmapsto & \sum_{i=1}^{n} f(x_i)y_i. \end{array}$$

Então

$$V_{E_g}(R) \simeq End_{V_{E_g}(R)}(J_g) \simeq J_g \otimes_{V_{E_g}(R)} J_g^* \simeq J_g \otimes_{V_{E_g}(R)} J_{g^{-1}}.$$

Como $V_{E_g}(R)$ é $V_{E_g}(R)$-módulo de posto 1, segue que $J_g \otimes_{V_{E_g}(R)} J_{g^{-1}}$ tem posto 1, e portanto J_g tem posto 1, já que $rank_{V_{E_g}(R)}(J_g \otimes_{V_{E_g}(R)} J_{g^{-1}}) = rank(J_g).rank(J_{g^{-1}})$ (veja mais detalhes em [20]), concluindo a demonstração. ■

O próximo teorema fornece uma condição suficiente para que a aplicação de Galois seja injetiva.

Teorema 3.2.6. *Se $J_g \neq 0$ para cada $g \in G$, então a aplicação de Galois θ, definida do conjunto dos subgrupóides de G no conjunto das subextensões de R sobre R^β, é injetiva.*

Demonstração: Por hipótese, $J_g \neq 0$ para cada $g \in G$. Logo, pelo Lema 3.2.4, θ é injetiva. ■

Uma aplicação deste teorema pode ser vista no seguinte corolário:

Corolário 3.2.7. *Se R é uma extensão β-Galois Hirata separável, ou uma álgebra de Galois central, então θ é injetiva.*

Demonstração: Para qualquer extensão β-Galois Hirata separável, temos pelo Lema 3.2.5 que J_g é um $V_{E_g}(R)$-módulo projetivo de posto 1 para cada $g \in G$. Logo $J_g \neq \{0\}$ para cada $g \in G$. Assim, θ é injetiva pelo Teorema 3.2.6. Como toda álgebra de Galois central é uma extensão Hirata-separável (veja a Observação 3.1.7), segue que θ é injetiva também nesse caso. ■

Com as notações anteriores, considere $\gamma : H \mapsto \bigoplus_{h\in H} J_h$.

Lema 3.2.8. *Seja H um subgrupóide amplo de G. Então $\gamma(H)$ é uma subálgebra de R sobre $C(R)$ e $\gamma(H) = V_R(R^{\beta_{\mathcal{S}_H}})$, onde $R^{\beta_{\mathcal{S}_H}} = \{r \in R \mid \beta_h(r1_{h^{-1}}) = r1_h$ para cada $h \in \mathcal{S}_H\}$.*

Demonstração: Como R é uma extensão β-Galois de R^β, R é uma extensão β_H-Galois de R^{β_H}, e o raciocínio para mostrar tal afirmação é o mesmo mostrado no Teorema 1.3.1, ressaltando que $G_0 = H_0$, logo $R = \bigoplus_{e\in G_0} E_e = \bigoplus_{e\in H_0} E_e$. Desta maneira, $V_R(R^{\beta_H}) = \bigoplus_{h\in H} J_h$, pelo Lema 3.2.1. Mas $J_h = \{0\}$ para cada $h \in \mathcal{T}_H$, logo $\gamma(H) = \bigoplus_{h\in\mathcal{S}_H} J_h = V_R(R^{\beta_H})$.

Observando que $C(R) \subseteq V_R(R^{\beta_H})$, temos que $\gamma(H)$ é uma subálgebra de R sobre $C(R)$. Mais ainda, como $\mathcal{S}_H \subseteq H$, $R^{\beta_H} \subseteq R^{\beta_{\mathcal{S}_H}}$. Desta maneira, $V_R(R^{\beta_{\mathcal{S}_H}}) \subseteq V_R(R^{\beta_H}) = \gamma(H)$.

Reciprocamente, queremos $\gamma(H) \subseteq V_R(R^{\beta_{\mathcal{S}_H}})$. De fato, para cada $r \in J_h$, onde $h \in \mathcal{S}_H$, $r\beta_h(x1_{h^{-1}}) = xr$ para todo $x \in R$, em particular para todo $x \in R^{\beta_{\mathcal{S}_H}}$. Disto segue que $rx = xr$ para todo $x \in R^{\beta_{\mathcal{S}_H}}$, concluindo que $J_h \subseteq V_R(R^{\beta_{\mathcal{S}_H}})$ para cada $h \in \mathcal{S}_H$. Portanto, $\bigoplus_{h\in\mathcal{S}_H} J_h \subseteq V_R(R^{\beta_{\mathcal{S}_H}})$. Como $\gamma(H) = \bigoplus_{h\in\mathcal{S}_H} J_h$, segue que $\gamma(H) \subseteq V_R(R^{\beta_{\mathcal{S}_H}})$. Logo $\gamma(H) = V_R(R^{\mathcal{S}_H})$. ∎

Teorema 3.2.9. *Seguindo as notações do Lema 3.2.8, se a aplicação γ é injetiva do conjunto dos subgrupóides amplos H de G no conjunto das $C(R)$-subálgebras de R, então não existem subgrupóides próprios entre $\mathcal{S}_H$ e H para qualquer subgrupóide amplo H de G. Particularmente, ou $\mathcal{S}_H$ é um subgrupóide de G, ou $H =< \mathcal{S}_H >$, o subgrupóide gerado pelos elementos em $\mathcal{S}_H$.*

Demonstração: Primeiro observe que se $G_0 \subseteq H$, então $G_0 \subseteq \mathcal{S}_H$, pois $J_e = V_{E_e}(R) \neq \emptyset$, já que $1_e \in V_{E_e}(R)$, para todo $e \in G_0$. Agora suponha que exista um subgrupóide próprio H' entre $\mathcal{S}_H$ e H. Então $\mathcal{S}_H \subset H' \subset H$; portanto $R^{\beta_H} \subseteq$

$R^{\beta_{H'}} \subseteq R^{\beta_{S_H}}$ e por conseguinte, $V_R(R^{\beta_H}) \subseteq V_R(R^{\beta_{H'}}) \subseteq V_R(R^{\beta_{S_H}})$.

Pelo Lema 3.2.1, $\gamma(H) = V_R(R^{\beta_H})$ e pelo Lema 3.2.8, $\gamma(H) = V_R(R^{\beta_{S_H}})$, logo $\gamma(H) = V_R(R^{\beta_{H'}})$. Isto implica que $V_R(R^{\beta_{H'}}) = V_R(R^{\beta_H})$, concluindo que $\gamma(H') = \gamma(H)$. Mas $H' \neq H$ e γ é injentiva por hipótese, o que gera uma contradição. ■

Definição 3.2.10. *Dizemos que R satisfaz a propriedade do duplo centralizador para um subanel A de R se $V_R(V_R(A)) = A$.*

O próximo teorema, encontrado em [9], mostra que toda $C(R)$-álgebra de Azumaya R satisfaz a propriedade do duplo centralizador para qualquer subálgebra separável S sobre $C(R)$.

Teorema 3.2.11. [[9], Theorem 4.3] *Considere S uma anel comutativo, R uma S-álgebra separável central e suponha que A é uma subálgebra de R que contém S. Então $V_R(A)$ é uma subálgebra separável de R e $V_R(V_R(A)) = A$. Se A é central, então $V_R(A)$ também o é, e a aplicação de S-álgebras $A \otimes V_R(A) \longrightarrow R$ dada por $a \otimes r \mapsto ar$ é um isomorfismo.*

Teorema 3.2.12. *Ainda com as mesmas notações do Lema 3.2.8, se R satisfaz a propriedade do duplo centralizador para R^{β_H} para cada subgrupóide H de G, então γ é injetiva se, e somente se, θ é injetiva.*

Demonstração: Como $\gamma(H) = \bigoplus_{h \in H} J_h = V_R(R^{\beta_H}) = V_R(\theta(H)) = (V_R \circ \theta)(H)$ para cada subgrupóide H de G, temos que $\gamma = V_R \circ \theta$, onde neste caso estamos considerando V_R como sendo a aplicação que leva cada subanel de R no seu comutador.

($\Leftarrow$) Assuma θ injentiva e R satisfazendo a propriedade do duplo centralizador para R^{β_H}. Suponha $\gamma(H) = \gamma(L)$, para H, L subgrupóides de G. Então $(V_R \circ \theta)(H) = (V_R \circ \theta)(L)$, isto é, $V_R(R^{\beta_H}) = V_R(R^{\beta_L})$. Assim, $V_R(V_R(R^{\beta_H})) = V_R(V_R(R^{\beta_L}))$. Aplicando a propriedade do duplo centralizador, temos $R^{\beta_H} = R^{\beta_L}$, ou seja, $\theta(H) =$

$\theta(L)$. Como θ é injetiva, obtemos $H = L$.

$(\Rightarrow)$ Se γ é injetiva, então V_R e θ também são. ■

Finalizamos esta seção caracterizando quando dois subgrupóides H e L de G são tais que $\gamma(H) = \gamma(L)$.

Teorema 3.2.13. *Assuma que, para cada subgrupóide F de G, R satisfaz a propriedade do duplo centralizador para R^{β_F}. Então para quaisquer dois subgrupóides H e L de G, as seguintes condições são equivalentes:*

(1) $\gamma(H) = \gamma(L)$;

(2) $\theta(H) = \theta(L)$;

(3) $J_g = \{0\}$ para cada $g \in < H, L > -(H \cap L)$.

Demonstração: (1) $\Rightarrow$ (2) Seja $\gamma(H) = \gamma(L)$ para subgrupóides H, L de G. Então $V_R(R^{\beta_H}) = \bigoplus_{h\in H} J_h = \gamma(H) = \gamma(L) = \bigoplus_{l\in L} J_l = V_R(R^{\beta_L})$. Logo $V_R(V_R(R^{\beta_H})) = V_R(V_R(R^{\beta_L}))$. Como R satisfaz a propriedade do duplo centralizador para R^{β_H} e para R^{β_L}, concluímos que $R^{\beta_H} = R^{\beta_L}$, ou seja, $\theta(H) = \theta(L)$.

(2) $\Rightarrow$ (1) Como foi visto na demonstração do Teorema 3.2.12, $\gamma = V_R \circ \theta$. Desta maneira, $\gamma(H) = V_R(\theta(H)) = V_R(\theta(l)) = \gamma(L)$.

(2) $\Rightarrow$ (3) Por hipótese, $\theta(H) = \theta(L)$, isto é, $R^{\beta_H} = R^{\beta_L}$. Seja $< H, L >$ o subgrupóide gerado pelos elementos em H e L. Então, como foi visto na demonstração do Lema 3.2.4,

$$\bigoplus_{g\in<H,L>} J_g = \bigoplus_{h\in H} J_h = \bigoplus_{l\in L} J_l.$$

Observando que $H \subseteq < H, L >$, temos que $\bigoplus_{g\in<H,L>} J_g = \bigoplus_{h\in H} J_h$ implica que $J_g = 0$ para cada $g \in < H, L > -H$. Similarmente, $\bigoplus_{g\in<H,L>} J_g = \bigoplus_{l\in L} J_l$ implica que $J_g = 0$ para cada $g \in < H, L > -L$. Ou seja, $J_g = 0$ para cada $g \in < H, L > -(H \cap L)$.

(3) $\Rightarrow$ (1) Como $J_g = \{0\}$ para cada $g \in < H, L > -(H \cap L)$, $\bigoplus\limits_{g \in H \cap L} J_g = \bigoplus\limits_{g \in <H,L>} J_g = \bigoplus\limits_{h \in H} J_h = \bigoplus\limits_{l \in L} J_l$. Logo $\gamma(H) = \gamma(L)$. ∎

3.3 Sobre Álgebras de Galois que satisfazem o Teorema Fundamental

Por toda essa seção, vamos assumir que R é uma álgebra de Galois sobre R^β e, para um subanel S de R, $H_S = \{g \in G |\ \beta_g(s1_{g^{-1}}) = s1_g, \forall s \in S\}$.

Considere R uma R^β-álgebra β-Galois central, S uma subálgebra separável de R e $S' = V_R(S)$. Vamos mostrar algumas propriedades de uma álgebra β-Galois central que satisfaz o Teorema Fundamental. Lembre que por "satisfazer o Teorema Fundamental"entendemos que "a aplicação de Galois $\theta : H \mapsto R^{\beta_H}$ é bijetiva dos subgrupóides amplos de G nas subálgebras R^β-separáveis de R".

Teorema 3.3.1. *Suponha que R é uma álgebra β-Galois central sobre R^β. Se R satisfaz o Teorema Fundamental, então para qualquer subálgebra R^β-separável S, $V_R(S) = \bigoplus\limits_{g \in H_S} J_g$ e $S = \bigoplus\limits_{g \in H_{S'}} J_g$.*

Demonstração: Como S é uma subálgebra separável de R e R satisfaz o Teorema Fundamental, $S = R^{\beta_{H_S}}$. Logo R é uma extensão β_{H_S}-Galois de S. Então $V_R(S) = V_R(R^{\beta_{H_S}}) = \bigoplus\limits_{g \in H_S} J_g$, pelo Lema 3.2.1.

Mais ainda, pela Observação 3.1.7, R é uma álgebra de Azumaya. Assim, aplicando o Teorema 3.2.11, temos que $S' = V_R(S)$ é uma R^β-subálgebra separável de R tal que $V_R(S') = V_R(V_R(S)) = S$. Sendo S' uma R^β-subálgebra separável de R, tem-se $S' = R^{\beta_{H_{S'}}}$, logo R é uma extensão $\beta_{H_{S'}}$-Galois de S'. Isto implica que $S = V_R(S') = V_R(R^{\beta_{H_{S'}}}) = \bigoplus\limits_{g \in H_{S'}} J_g$, pelo Lema 3.2.1. ∎

Lema 3.3.2. *Seja H um subgrupóide de G. Se R é uma R^{β}-álgebra separável, então R é uma R^{β_H}-álgebra separável.*

Demonstração: Considere a aplicação

$$\begin{array}{rcl} \varphi \ : \ R \times R & \longrightarrow & R \otimes_{R^{\beta_H}} R \\ (r,s) & \longmapsto & r \otimes_{R^{\beta_H}} s \end{array}$$

Afirmação 1: φ é R^{β}-balanceada.

De fato, $\varphi(\lambda r, s) = \lambda r \otimes_{R^{\beta_H}} s = r \otimes_{R^{\beta_H}} \lambda s = \varphi(r, \lambda s)$, para todo $\lambda \in R^{\beta}$ e $r, s \in R$. A segunda igualdade segue do fato que $R^{\beta} \subseteq R^{\beta_H}$.

Afirmação 2: φ é aditiva.

$\varphi(r_1 + r_2, s) = (r_1 + r_2) \otimes_{R^{\beta_H}} s = (r_1 \otimes_{R^{\beta_H}} s) + (r_2 \otimes_{R^{\beta_H}} s) = \varphi(r_1, s) + \varphi(r_2, s)$, para todo $r_1, r_2, s \in R$.

Analogamente, $\varphi(r, s_1 + s_2) = \varphi(r, s_1) + \varphi(r, s_2)$, para todo $r, s_1, s_2 \in R$.

Assim, pela propriedade universal do produto tensorial (para mais detalhes, veja [18], pg 7), existe

$$\begin{array}{rcl} \overline{\varphi} \ : \ R \otimes_{R^{\beta}} R & \longrightarrow & R \otimes_{R^{\beta_H}} R \\ r \otimes_{R^{\beta}} s & \longmapsto & r \otimes_{R^{\beta_H}} s \end{array}$$

tal que $\overline{\varphi} \circ f = \varphi$, onde $f : R \times R \longrightarrow R \otimes_{R^{\beta}} R$ é aditiva e R^{β}-balanceada. Observe que $\overline{\varphi}$ é R-linear.

Por hipótese, R é R^{β}-separável, logo existe um idempotente $e = \sum_i a_i \otimes_{R^{\beta}} b_i \in R \otimes_{R^{\beta}} R$ tal que $er = re$ para todo $r \in R$ e $\sum a_i b_i = 1_R$. Considere $e' = \overline{\varphi}(e) = \sum_i a_i \otimes_{R^{\beta_H}} b_i \in R \otimes_{R^{\beta_H}} R$. Assim,

$$e'r = \overline{\varphi}(e)r = \overline{\varphi}(er) = \overline{\varphi}(re) = r\overline{\varphi}(e) = re',$$

para todo $r \in R$, e $\sum a_i b_i = 1_R$, mostrando que R é R^{β_H}-separável. ■

O próximo teorema é a recíproca do Teorema 3.3.1.

Teorema 3.3.3. *Suponha que R é uma R^β-álgebra β-Galois central. Se para qualquer subálgebra separável S de R, $V_R(S) = \bigoplus_{g\in H_S} J_g$, então R satisfaz o Teorema Fundamental.*

Demonstração: Como R é uma álgebra β-Galois central, a aplicação $\theta : H \mapsto R^{\beta_H}$ é injetiva, pelo Corolário 3.2.7. Além disso, como R é R^β-separável, segue que R é R^{β_H}-separável, pelo Lema 3.3.2.

Agora seja S uma subálgebra separável de R. Então pelo Teorema 3.2.11, $S' = V_R(S)$ também é uma subálgebra separável de R tal que $V_R(S') = V_R(V_R(S)) = S$. Por outro lado, R é uma extensão β_{H_S}-Galois de $R^{\beta_{H_S}}$ com grupóide de Galois H_S, logo $V_R(R^{\beta_{H_S}}) = \bigoplus_{g\in H_S} J_g$, pelo Lema 3.2.1. Desta maneira, $V_R(S) = \bigoplus_{g\in H_S} J_g = V_R(R^{\beta_{H_S}})$. Mais ainda, como H_S é um subgrupóide de G, R é $R^{\beta_{H_S}}$-separável, pelo Lema 3.3.2. Portanto, pelo Teorema 3.2.11,

$$S = V_R(V_R(S)) = V_R(V_R(R^{\beta_{H_S}})) = R^{\beta_{H_S}}.$$

Isto implica que a aplicação $\theta : H \mapsto R^{\beta_H}$ é sobrejetiva, completando a demonstração. ■

Para encerrar este capítulo, combinando os Teoremas 3.3.1 e 3.3.3, fornecemos uma caracterização de uma álgebra β-Galois central que satisfaz o Teorema Fundamental.

Teorema 3.3.4. *Suponha R uma R^β-álgebra β-Galois central. Então R satisfaz o Teorema Fundamental se, e somente se, para qualquer R^β-subálgebra separável S de R, $V_R(S) = \bigoplus_{g\in H_S} J_g$.*

Referências Bibliográficas

[1] M. F. Atiyah; I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley series in Mathematics, 1969.

[2] D. Bagio; W. Cortes; M. Ferrero; A. Paques, *Actions of Inverse Semigroups on Algebras*, Comm. Algebra 35 (2007), 3865-3874.

[3] D. Bagio; D. Flôres; A. Paques, *Partial Actions of Ordered Groupoids on rings*, J. Algebra Appl., Vol 9, nº 3 (2010), 501-517.

[4] D. Bagio; A. Paques, *Partial groupoid actions: globalization, Morita theory and Galois theory*, to appear in Comm. Algebra (2012).

[5] H. Brandt, *Über eine Verallgemeinerung des Gruppenbegriffes*, Math. Ann. 96 (1926) 360-366.

[6] R. Brown, *From Groups to Groupoids: a brief survey*, Bull. London Math. Soc. 19 (1987) 113-134.

[7] R. Brown, *Groupoids and Van Kampen's Theorem*, Bull. London Math. Soc. (3) 17 (1967) 385-401.

[8] S. Chase; D. K. Harrison; A. Rosenberg, *Galois Theory and Galois Cohomology of Commutative Rings*, Mem. AMS 52 (1968), 1-19.

[9] F. Demeyer; E. Ingraham, *Separable Algebras over Commutative Rings*, Springer Verlag, Berlin, Heidelberg, New York, LNM vol 181 (1971).

[10] M. Dokuchaev; M. Ferrero; A. Paques, *Partial Actions and Galois Theory*, Journal of Pure and Applied Algebra 208 (2007) 77-87.

[11] M. Dokuchaev; R. Exel, *Associativity of Crossed Products by Partial Actions, Enveloping Actions and Partial Representations*, Trans. Amer. Math. Society 357 (5) (2005), 1931-1952.

[12] A. Dress, *One More Shortcut to Galois Theory*, Adv. Math. 110 (1995), 129-140.

[13] R. Exel, *Partial Actions of Groups and Actions of Semigroups*, Proc. AMS 126 (1998), 3481-3494.

[14] M. Ferrero; A. Paques, *Galois Theory of Commutative Rings Revisited*, Beiträge zur Algebra und Geometrie, 38 (1997), nº2, 399-410.

[15] D. Flôres, *Tese de Doutorado* (2011).

[16] T. Kanzaki, *On Galois Algebra Over a Commutative Ring*, Osaka J. Math., 2 (1965), 309-317.

[17] M. A. Knus; M. Ojanguren, *Théorie de la Descente et Algèbres d'Azumaya*, Lecture Notes in Math. 389, Springer-Verlag (1974).

[18] G. Karpilovsky, *The Algebraic Structure of Crossed Products*, Elsevier Science Publisher B. V. (1987).

[19] M. V. Lawson, *Inverse Semigroups. The Theory of Partial Symmetries*, World Scientific Pub. Co, London (1998).

[20] B. R. McDonald, *Linear Algebra over Commutative Rings*, Pure and Applied Mathematics, 87 (1984).

[21] A. Paques, *Teorias de Galois*, XXII Brazilian Algebra Meeting (2012).

[22] K. Sugano, *On a Special Type of Galois Extensions*, Hokkaido Math. Journal, 9 (1980) 123-128.

[23] G. Szeto; L. Xue, *On Galois Algebras Satisfying the Fundamental Theorem*, Comm. Algebra, 35(12) (2007), 238-246.

[24] G. Szeto; L. Xue, *On Galois Extensions with a One-to-One Galois Map*, International Journal of Algebra, Vol. 5, nº17 (2011), 801-807.

[25] O. E. Villamayor; D. Zelinsky, *Galois Theory for Rings with Finitely Many Idempotents*, Nagoya Math. J. 27 (1966) 721-731.

[26] O. E. Villamayor; D. Zelinsky, *Galois Theory for Rings with Infinitely Many Idempotents*, Nagoya Math. J. 35 (1969) 83-98.