UNIVERSIDADE FEDERAL DO PARANÁ

Willian Valverde

Álgebra Parcial de Grupo

Curitiba, 2016.

UNIVERSIDADE FEDERAL DO PARANÁ

Willian Valverde

Álgebra Parcial de Grupo

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Paraná, como requisito parcial à obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Marcelo Muniz Silva Alves.

Curitiba

Fevereiro de 2016

V215a Valverde, Willian
Álgebra parcial de grupo / Willian Valverde. – Curitiba, 2016.
94 f. ; 30 cm.

Dissertação - Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Matemática, 2016.

Orientador: Marcelo Muniz Silva Alves .
Bibliografia: p. 93-94.

1. Álgebra. 2. Estruturas algébricas ordenadas. 3. Grupos quânticos. I. Universidade Federal do Paraná. II.Alves, Marcelo Muniz Silva. III. Título.

CDD: 512

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
Setor CIÊNCIAS EXATAS
Programa de Pós Graduação em MATEMÁTICA
Código CAPES: 40001016041P1

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em MATEMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **WILLIAN VALVERDE**, intitulada: "**Álgebra Parcial de Grupo**", após terem inquirido o aluno e realizado a avaliação do trabalho, são de parecer pela sua APROVAÇÃO.

Curitiba, 29 de Fevereiro de 2016.

Prof MARCELO MUNIZ SILVA ALVES (UFPR)
(Presidente da Banca Examinadora)

Prof ELIEZER BATISTA (UFSC)

Prof MARI SANO (UTFPR)

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
Setor CIÊNCIAS EXATAS
Programa de Pós Graduação em MATEMÁTICA
Código CAPES: 40001016041P1

ATA DE SESSÃO PÚBLICA DE DEFESA DE DISSERTAÇÃO PARA A OBTENÇÃO DO GRAU DE MESTRE EM MATEMÁTICA

No dia vinte e nove de Fevereiro de dois mil e dezesseis às 09:30 horas, na sala Anfiteatro B, Blocos das PCs, Coordenação PPGMA, Centro Politécnico, UFPR, do Setor de CIÊNCIAS EXATAS da Universidade Federal do Paraná, foram instalados os trabalhos de arguição do mestrando **WILLIAN VALVERDE** para a Defesa Pública de sua Dissertação intitulada: "**Álgebra Parcial de Grupo**". A Banca Examinadora, designada pelo Colegiado do Programa de Pós-Graduação em MATEMÁTICA da Universidade Federal do Paraná, foi constituída pelos seguintes Professores Doutores: MARCELO MUNIZ SILVA ALVES (UFPR), ELIEZER BATISTA (UFSC), MARI SANO (UTFPR). Dando início à sessão, a presidência passou a palavra ao discente, para que o mesmo expusesse seu trabalho aos presentes. Em seguida, a presidência passou a palavra a cada um dos Examinadores, para suas respectivas arguições. O aluno respondeu a cada um dos arguidores. A presidência retomou a palavra para suas considerações finais e, depois, solicitou que os presentes e o mestrando deixassem a sala. A Banca Examinadora, então, reuniu-se sigilosamente e, após a discussão de suas avaliações, decidiu-se pela ...APROVAÇÃO... do aluno. O mestrando foi convidado a ingressar novamente na sala, bem como os demais assistentes, após o que a presidência fez a leitura do Parecer da Banca Examinadora, outorgando-lhe o Grau de **Mestre em MATEMÁTICA**. Nada mais havendo a tratar a presidência deu por encerrada a sessão, da qual eu, MARCELO MUNIZ SILVA ALVES, lavrei a presente ata, que vai assinada por mim e pelos membros da Comissão Examinadora.

Curitiba, 29 de Fevereiro de 2016.

Prof MARCELO MUNIZ SILVA ALVES (UFPR)
(Presidente da Banca Examinadora)

Eliezer Batista

Prof ELIEZER BATISTA (UFSC)

Mari Sano

Prof MARI SANO (UTFPR)

Agradecimentos

Agradeço primeiramente ao professor Marcelo, por ser muito mais que um professor e orientador, por ser um verdadeiro amigo. Teve paciência comigo, acreditou em mim e me ajudou em todos os momentos. Se não fosse por ele eu sequer teria entrado no programa de mestrado, quanto menos teria chegado até aqui.

Agradeço à minha esposa Izabelle pela paciência, incentivo e sacrifício que fez junto a mim.

Aos meus pais Osni e Marilete e meu irmão Lucca, pela força que sempre me deram, esforço, compreensão e por perdoarem minhas falhas.

Ao programa de Pós-Graduação em Matemática da UFPR pela oportunidade e aos professores que me ajudaram nesse período, bem como a todos os professores que ajudaram na minha trajetória.

Aos amigos de pós-graduação e graduação que me ajudaram, incentivaram e motivaram de alguma forma.

À May (minha cachorra), pela companhia e carinho nesta reta final.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior pelo apoio financeiro.

E aos professores da banca, por atender ao pedido do professor Marcelo e dedicarem seu tempo ao meu trabalho.

” Você não sabe o quanto eu caminhei

Pra chegar até aqui

Percorri milhas e milhas antes de dormir

Eu nem cochilei

Os mais belos montes escalei

Nas noites escuras de frio chorei (...)”

A Estrada - Cidade Negra

(Da Gama e Toni Garrido)

Resumo

Sendo G um grupo e K um anel, abordaremos o conceito de álgebra parcial do grupo G, denotada por $K_{par}(G)$, que é a K-álgebra associada às representações parciais de G sobre K e é uma ferramenta bastante fina para dizer quando dois grupos não são isomorfos. Mostraremos uma construção de $K_{par}(G)$ por meio de um grupoide denotado por $\Gamma(G)$ e faremos detalhadamente a construção das componentes conexas de $\Gamma(S_3)$, a fim de calcularmos $K_{par}(S_3)$. Também apresentaremos o cálculo das álgebras parciais $\mathbb{C}_{par}(S_3)$, $\mathbb{C}_{par}(\mathbb{Z}_p \times \mathbb{Z}_p)$ e $\mathbb{C}_{par}(\mathbb{Z}_{p^2})$. Para compreender melhor este assunto, apresentaremos o Semigrupo de Exel $S(G)$, que é um monóide inverso cujas ações em um conjunto X estão em correspondência biunívoca com ações parciais de G em X. Além do mais, temos que a álgebra de semigrupo $KS(G)$, que é semissimples, é isomorfa à $K_{par}(G)$.

Palavras-chave: Álgebra parcial de grupo; Semigrupo inverso; Ação parcial de grupo.

Abstract

Let G be a group and K be a ring. In this work we study the partial group algebra of G, denoted by $K_{par}(G)$, which is the algebra associated to partial representations of G over K and is a refined tool to tell when two groups are not isomorphic. We present a construction of $K_{par}(G)$ by means of a groupoid denoted by $\Gamma(G)$. We present in detail the description of $K_{par}(S_3)$ via construction of the connected components of the groupoid $\Gamma(S_3)$. We also present the calculation of the partial group algebras $\mathbb{C}_{par}(S_3)$, $\mathbb{C}_{par}(\mathbb{Z}_p \times \mathbb{Z}_p)$ and $\mathbb{C}_{par}(\mathbb{Z}_{p^2})$. In order to better understand this issue, we present the Exel Semigroup $S(G)$, which is an inverse monoid whose actions in a set X are in one-one correspondence with partial actions of G in X. Moreover, the algebra semigroup $KS(G)$ (that is semisimple) is isomorphic to $K_{par}(G)$.

Keywords: Partial group algebra; Inverse semigroup; Partial group actions.

Sumário

Introdução

O objetivo central do trabalho é descrever o que vem a ser a álgebra parcial de um grupo G dado. Esta álgebra é denotada por $K_{par}(G)$, onde K é um anel comutativo com unidade, e foi apresentada inicialmente em $[4]$ por Dokuchaev, Exel e Piccione.

A álgebra parcial de grupo faz parte de uma série de trabalhos que vem sendo desenvolvidos recentemente na área de Álgebra após a apresentação do conceito de *ação parcial* por Exel na década de 90. Uma de suas aplicações é identificar quando dois grupos não são isomorfos. Ou seja, se, dados dois grupos G e H, suas respectivas álgebras parciais $K_{par}(G)$ e $K_{par}(H)$ não são isomorfas, então G e H também não são.

No entanto, a importância do estudo das álgebras parciais não se resume somente a conhecer uma ferramenta mais fina para identificar quando dois grupos não são isomorfos. A álgebra parcial $K_{par}(G)$ é isomorfa a álgebra do Semigrupo de Exel $S(G)$. O Semigrupo de Exel (ou Monóide de Exel) é, na verdade um semigrupo definido por geradores G e relações iguais às que definem a álgebra parcial $K_{par}(G)$, logo tratam-se, em suas essências, do mesmo objeto matemático. Em especial, a importância de $S(G)$ é que suas ações em um conjunto X, estão em correspondência biunívoca com ações parciais de G no mesmo conjunto.

No primeiro capítulo, apresentamos um breve estudo a respeito de semigrupos, em especial semigrupos inversos. Um semigrupo inverso é um caso particular de um semigrupo regular. Um semigrupo regular é um semigrupo S em que, para cada $s \in S$ existe um elemento $s^* \in S$ tal que

$$ss^*s = s \text{ e } s^*ss^* = s^*.$$

A diferença do semigrupo regular para o semigrupo inverso é que, no segundo caso, o elemento s^* precisa ser único.

No capítulo 2, vemos que $S(G)$ é um semigrupo inverso e também vemos o já mencionado resultado que ações de $S(G)$, estão em correspondência biunívoca com ações parciais de G. Nesse capítulo também vemos a construção de grupo e semigrupo livre, deixando claro,

assim, que $S(G)$ é, de fato, um semigrupo.

Neste mesmo capítulo, construimos a álgebra de um grupo e de um monóide, além de apresentar resultados importantes a respeito da semissimplicidade da álgebra de um grupo finito, como os teoremas de Wedderburn-Artin e de Molien, que serão importantes para melhor compreensão do capítulo 3.

O capítulo 3, último do trabalho, além de apresentar a definição de álgebra parcial de grupo e resultados teóricos que a relacionam com o Semigrupo de Exel, apresentamos uma construção equivalente por meio de um grupoide específico, o grupoide $\Gamma(G)$, cuja álgebra $K\Gamma(G)$ é isomorfa à álgebra parcial $K_{par}(G)$. Esta construção é vital para compreender resultados a respeito da álgebra parcial e, por meio do grafo associado ao grupoide, apresentar uma fórmula recursiva para o cálculo de $K_{par}(G)$. Com detalhes, apresentamos o grafo, por meio de suas componentes conexas, do grupoide $\Gamma(S_3)$.

Para finalizar, calculamos alguns exemplos de álgebra parcial de grupo, em especial, $\mathbb{C}_{par}(S_3)$, $\mathbb{C}_{par}(\mathbb{Z}_p \times \mathbb{Z}_p)$ e $\mathbb{C}_{par}(\mathbb{Z}_{p^2})$.

Capítulo 1

Semigrupos

Neste capítulo, apresentarmos um pouco da teoria básica a respeito de semigrupos e, em especial, semigrupos inversos. A importância desse capítulo se dá para compreender melhor o Semigrupo de Exel, que será definido no capítulo seguinte. Como principais referências nos baseamos em [5], [8] e [10].

1.1 Semigrupos

Definição 1.1 *Um conjunto não vazio S munido de uma operação binária*

$$\begin{aligned} * : \quad S \times S &\longrightarrow S \\ (s_1, s_2) &\longmapsto s_1 * s_1 \end{aligned}$$

*é um **semigrupo** se tal operação for associativa, ou seja, se*

$$(s_1 * s_2) * s_3 = s_1 * (s_2 * s_3)$$

para todos $s_1, s_2, s_3 \in S$.

*Além disso, se existe $1_S \in S$, chamado **elemento neutro**, tal que*

$$1_S * s = s * 1_S = s$$

*para todo $s \in S$, dizemos que S é um **monóide**.*

*Se , para todo $s_1, s_2 \in S$, temos $s_1 * s_2 = s_2 * s_1$, dizemos que S é um **semigrupo comutativo**.*

Notação 1.2 *Podemos denotar o semigrupo cujo conjunto é S e operação $*$ por $(S, *)$ quando se fizer necessário explicitar o conjunto e operação.*

Obs. 1.3 *i) Quando não houver risco de confusão, podemos denotar* $s_1 * s_2$ *por* $s_1.s_2$ *ou simplesmente* s_1s_2*, fazendo referência à multiplicação, operação comum nos exemplos de semigrupos.*

ii) 1 *é único. De fato, suponha que existam* $1, 1' \in S$ *que são elementos neutros.*

Como $1 \in S$*, usando o fato que* $1'$ *é elemento neutro, temos* $1 = 11'$*. Como* $1' \in S$*, usando o fato que* 1 *é elemento neutro, temos* $11' = 1'$*. Por transitividade,* $1 = 1'$*.*

Exemplo 1.4 *Sejam* G *um grupo e* $1_G \in G$ *o elemento neutro de* G*. Considere* P_{1_G} *o conjunto de todos os subconjuntos finitos de* G *que contém o elemento* 1_G*. Isto é,*

$$P_{1_G} = \{H \subseteq G : |H| < \infty, 1_G \in H\}$$

Defina $\tilde{G}^R = \{(A, g) \in P_{1_G} \times G : g \in A\}$.
Então, $\tilde{G}^R$ *é um monóide com respeito à operação:*

$$(A, g)(B, h) = (A \cup gB, gh)$$

De fato, para mostrar a associatividade considere $(A, g), (B, h), (C, i) \in \tilde{G}^R$

$$\begin{aligned}((A, g)(B, h))(C, i) =&(A \cup gB, gh)(C, i) = ((A \cup gB) \cup ghC, (gh)i)\\ =&(A \cup (gB \cup ghC), g(hi)) = (A \cup g(B \cup hC), g(hi))\\ =&(A, g)(B \cup hC, hi) = (A, g)((B, h)(C, i))\end{aligned}$$

O elemento neutro de $\tilde{G}^R$ *é* $(\{1_G\}, 1_G)$*. Com efeito, considere* $(A, g) \in \tilde{G}^R$*, então*

$$(\{1_G\}, 1_G)(A, g) = (\{1_G\} \cup 1_G A, 1_G g) = (A, g).$$

Também,

$$(A, g)(\{1_G\}, 1_G) = (A \cup g\{1_G\}, g1_G) = (A, g).$$

O semigrupo $\tilde{G}^R$ *é chamado de* ***expansão de Birget-Rhodes do grupo*** G*. Veja* [2] *e* [13].

Definição 1.5 *Seja* S *um semigrupo. Um subconjunto* T*, não vazio, de* S *é dito um* ***subsemigrupo*** *de* S *se é fechado com respeito à operação de* S*. Ou seja, se* $s_1, s_2 \in T$*, então* $s_1s_2 \in T$*.*

Definição 1.6 *Seja* e *um elemento pertencente a algum semigrupo* S*. Então* e *é um* ***idempotente*** *se* $e^2 = e$*, onde* e^2 *denota* ee*.*

Obs. 1.7 *O conceito de idempotente estende-se a qualquer conjunto com alguma operação definida e não somente a semigrupos.*

Um fato interessante a ser observado é que em um grupo G, o único idempotente é o elemento neutro 1_G. De fato, se e é um idempotente de G, então

$$e^2 = e \Rightarrow (ee)e^{-1} = ee^{-1} \Rightarrow e(ee^{-1}) = ee^{-1} \Rightarrow e1_G = 1_G \Rightarrow e = 1_G.$$

Já se estivermos trabalhando com um monóide, podemos ter idempotentes diferentes do elemento neutro. Por exemplo, no caso do monóide $\tilde{G}^R$, seus idempotentes são elementos (A, g) tais que $(A, g)^2 = (A, g)$, mas

$$(A, g)^2 = (A, g) \Leftrightarrow (A, g)(A, g) = (A, g) \Leftrightarrow (A \cup gA, g^2) = (A, g)$$

o que ocorre se, e somente se, $A \cup gA = A$ e $g^2 = g$.

Observe que a segunda igualdade só é válida se $g = 1_G$, por ser G um grupo, logo seu único idempotente é 1_G. Com isso, tendo $g = 1_G$, a igualdade $A \cup gA = A$ é válida também. Então, os idempotentes de $\tilde{G}^R$ são da forma $(A, 1_G)$.

1.2 Semirreticulados

Definição 1.8 *Seja Y um subconjunto de um conjunto parcialmente ordenado $(X, \leq)$. Dizemos que $c \in X$ é **limitante inferior** de Y se $c \leq y$ para todo $y \in Y$. E dizemos que $d \in X$ é o **maior limitante inferior** ou **ínfimo** de Y se $d \geq c$ para todo c limitante inferior.*

Observe que, caso exista, o ínfimo de um conjunto é, claramente, único.

Notação 1.9 *$\wedge\{y : y \in Y\}$ denota o ínfimo de Y. $a \wedge b$ denota o ínfimo de $\{a, b\}$.*

Definição 1.10 *Um conjunto parcialmente ordenado $(X, \leq)$ é dito **semirreticulado inferior** se $a \wedge b$ existe para todo $a, b \in X$.*

Exemplo 1.11 ?? *Considere o conjunto dos idempotentes de $\tilde{G}^R$ e a relação parcial de ordem dada por $(A, 1_G) \leq (B, 1_G) \Leftrightarrow A \subseteq B$. Assim $(A, 1_G) \wedge (B, 1_G) = (A \cap B, 1_G)$ e este conjunto é um semirreticulado inferior.*

Note que, se X é um semirreticulado inferior, temos

$$a \leq b \Leftrightarrow a \wedge b = a,$$

com isso, $\wedge$ define, em $(X, \leq)$ semirreticulado inferior, uma operação binária. Então, dados $a, b, c \in X$,

- $(a \wedge b) \wedge c \leq a \wedge b \leq a$
- $(a \wedge b) \wedge c \leq a \wedge b \leq b$
- $(a \wedge b) \wedge c \leq c$.

Logo, $(a \wedge b) \wedge c$ é limitante inferior de $\{a, b, c\}$.

Seja d limitante inferior de $\{a, b, c\}$. Então, $d \leq a$, $d \leq b$ e $d \leq c$. O que implica que $d \leq a \wedge (b \wedge c)$ e, portanto, $a \wedge (b \wedge c)$ é o ínfimo de $\{a, b, c\}$.

Da mesma forma, temos que $(a \wedge b) \wedge c$ é o ínfimo de $\{a, b, c\}$. Como o ínfimo é único, temos $a \wedge (b \wedge c) = (a \wedge b) \wedge c$, o que implica que $(X, \wedge)$ é semigrupo.

Proposição 1.12 *Seja $(E, \leq)$ um semirreticulado inferior. Então, $(E, \wedge)$ é um semigrupo comutativo de idempotentes e para todo $a, b \in E$ temos*

$$a \leq b \Leftrightarrow a \wedge b = a.$$

Seja $(E, \cdot)$ um semigrupo comutativo de idempotentes. Então, a relação $\leq$ em E definida por

$$a \leq b \Leftrightarrow ab = a$$

é ordem parcial em E com respeito a qual E é um semirreticulado inferior. Em $(E, \leq)$, o ínfimo de a e b é seu produto ab.

Prova: Para provar a primeira parte, primeiro observe que já provamos que $(E, \wedge)$ é semigrupo. Que é um semigrupo comutativo basta observar que a igualdade $a \wedge b = b \wedge a$ é imediata da igualdade dos conjuntos $\{a, b\} = \{b, a\}$.

Os elementos de $(E, \wedge)$ são idempotentes uma vez que $a \leq a$ implica que $a \wedge a = a$. Resta, portanto, verificar que $a \leq b \Leftrightarrow a \wedge b = a$.

Para mostrar que $a \leq b \Rightarrow a \wedge b = a$, observe que de $a \leq a$ e $a \leq b$, segue que $a \leq a \wedge b$. Suponha que $a \wedge b = d$. Então, $a \leq a \wedge b = d$ e, como $d = a \wedge b$, segue da definição de ínfimo que $d \leq a$. Logo $a = d$.

Já para mostra que $a \wedge b = a \Rightarrow a \leq b$ basta notar que de $a \wedge b = a$ segue que $a \leq a$ e $a \leq b$.

Para a segunda parte do teorema, vejamos que a relação $a \leq b \Leftrightarrow ab = a$ define uma ordem parcial em E.

- $aa = a \Rightarrow a^2 = a \Rightarrow a \leq a$
- $a \leq b \Rightarrow ab = a$ e $b \leq a \Rightarrow ab = b$. Portanto $a = b$
- Por um lado, $a \leq b \Rightarrow ab = a \Rightarrow abc = ac$. Por outro lado, $b \leq c \Rightarrow bc = b \Rightarrow abc = ab$. Então, $a = ab = abc = ac \Rightarrow a = ac \Rightarrow a \leq c$.

E, por fim, vejamos que $(E \leq)$ é um semirreticulado inferior cujo ínfimo de $\{a, b\}$ é ab.

- ab é limitante inferior de $\{a, b\}$:

$$(ab)a = a^2b = ab \Rightarrow ab \leq a$$

$$(ab)b = ab^2 = ab \Rightarrow ab \leq b$$

- Suponha $c \leq a, b$, então $ca = c$ e $cb = c$, o que implica $cab = c$ e, potanto, $c \leq ab$.

□

Observe que a ordem definida no exemplo no semigrupo dos idempotentes de $\tilde{G}^R$ é exatamente a ordem estabelecida nesta proposição.

1.3 Semigrupos Regulares e Semigrupos Inversos

Definição 1.13 *Um semigrupo S é um **semigrupo regular** se, para cada $s \in S$, existe $s^* \in S$ tal que*

$$ss^*s = s \text{ e } s^*ss^* = s^*.$$

*O elemento s^* é chamado **inverso** de s em S.*

Teorema 1.14 *Seja S um semigrupo regular. Então, os idempotentes de S comutam entre si se, e somente se, cada elemento de S possui um único inverso.*

Prova: Para mostrar a primeira parte do teorema, suponha $s \in S$ idempotente e $x, y \in S$ inversos de s em S. Então,

$$(xs)^2 = (xs)(xs) = x(sxs) = xs.$$

Analogamente, $(ys)^2 = ys$. Então xs e ys são idempotentes (também de maneira análoga sx e sy são idempotentes). Portanto, comutam entre si. Com isso:

$$x = xsx = x(sys)x = (xs)(ys)x = (ys)(xs)x = y(sxs)x = ysx =$$

$$= y(sys)x = y(sy)(sx) = y(sx)(sy) = y(sxs)y = ysy = y.$$

Já para mostrar a segunda parte do teorema, suponha que cada $s \in S$ possui um único inverso. Sejam e, f idempotentes de S. Antes, observe que se e é idempotente, então $e^* = e$ pela unicidade do inverso, já que um idempotente sempre é um inverso de si mesmo.

- $f(ef)^*e$ é idempotente: $(f(ef)^*e)(f(ef)^*e) = f((ef)^*ef(ef)^*)e = f(ef)^*e$.
- $f(ef)^*e$ e ef são inversos:

  $$f(ef)^*e(ef)f(ef)^*e = f(ef)^*(ee)(ff)(ef)^*e = (f(ef)^*e)(f(ef)^*e) = f(ef)^*e$$

  $$(ef)(f(ef)^*e)(ef) = e(ff)f(ef)^*(ee)f = eff(ef)^*eef = ef(ef)^*ef = ef$$

  $\Rightarrow f(ef)^*e = (ef)^*$.

  Como $f(ef)^*e$ é idempotente e $f(ef)^*e = (ef)^*$, temos que $(ef)^*$ é idempotente. Logo ef é idempotente.

  Da mesma maneira, podemos mostrar que fe é idempotente e daí segue que

  $$(ef)(fe)(ef) = e(ff)(ee)f = (ef)(ef) = ef$$

  $$(fe)(ef)(fe) = f(ee)(ff)e = (fe)(fe) = fe$$

  Portanto, $ef = fe$ pela unicidade do inverso.

□

Definição 1.15 *Um semigrupo S é um **semigrupo inverso** se existe, para cada $s \in S$, um único elemento $s^* \in S$ tal que*

$$ss^*s = s \text{ e } s^*ss^* = s^*$$

*O elemento s^* é o **inverso** de s em S.*

Obs. 1.16 *Semigrupo inverso é um semigrupo regular cujos idempotentes comutam. Um grupo é um caso particular de semigrupo inverso.*

Exemplo 1.17 *$\tilde{G}^R$ é um monóide inverso.*

Já mostramos que $\tilde{G}^R$ é monóide. Resta verificar que é inverso. Para isso, dado $(A, g) \in \tilde{G}^R$, vejamos quem é $(A, g)^*$. Denote $(A, g)^*$ por (B, h):

- $(A, g)(B, h)(A, g) = (A, g) \Leftrightarrow (A \cup gB \cup ghA, ghg) = (A, g)$

  De $ghg = g$, segue que $h = g^{-1}$, o que implica $ghA = gg^{-1}A = 1_G A = A$. Logo, $A \cup gB \cup ghA = A \cup gB$.

  Então $A \cup gB = A \Leftrightarrow gB \subseteq A$.

- $(B, g^{-1})(A, g)(B, g^{-1}) = (B, g^{-1}) \Leftrightarrow (B \cup g^{-1}A \cup B, g^{-1}) = (B, g^{-1})$

  O que ocorre se, e somente se, $g^{-1}A \subseteq B \Leftrightarrow A \subseteq gB$.

  Portanto, temos $B = g^{-1}A$ e $(A, g)^* = (g^{-1}A, g^{-1})$.

Notação 1.18 *$E(S)$ denota o conjunto dos idempotentes do semigrupo inverso S.*

Note que $E(S)$ é subsemigrupo de S uma vez que, para $e, f \in E(S)$, temos $(ef)^2 = e^2 f^2 = ef$.

Exemplo 1.19 *Seja $\mathscr{I}(X)$ o conjunto de todas as bijeções entre subconjuntos de X e defina a função $\emptyset$ como sendo a "bijeção" entre o subconjunto vazio de X nele mesmo. Considere o produto entre $\alpha, \beta \in \mathscr{I}(X)$ como sendo a composição $\alpha \circ \beta$ definida da seguinte forma:*

$$\alpha \circ \beta : \beta^{-1}(im\beta \cap dom\alpha) \longrightarrow \alpha(im\beta \cup dom\alpha)$$

Se $im\beta \cap dom\alpha = \emptyset$, então $\alpha \circ \beta = \emptyset$. Observe que, desta forma, o produto está bem definido.

Tal operação é associativa:

$$\begin{aligned}
dom(\alpha \circ (\beta \circ \gamma)) =& (\beta \circ \gamma)^{-1}(im(\beta \circ \gamma) \cap dom\alpha) \\
=& (\beta \circ \gamma)^{-1}(\beta(im\gamma \cap dom\beta) \cap dom\alpha) \\
=& (\gamma^{-1} \circ \beta^{-1})((\beta im\gamma \cap \beta dom\beta) \cap dom\alpha) \\
=& \gamma^{-1}((\beta^{-1}\beta im\gamma \cap \beta^{-1} im\beta) \cap \beta^{-1} dom\alpha) \\
=& \gamma^{-1}((im\gamma \cap \beta^{-1} im\beta) \cap \beta^{-1} dom\alpha) \\
=& \gamma^{-1}(im\gamma \cap \beta^{-1}(im\beta \cap dom\alpha)) \\
=& \gamma^{-1}(im\gamma \cap dom(\alpha \circ \beta)) \\
=& dom((\alpha \circ \beta) \circ \gamma)
\end{aligned}$$

Como a composição de funções definidas num mesmo domínio é associativa, segue que $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

Vejamos quais são os idempotentes de $\mathscr{I}(X)$. *Seja* $\alpha \in \mathscr{I}(X)$,

$$\alpha^2 = \alpha \circ \alpha : \alpha^{-1}(im\alpha \cap dom\alpha) \longrightarrow \alpha(im\alpha \cap dom\alpha)$$

Então, $\alpha^2 = \alpha$ *se, e somente se,*

$$\alpha^{-1}(im\alpha \cap dom\alpha) = dom\alpha$$

e

$$\alpha(im\alpha \cap dom\alpha) = im\alpha.$$

O que ocorre se, e somente se, $im\alpha \subseteq dom\alpha$ *e* $dom\alpha \subseteq im\alpha$. *Portanto, precisamos ter* $dom\alpha = im\alpha$.

Além do mais, $\alpha^2(x) = \alpha(x) \Leftrightarrow \alpha^{-1}\alpha^2(x) = \alpha^{-1}\alpha(x) \Leftrightarrow \alpha(x) = x$ *para todo* $x \in dom\alpha$.

Assim, os idempotentes de $\mathscr{I}(X)$ *são identidades locais* Id_A *para subconjuntos* A *de* X.

Observe que $Id_A \circ Id_B = Id_{A\cap B} = Id_{B\cap A} = Id_B \circ Id_A$. *Logo, os idempotentes de* $\mathscr{I}(X)$ *comutam e* $\mathscr{I}(X)$ *é monóide inverso.*

Proposição 1.20 *Seja* S *um semigrupo inverso. Então, para todo* $a, b \in S$ *e* $e \in E(S)$, *temos*

i) $(a^*)^* = a$

ii) $e^* = e$

iii) $aa^*, a^*a \in E(S)$

iv) $(ab)^* = b^*a^*$

v) $aea^*, a^*ea \in E(S)$

vi) Para todo $e \in E(S)$ *e para todo* $s \in S$, *existe* $f \in E(S)$ *tal que* $es = sf$

vii) Para todo $e \in E(S)$ *e para todo* $s \in S$, *existe* $f \in E(S)$ *tal que* $se = fs$

Prova:

i) Imediato

ii) Imediato

iii) $(aa^*)aa^* = (aa^*a)a^* = aa^*$

$(a^*a)a^*a = (a^*aa^*)a = a^*a$

iv) $(ab)(b^*a^*)(ab) = a(bb^*)(a^*a)b = (aa^*a)(bb^*b) = ab$

$(b^*a^*)(ab)(b^*a^*) = b^*(a^*a)(bb^*)a^* = (b^*bb^*)(a^*aa^*) = b^*a^*$

v) $(aea^*)(aea^*) = ae(a^*a)ea^* = a(a^*a)eea^* = aea^*$

$(a^*ea)(a^*ea) = (a^*aa^*)eea = a^*ea$

vi) Tome $f = s^*es$

$sf = s(s^*es) = (ss^*)es = e(ss^*s) = es$

vii) Tome $f = ses^*$

$fs = (ses^*)s = se(s^*s) = (ss^*s)e = se$

□

Corolário 1.21 *Sejam $\alpha_1, \alpha_2, ..., \alpha_n$ elementos de um semigrupo inverso S. Então $(\alpha_1\alpha_2...\alpha_n)^* = \alpha_n^*...\alpha_2^*\alpha_1^*$.*

Prova: Provaremos por indução nos subíndices maiores ou igual a 2 de α. Para $n = 2$ o resultado é válido pela proposição anterior.

Suponhamos que o resultado é válido para o subíndice n.

$$(\alpha_1\alpha_2...\alpha_n\alpha_{n+1})^* = ((\alpha_1\alpha_2...\alpha_n)\alpha_{n+1})^* =$$

$$= \alpha_{n+1}^*(\alpha_1\alpha_2...\alpha_n)^* = \alpha_{n+1}^*\alpha_n^*...\alpha_2^*\alpha_1^*$$

□

Proposição 1.22 *Sejam S um semigrupo inverso, T um semigrupo e $\varphi : S \to T$ um homomorfismo. Então, $\varphi(S)$ é semigrupo inverso.*

Prova: Para mostrar esta proposição, primeiramente mostraremos que $\varphi(S)$ é um semigrupo regular. Depois provaremos que os idempotentes comutam. Assim, podemos utilizar o teorema **??** para concluir a prova.

- Seja $\varphi(s) \in \varphi(S)$, então

$$\varphi(s^*) = \varphi(s^*ss^*) = \varphi(s^*)\varphi(s)\varphi(s^*)$$

$$\varphi(s) = \varphi(ss^*s) = \varphi(s)\varphi(s^*)\varphi(s).$$

  Portanto, $\varphi(s)^* = \varphi(s^*)$.

- Sejam $\varphi(s), \varphi(t) \in E(\varphi(S))$. Então, pelo lema anterior, podemos supor s e t idempotentes, e

$$\varphi(s)\varphi(t) = \varphi(st) = \varphi(ts) = \varphi(t)\varphi(s).$$

  Assim, os idempotentes de $\varphi(S)$ comutam e, pelo teorema **??**, $\varphi(S)$ é um semigrupo inverso.

□

Lema 1.23 *Sejam S e T semigrupos inversos e $\varphi : S \to T$ um homomorfismo. Então, idempotentes de $\varphi(S)$ são imagens de idempotentes de S.*

Prova: Seja $e \in E(\varphi(S))$, então $\varphi^{-1}(\{e\})$ é subsemigrupo inverso de S.

De fato, sejam $a, b \in \varphi^{-1}(\{e\})$, então $\varphi(ab) = \varphi(a)\varphi(b) = e^2 = e$.

Seja $a \in \varphi^{-1}(\{e\})$, então $a^* \in \varphi^{-1}(\{e\})$. Com efeito, $e = \varphi(a) = \varphi(aa^*a) = \varphi(a)\varphi(a^*)\varphi(a) = e\varphi(a^*)e$ e $\varphi(a^*) = \varphi(a^*aa^*) = \varphi(a^*)e\varphi(a^*)$. Da unicidade do inverso em T, tem-se $\varphi(a^*) = e^* = e$.

Então, $aa^*, a^*a \in \varphi^{-1}(\{e\})$, com aa^*, a^*a idempotentes. Portanto, $\varphi(aa^*) = \varphi(a^*a) = e$. □

Lema 1.24 *Seja S um semigrupo inverso. Então $aS = aa^*S$ para todo $a \in S$ e aa^* é o único idempotente gerador de aS.*

Prova: Seja $a \in S$, então $aS = aa^*aS \subseteq aa^*S \subseteq aS$, o que implica $aS = aa^*S$.

Seja e idempotente tal que $aS = eS$, então $aa^*S = aS = eS$, o que implica $aa^* \in eS$. Então, $aa^* = es_1$ para algum $s_1 \in S$. Além do mais, temos $e \in aa^*S$, o que implica $e = aa^*s_2$ para algum $s_2 \in S$.

Portanto, $aa^* = es_1 = e(es_1) = e(aa^*) = (aa^*)e = (aa^*)(aa^*s_2) = (aa^*)s_2 = e$. □

Obs. 1.25 *Um resultado análogo vale para $Sa = Sa^*a$ para todo $a \in S$ com a^*a gerador.*

Lema 1.26 *Se e, f são idempotentes de um semigrupo inverso S então $eS \cap fS = efS$.*

Prova: Como e, f comutam, temos $efS \subset eS \cap fS$, pois se a está em efS, então $a = efr$ para algum r em S, $a = e(fr) \in eS$, $a = efr = f(er) \in fS$. Reciprocamente, se $a \in eS \cap fS$, então existem r e s em S tais que $a = er = fs$. Segue que $a = ea$, pois $ea = e^2r = er = a$ e, portanto, $a = ea = efs \in efS$. □

Teorema 1.27 ***(de Representação de Wagner-Preston)*** *Seja S um semigrupo inverso. Então, existe um conjunto X e um homomorfismo injetivo $\rho : S \to \mathscr{I}(X)$.*

Prova: Considere $X = S$ enquanto conjunto e, para cada $a \in S$ defina $\rho_a : a^*aS \to aa^*S$ por $\rho_a(x) = ax$. Note que, a função ρ_a está bem definida, pois para $s \in S$, $\rho_a(a^*as) = aa^*as \in aa^*S$.

Além do mais, ρ_a é uma bijeção, cuja inversa ρ_a^{-1} é ρ_{a^*}. De fato,

$$\rho_a \circ \rho_{a^*}(aa^*s) = \rho_a(a^*aa^*s) = \rho_a(a^*s) = aa^*s$$

e

$$\rho_{a^*} \circ \rho_a(a^*as) = \rho_{a^*}(aa^*as) = \rho_{a^*}(as) = a^*as.$$

Agora, defina $\rho : S \to \mathscr{I}(X)$ por $\rho(a) = \rho_a$. Então, ρ é homomorfismo. Com efeito, sejam $a, b \in S$, então

$$\begin{aligned} dom(\rho_a \circ \rho_b) =& \rho_b^{-1}(a^*aS \cap bb^*S) \\ =& \rho_{b^*}(bb^*a^*aS) = b^*bb^*a^*aS \\ =& b^*a^*aS = (b^*a^*a)(b^*a^*a)^*S \\ =& b^*a^*aa^*abS = b^*a^*abS = (ab)^*abS \\ =& dom\rho_{ab} \end{aligned}$$

além do mais, $\rho_a \circ \rho_b(x) = \rho_a(bx) = abx = \rho_{ab}(x)$.

Também temos que ρ é injetora: suponha $\rho_a = \rho_b$.

$$dom\rho_a = dom\rho_b \Rightarrow a^*aS = b^*bS$$

o que implica, pela unicidade do gerador, que $a^*a = b^*b$.

Em particular, para $x = b^*$, tem-se

$$\rho_a(b^*) = ab^*$$

$$\rho_b(b^*) = bb^*$$

Daí,

$$b = bb^*b = \rho_b(b^*b) = \rho_a(b^*b) = ab^*b = aa^*a = a.$$

□

Proposição 1.28 *Grupos são, precisamente, os semigrupos inversos com um único idempotente.*

Prova: Grupos são, claramente, semigrupos inversos com um único idempotente.

Seja S um semigrupo inverso e e seu único idempotente. Como, para todo $s \in S$, $s^*s = e = ss^*$, o que implica que $s^* = s^{-1}$ para todo $s \in S$.

Além do mais,

$$es = (ss^*)s = s$$

$$se = s(s^*s) = s,$$

Então, e é o elemento neutro do grupo e a associatividade vem imediatamente da associatividade em S. Logo, S é um grupo. □

1.4 Equivalência e Congruência

Definição 1.29 *Seja R uma relação binária em um conjunto não vazio X. Definimos a relação **inversa** por $R^{-1} = \{(x, y) \in X \times X : (y, x) \in R\}$.*

*Se R_1, R_2 são duas relações binárias em X, definimos a relação **composta** $R_1 \circ R_2 = \{(x, y) \in X \times X : (\exists z \in X : (x, z) \in R_2, (z, y) \in R_1)\}$*

Obs. 1.30 *Dada uma relação R qualquer em um conjunto não vazio X, define-se as potências R^n de R recursivamente:*

i) $R^0 = 1_X = \{(x, x) : x \in X\}$

ii) $R^1 = R$

iii) $R^{n+1} = R^n \circ R$

Definição 1.31 *Dada R uma relação qualquer, definimos o* ***fecho transitivo*** *de R por*

$$R^\infty = \bigcup_{n=1}^{\infty} R^n.$$

Lema 1.32 *Se R é uma relação em um conjunto X, então R^∞ é a menor relação transitiva em X que contém R.*

Prova: Primeiro vejamos que R^∞ é transitiva. Sejam $(x, y), (y, z) \in R^\infty$, então existem $n, m \in \mathbb{N}$ tais que $(x, y) \in R^n$ e $(y, z) \in R^m$. Assim, por definição $(x, z) \in R^m \circ R^n = R^{n+m} \subseteq R^\infty$.

Agora, seja T uma relação transitiva em X que contém R. Assim,

$$R^2 = R \circ R \subseteq T \circ T \subseteq T,$$

Então, $R^n \subseteq T$ para todo $n \geq 1$, o que implica $R^\infty \subseteq T$. □

Proposição 1.33 *Se R é uma relação em um conjunto X e R^e é a menor relação de equivalência em X que contém R, então*

$$R^e = [R \cup R^{-1} \cup 1_X]^\infty$$

Prova: Para que a relação R^e seja reflexiva e simétrica, deve conter 1_X e $R \cup R^{-1}$, além do próprio R, e a menor relação transitiva que contém $R \cup R^{-1} \cup 1_X$ é, pelo lema anterior, $[R \cup R^{-1} \cup 1_X]^\infty$. □

Corolário 1.34 *Se R é uma relação em um conjunto X e R^e é a menor relação de equivalência em X que contém R, então $(x, y) \in R^e$ se, e somente se, ou $x = y$ ou, para algum $b \in \mathbb{N}$, existe uma sequência*

$$x = z_1 \to z_2 \to ... \to z_n = y$$

em que, para cada $i = 1, 2, ..., n-1$, ou $(z_i, z_{i+1}) \in R$ ou $(z_{i+1}, z_i) \in R$.

Prova: Basta observar que esta é apenas uma reescrita da proposição anterior. □

Definição 1.35 *Seja ρ uma relação de equivalência. Definimos a ρ-**classe** ou **classe de equivalência** de x como sendo o conjunto*

$$\rho x = \{y \in X : (x, y) \in \rho\}$$

*Também definimos o conjunto **quociente** de X por ρ como sendo*

$$X/\rho = \{\rho x : x \in X\}$$

*e a **sobrejeção natural** pela função*

$$\begin{array}{rccc} \rho^\natural : & X & \longrightarrow & X/\rho \\ & x & \longmapsto & \rho x \end{array}$$

Proposição 1.36 *Seja X um conjunto. Uma relação binária $\rho \subseteq X \times X$ é relação de equivalência se:*

i) $1_X = \{(x, x) \in X \times X : x \in X\} \subseteq \rho$

ii) $\rho^{-1} = \rho$

iii) $\rho \circ \rho = \rho$.

Prova: Basta observar que cada propriedades de relação de equivalência é obtidas diretamente de cada item da proposição. □

Proposição 1.37 *Se f é uma função com domínio em um conjunto X, então $f^{-1} \circ f$ é uma relação de equivalência em X.*

Prova: Observe que

$$\begin{aligned} f^{-1} \circ f &= \big\{(x, y) \in X \times X : (\exists z \in X : (x, z) \in f, (z, y) \in f^{-1})\big\} \\ &= \{(x, y) \in X \times X : (\exists z \in X : (x, z) \in f, (y, z) \in f)\} \\ &= \{(x, y) \in X \times X : f(x) = f(y)\} \end{aligned}$$

Daí, se torna óbvio que $f^{-1} \circ f$ é reflexiva, transitiva e simétrica. □

Definição 1.38 *O **núcleo** de uma função f, denotado por $Ker(f)$, é a composição $f^{-1} \circ f$.*

Obs. 1.39 *Esta definição de núcleo, generaliza a definição usual de núcleo de um homomorfismo de grupos. De fato, sejam G e H dois grupos e $f : G \to H$ um homomorfismo. Temos, pela definição anterior, que*

$$Ker(f) = \{(x, y) \in G \times G : f(x) = f(y)\}$$

Daí, como f é homomorfismo, segue que $(x, y) \in Ker(f) \Leftrightarrow f(xy^{-1}) = 1_H$ e, deste modo, (x, y) pertence a $Ker(f)$ se, e somente se, xy^{-1} pertence ao conjunto

$$N = \{z \in G : f(z) = 1_H\},$$

que é o núcleo de f como homomorfismo de grupos.

1.5 Relações em Semigrupos

Definição 1.40 *Seja S um semigrupo e R uma relação em S. Dizemos que R é*

- ***compatível à esquerda** (com operação de S) se $(s, t) \in R$ implica $(as, at) \in R$ para todo $a, s, t \in S$;*
- ***compatível à direita** (com operação de S) se $(s, t) \in R$ implica $(sa, ta) \in R$ para todo $a, s, t \in S$;*
- ***compatível** (com operação de S) se $(s, t), (s', t') \in R$ implica $(ss', tt') \in R$ para todo $s, s', t, t' \in S$.*

*Uma relação de equivalência compatível à esquerda (direita) é chamada **congruência à esquerda (direita)**. Relação de equivalência compatível é chamada **congruência**.*

Proposição 1.41 *Uma relação de equivalência ρ num semigrupo S é uma congruência se, e somente se, é ambos congruência à esquerda e a direita.*

Prova: Para a primeira parte do teorema, suponha ρ uma congruência. Seja $(s, t) \in \rho$ e $a \in S$. Como ρ é relação de equivalência, temos que $(a, a) \in \rho$. Logo, pela compatibilidade, temos $(as, at), (sa, ta) \in \rho$. Para o outo lado, sejam $(s, t), (s', t') \in \rho$. Então, em particular, $(s', s'), (t, t) \in \rho$. Logo,

$$(ss', ts') \in \rho$$

$$(ts', tt') \in \rho$$

Com isso, pela transitividade, temos $(ss', tt') \in \rho$. □

Proposição 1.42 *Se ρ é uma congruência em um semigrupo S, então ${}^{S}/_{\rho}$ é um semigrupo com respeito à operação $\rho a \rho b = \rho(ab)$ e a função $\rho^{\natural} : S \to {}^{S}/_{\rho}$ definida por $s \mapsto \rho s$, para todo $s \in S$ é um homomorfismo. Além do mais, se S é semigrupo inverso então ${}^{S}/_{\rho}$ também é semigrupo inverso.*

Prova: Se ρ é uma congruência em S, definimos uma operação binária no conjunto quociente ${}^{S}/_{\rho}$ por $\rho a \rho b = \rho(ab)$. Esta operação está bem definida pois, se $\rho a = \rho a'$ e $\rho b = \rho b'$, temos $(a, a'), (b, b') \in \rho$, o que implica, $(ab, a'b') \in \rho$ e, portanto, $\rho(ab) = \rho(a'b')$.

Além do mais temos que tal operação é claramente associativa e $\rho^{\natural}$ de S em ${}^{S}/_{\rho}$ é homomorfismo por construção.

Já para mostrar que se S é semigrupo inverso então ${}^{S}/_{\rho}$ também é semigrupo inverso, considere $(s, t) \in \rho$, então $\rho(s) = \rho(t)$ em ${}^{S}/_{\rho}$. Observe que $\rho(s^*) = \rho(s)^*$. De fato,

$$\rho(s) = \rho(ss^*s) = \rho(s)\rho(s^*)\rho(s)$$

$$\rho(s^*) = \rho(s^*ss^*) = \rho(s^*)\rho(s)\rho(s^*).$$

Pra provar que ${}^{S}/_{\rho}$ é inverso, basta mostrar que seus idempotentes comutam. Pelo lema **??**, os idempotentes de ${}^{S}/_{\rho}$ são da forma $\rho(e)$ com e idempotente em S. Daí é claro que quaisquer dois idempotentes em ${}^{S}/_{\rho}$ comutam. □

Teorema 1.43 *Sejam S e T semigrupos. Se $\phi : S \to T$ é um homomorfismo e $\equiv$ é uma congruência que está contida em $Ker(\phi)$, então existe um único homomorfismo $\tilde{\phi} : {}^{S}/_{\equiv} \to T$ tal que*

$$\tilde{\phi} \circ \pi = \phi,$$

onde $\pi : S \to {}^{S}/_{\equiv}$ é a projeção canônica.

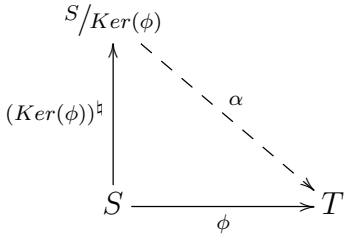
Prova: A aplicaçao $\tilde{\phi}$ que leva $[a]$ em $\phi(a)$ está bem definida pois $\equiv$ está contida em $Ker(\phi)$: se $a \equiv a'$, então $(a, a') \in Ker(\phi)$, ou seja, $\phi(a) = \phi(a')$.

É imediato que $\tilde{\phi}$ é homomorfismo, e a equação

$$\tilde{\phi} \circ \pi = \phi$$

segue da definição de $\tilde{\phi}$. □

Teorema 1.44 ***(Primeiro Teorema dos Isomorfismos)*** *Se $\phi : S \to T$ é um homomorfismo, com S e T semigrupos, então a relação $Ker(\phi) = \phi^{-1} \circ \phi = \{(a, b) \in S \times S : \phi(a) = \phi(b)\}$ é uma congruência em S e existe uma única função injetora $\alpha : {}^{S}/_{Ker(\phi)} \to T$ tal que o diagrama abaixo comuta.*



Prova: Faremos a demonstração passo a passo: $Ker(\phi)$ é relação de equivalência pela própria definição de $Ker(\phi)$ como $\phi^{-1} \circ \phi$.

Compatibilidade com a multiplicação: Sejam $a, b, c, d \in S$ com $(a, b), (c, d) \in Ker(\phi)$. Então, $\phi(a) = \phi(b)$ e $\phi(c) = \phi(d)$. Daí,

$$\phi(ac) = \phi(a)\phi(c) = \phi(b)\phi(d) = \phi(bd)$$

Portanto, $(ac, bd) \in Ker(\phi)$.

Defina

$$\begin{array}{rccc} \alpha : & {}^{S}/_{Ker(\phi)} & \longrightarrow & T \\ & (Ker(\phi))^{\natural}a & \longmapsto & \phi a. \end{array}$$

Claramente a função α está bem definida e é um homomorfismo pela proposição anterior. Além disso,

α é injetora: $(Ker(\phi))^{\natural}a = (Ker(\phi))^{\natural}b \Leftrightarrow (a, b) \in Ker(\phi) \Leftrightarrow \phi(a) = \phi(b)$.

E que o diagrama comuta é imediato pela contrução. □

Proposição 1.45 *Seja ρ uma congruência em um semigrupo inverso S.*

i) Se $(s, t) \in \rho$, então $(s^*, t^*), (s^*s, t^*t), (ss^*, tt^*) \in \rho$

ii) Se $(s, e) \in \rho$, com $e \in E(S)$, então $(s, s^*), (s, s^*s), (s, ss^*) \in \rho$

Prova:

i) Temos que $\rho(s^*) = \rho(s)^*$. Daí, se $\rho(s) = \rho(t)$ em ${}^{S}/_{\rho}$, temos que $\rho(s^*) = \rho(t^*)$ em ${}^{S}/_{\rho}$, o que implica $(s^*, t^*) \in \rho$.

Agora, como $(s, t) \in \rho$, temos que $(s^*, t^*) \in \rho$ e pela compatibilidade, temos (ss^*, tt^*), $(s^*s, t^*t) \in \rho$.

ii) Como $(s, e) \in \rho$, temos, pelo item $i)$ que $(s^*, e) \in \rho$, pois $e^* = e$. Usando o fato que ρ é relação de equivalência, temos que $(e, s^*) \in \rho$. Daí, pela compatibilidade, temos $(s, s^*) \in \rho$.

Ja temos $(s^*, e) \in \rho$ e $(s, s) \in \rho$ por ser ρ relação de equivalência. Então, pela compatibilidade, temos $(ss^*, s), (s^*s, s) \in \rho$.

□

Se ρ é uma congruência e S um semigrupo, ρ é chamada **congruência de grupo** quando S/ρ é grupo.

Como S/ρ é semigrupo inverso, temos que ρ é congruência de grupo se, e somente se, $(e, f) \in \rho$ para todo $e, f \in E(S)$ pois, assim, todos os idempotentes de S estarão na mesma classe em S/ρ.

1.6 Ordem Parcial em Semigrupo Inverso

Nesta seção, mostraremos uma relação de ordem "natural" em um semigrupo inverso. Esta relação de ordem, na verdade, generaliza a relação de ordem natural no conjunto $\mathscr{I}(X)$, que é $\alpha \leq \beta$ se β estende α onde α, β são bijeções definidas em subconjuntos de X.

Considere a relação $\leq$ em um semigrupo inverso S definida da seguinte maneira:

$$s \leq t \Leftrightarrow s = te$$

para algum $e \in E(S)$.

Lema 1.46 *Seja S um semigrupo inverso. São equivalentes:*

1) $s \leq t$

2) $s = ft$ *para algum* $f \in E(S)$

3) $s^* \leq t^*$

4) $s = ss^*t$

5) $s = ts^*s$

Prova: $(1) \Rightarrow 2))$:

$s \leq t \Rightarrow s = te \overset{Prop.??}{=} s = ft$

$(2) \Rightarrow 3))$:

$s = ft \Rightarrow s^* = t^* f \Rightarrow s^* \leq t^*$

$(3) \Rightarrow 4))$:

$s^* \leq t^* \Rightarrow s^* = t^* e \Rightarrow s = et$

$es = eet = et = s$

$\Rightarrow ess^* = ss^* \Rightarrow s = (ss^*)s = ess^*et = eess^*t = (es)s^*t = ss^*t$

$(4) \Rightarrow 5))$:

$s = ss^*t \overset{Prop.??}{=} s = te$

$se = tee = te = s$

$\Rightarrow s^*se = s^*s$

$\Rightarrow s = ss^*s = tes^*se = ts^*se = ts^*s$

$(5) \Rightarrow 1))$:

$s = ts^*s \Rightarrow s \leq t$, pois $s^*s \in E(S)$. □

Proposição 1.47 *Seja S um semigrupo inverso. Tem-se*

i) A relação $\leq$ é de ordem parcial em S

ii) Se $s \leq t$ e $u \leq v$, então $su \leq tv$

iii) Se $s \leq t$, então $s^*s \leq t^*t$ e $ss^* \leq tt^*$

iv) O semirreticulado de idempotentes E satisfaz: dados $s \in S$ e $e \in E(S)$, com $s \leq e$, então $s \in E(S)$.

Prova:

i)
- Reflexiva: $s = s(s^*s) \Rightarrow s \leq s$
- Antissimétrica: $s \leq t, t \leq s \overset{Lema??}{=} s = ts^*s, t = st^*t$

  $\Rightarrow s = ts^*s = st^*ts^*s = ss^*st^*t = st^*t = t$

- Transitiva: $s \leq t, t \leq u \overset{Lema??}{=} s = te, t = uf$

  $\Rightarrow s = te = u(fe) \Rightarrow s \leq u$

ii) $s \leq t \Rightarrow s = te$ e $u \leq v \Rightarrow u = vf$

$\Rightarrow su = tevf = tve'f \Rightarrow su \leq tv$

iii) Análogo ao item anterior, basta observar que $s \leq t \Rightarrow s^* \leq t^*$

iv) $s \leq e \Rightarrow s = ef$ para algum $f \in E(S)$. Logo, $s \in E(S)$

□

Obs. 1.48 *Dado um conjunto parcialmente ordenado $(P, \leq)$, $Q \subseteq (P, \leq)$ é chamado* ***ideal de ordem*** *se satisfaz iv), isto é, $p \leq q$ e $q \in Q$, então $p \in Q$*

Exemplo 1.49 *Relação $\leq$ em $\tilde{G}^R$. Dados (A, g) e (B, h) em $\tilde{G}^R$, $(A, g) \leq (B, h) \Leftrightarrow \exists (C, 1_G) \in E(\tilde{G}^R)$ tal que*

$(A, g) = (B, h)(C, 1_G) = (B \cup hC, h) \Leftrightarrow h = g$ *e* $B \subseteq A$.

Observe que se $B \cup hC = A$, então B está contido em A e, reciprocamente, se B é subconjunto de A basta então tomar $C = g^{-1}A$.

Exemplo 1.50 *Relação $\leq$ em $\mathscr{I}(X)$ Dados*

$$\alpha : dom\alpha \longrightarrow im\alpha$$

$$\beta : dom\beta \longrightarrow im\beta$$

temos

$\alpha \leq \beta \Leftrightarrow \beta$ *estende* α. *De fato,*

$(\Rightarrow)$ $\alpha \leq \beta$, *então existe* $1_A \in E(\mathscr{I}(X))$ *tal que* $\alpha = \beta \circ 1_A$

Para que faça sentido a composição, podemos tomar $A = dom\alpha$.

Denote $Graf\alpha$ o gráfico da função α. Seja $(x, y) \in Graf\alpha$, então $(x, x) \in Graf1_A$ e $(x, y) \in Graf\beta$.

Então β estende α.

$(\Leftarrow)$ β *estende* α: *seja* $x \in dom\alpha$ *e* $(x, y) \in Graf\beta$. *Como* β *estende* α, *deve-se ter* $y = \alpha(x)$, *o que implica* $(x, y) \in Graf\alpha$.

Então $\alpha = \beta \circ 1_{dom\alpha} \Rightarrow \alpha \leq \beta$.

Lema 1.51 *Sejam S um semigrupo inverso e σ a menor relação de equivalência em S que contém $\leq$. Então, para todos $s,t \in S$, tem-se $(s,t) \in \sigma$ se, e somente se, existe $u \in S$ tal que $u \leq s,t$.*

Prova:

Para a primeira parte da prova, tome $(s,t) \in \sigma$. Então, existe $s = s_1, s_2, ..., s_n = t \in S$ tais que $s_i \leq s_{i+1}$ ou $s_{i+1} \leq s_i$ para $i = 1, 2, ..., n-1$.

Tome $s_i = e_i s_{i+1}$ ou $s_{i+1} = e_i s_i$ com $e_i \in E(S)$. Então $e_i s_i = e_i s_{i+1}$. Considere $e = e_1 e_2 ... e_{n-1}$.

$$\begin{aligned} es = es_1 =& (e_2 ... e_{n-1})(e_1 s_1) \\ =& (e_2 ... e_{n-1})(e_1 s_2) \\ =& (e_1 e_3 ... e_{n-1})(e_2 s_2) \\ =& (e_1 e_3 ... e_{n-1})(e_2 s_3) \\ =& ... \\ =& (e_1 ... e_{n-2})(e_{n-1} s_n) \\ =& es_n = et \end{aligned}$$

Tomando $u = es = et$. Assim, tem-se $u \leq s,t$.

Já para mostrar a segunda parte do teorema, suponha que existe $u \in \sigma$ tal que $u \leq s,t$. Tem-se que $z_1 = s, z_2 = u, z_3 = t$.

Defina a sequência $z_i \leq z_{i+1}$ ou $z_{i+1} \leq z_i$ para $i = 1, 2$. Segue do corolário **??** que $(s,t) \in \sigma$. □

Obs. 1.52 *Considere o monóide inverso $\tilde{G}^R$ e σ a menor relação de equivalência que contém $\leq$. Todos os idempotentes de $\tilde{G}^R$ são da forma $(A, 1_G)$. Os idempotentes de ${}^{\tilde{G}^R}/_{\sigma}$ são as classes de $(A, 1_G)$. Mas $(A, 1_G) \leq (\{1_G\}, 1_G)$ para todo $A \in P_{1_G}$.*

Então, ${}^{\tilde{G}^R}/_{\sigma}$ é monóide inverso com um único idempotente. Portanto, ${}^{\tilde{G}^R}/_{\sigma}$ é um grupo e é isomorfo a G pelo isomorfismo

$$\begin{aligned} \varphi : \ G &\longrightarrow {}^{\tilde{G}^R}/_{\sigma} \\ g &\longmapsto \sigma^{\natural}(\{1_G, g\}, g). \end{aligned}$$

Capítulo 2

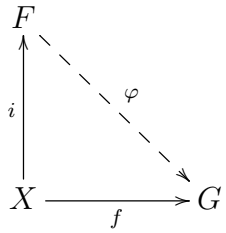
Semigrupo de Exel e Estruturas Algébricas por Geradores e Relações

Neste capítulo estudaremos estruturas algébricas definidas a partir de um determinado conjunto que possam satisfazer ou não determinadas relações. Ou seja, dado um determinado conjunto A, qual é o menor conjunto $\bar{A}$, contendo A, que tem uma determinada estrutura álgebrica, como a de um grupo, anel, grupoide, algebra, etc., e que satisfaz ou não determinadas condições. Como principal referênciano baseamos em [12].

Também apresentamos aqui o Semigrupo de Exel, trabalhamos com representações do mesmo e tentamos compreender melhor ações dele em um conjunto. No que diz respeito, utilizamos como principal referência [5].

2.1 Grupos Livres

Definição 2.1 *Sejam X um subconjunto de um grupo F. Então, dizemos que F é um **grupo livre** com **base** X se, para cada grupo G e cada função $f : X \to G$, existe um único morfismo $\varphi : F \to G$ que estende f, ou seja, o seguinte diagrama comuta:*



Obs. 2.2 *Veremos depois que X deve gerar F.*

Usaremos a seguinte construção para provar a existência de um grupo livre dado um conjunto X qualquer.

Considere X um conjunto qualquer e X^{-1} um conjunto disjunto de X para o qual há uma bijeção $X \to X^{-1}$ denotada por $x \mapsto x^{-1}$. Seja X' um conjunto unitário disjunto de $X \cup X^{-1}$ cujo elemento é denotado por 1. Dado $x \in X$, então x^1 denota x e x^0 denota 1.

Definição 2.3 *Uma **palavra** em X é uma sequência $w = (a_1, a_2, ...)$, onde $a_i \in X \cup X^{-1} \cup \{1\}$, para todo i, tal que $a_i = 1$ a partir de algum índice, isto é, há um inteiro $n \geq 0$ com $a_i = 1$ para todo $i > n$. Em particular, a sequência constante*

$$(1, 1, 1, ...)$$

*é uma palavra, chamada **palavra vazia**, e também denotada por* 1.

Como as palavras possuem somente um número finito de termos antes de se tornarem constantes, usaremos a notação simplificada

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$$

onde $x_i \in X$, $\epsilon_i = +1, -1$ ou 0, para $i = 1, 2, ..., n-1$, e $\epsilon_n = \pm 1$.

Esta "ortografia" de uma palavra é única, ou seja, duas palavras (a_i) e (b_i) são iguais se, e somente se, $a_i = b_i$ para todo i. O **comprimento** de $w = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$ é definido como sendo n.

Definição 2.4 *Se $w = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$ é uma palavra, então sua **inversa** é a palavra $w^{-1} = x_n^{-\epsilon_n} ... x_2^{-\epsilon_2} x_1^{-\epsilon_1}$.*

Observe da forma que definimos uma palavra, temos que palavras como xy e $x11y$, por exemplo, são diferentes, mas, para a construção de semigrupos livres, seria interessante que fossem iguais. A partir daí, surge a definição seguinte.

Definição 2.5 *Uma palavra $w \in X$ é dita **reduzida** se w é vazia ou $w = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$, onde todo $\epsilon_i = \pm 1$, e x e x^{-1} nunca são adjacentes.*

Se uma palavra é reduzida, então a sua inversa também o é.

Definição 2.6 *Uma **subpalavra** de $w = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$ é a palavra vazia ou uma palavra na forma $v = x_i^{\epsilon_i} ... x_j^{\epsilon_j}$, com $1 \leq i \leq j \leq n$. Ou seja, v é subpalavra de w se existem palavras w' e w'' tais que $w = w'vw''$.*

Assim, temos que uma palavra não vazia w é reduzida se, e somente se, não contém subpalavras na forma $x^{\epsilon}x^{-\epsilon}$ ou x^0.

Também podemos definir uma multiplicação de duas palavras $w = x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n}$ e $u = y_1^{\epsilon_1}y_2^{\epsilon_2}...y_n^{\epsilon_n}$ por justaposição, ou seja, $wu := x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n}y_1^{\epsilon_1}y_2^{\epsilon_2}...y_n^{\epsilon_n}$, mas, nesse caso, tal multiplicação não define um produto no conjunto de todas as palavras reduzidas de X, mesmo que w e u sejam reduzidas. Mas podemos definir uma nova multiplicação de palavras reduzidas como sendo a palavra reduzida obtida após cancelamentos da palavra obtida por justaposição. Mais precisamente, se $w = w'v$ com v^{-1} subpalavra de u com $u = v^{-1}u'$ e tal que $w'u'$ é reduzida, finalmente definimos o produto de palavras reduzidas por **justaposição** como sendo $wu := w'u'$.

Com estas feramentas, podemos, dado um conjunto X, garantir a existência de um grupo livre gerado pelo mesmo.

Teorema 2.7 *Dado um conjunto X, então existe um grupo livre F com base X.*

Prova: Se considerarmos F como sendo o conjunto de todas as palavras reduzidas em X, temos que F será um grupo com a operacao de "justaposição com cancelamento" definida acima. No entanto, não é nada simples verificar a associatividade. Então usaremos o truque de *van der Wearden* (1945) conforme [12]:

Para cada $x \in X$, considere as funções $|x| : F \to F$ e $|x^{-1}| : F \to F$ definidas, para $\epsilon = \pm 1$, da seguinte maneira:

$$|x^{\epsilon}|\left(x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n}\right) = \begin{cases} x^{\epsilon}x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n} & \text{se } x^{\epsilon} \neq x_1^{-\epsilon_1} \\ x_2^{\epsilon_2}...x_n^{\epsilon_n} & \text{se } x^{\epsilon} = x_1^{-\epsilon_1} \end{cases}$$

Como $|x^{\epsilon}| \circ |x^{-\epsilon}|$ e $|x^{-\epsilon}| \circ |x^{\epsilon}|$ são iguais à identidade $1_F : F \to F$, segue que $|x^{\epsilon}|$ é uma permutação de F com inverso $|x^{-\epsilon}|$.

Sejam S_F o grupo das bijeções de F e $\mathscr{F}$ o subgrupo de S_F gerado por $[X] = \{|x| : x \in X\}$. Então $\mathscr{F}$ é um grupo com base $[X]$. De fato, note que há uma bijeção natural $\zeta : [X] \to X$ dada por $|x| \to x$.

Um elemento arbitrário $g \in \mathscr{F}$, diferente de 1, tem a fatoração

$$g = |x_1^{\epsilon_1}| \circ |x_2^{\epsilon_2}| \circ ... \circ |x_n^{\epsilon_n}| \tag{2.1}$$

onde $\epsilon_i = \pm 1$ e $|x^{\epsilon}|$ e $|x^{-\epsilon}|$ nunca são adjacentes (ou podemos cancelá-los). Tal fatoração de g é única pois $g(1) = x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n}$ e a ortografia é única.

Para ver que $\mathscr{F}$ é livre com base $[X]$, suponha que G é um grupo e que $f : [X] \to G$ é uma função. Como a fatoração **??** é única, a função $\varphi : \mathscr{F} \to G$, dada por $\varphi(|x_1^{\epsilon_1}| \circ |x_2^{\epsilon_2}| \circ ... \circ |x_n^{\epsilon_n}|) = f(|x_1^{\epsilon_1}|)f(|x_2^{\epsilon_2}|)...f(|x_n^{\epsilon_n}|)$ está bem definida e é a única função que estende f. Como $[X]$ gera $\mathscr{F}$, basta verificar que φ é homomorfismo.

Sejam w e u palavras reduzidas em $[X]$. Neste caso, é claro que $\varphi(w \circ u) = \varphi(w)\varphi(u)$ sempre que palavra wu, obtida de $w \circ u$, apagando as barras verticais, é reduzida. Caso contrário, tome $w = w' \circ v$ e $u = v^{-1}u'$ como na definição de justaposição. Agora, $\varphi(w) = \varphi(w')\varphi(v)$ e $\varphi(u) = \varphi(v^{-1})\varphi(u') = \varphi(v)^{-1}\varphi(u')$ (por serem e $w' \circ v$, e $v^{-1}u'$ reduzidas). Portanto, $\varphi(w)\varphi(u) = \varphi(w')\varphi(u')$. Por outro lado, $\varphi(w \circ u) = \varphi(w' \circ u') = \varphi(w')\varphi(u')$ (pois $w' \circ u'$ é reduzida). Então φ é homomorfismo, de onde segue que $\mathscr{F}$ é grupo livre com base $[X]$.

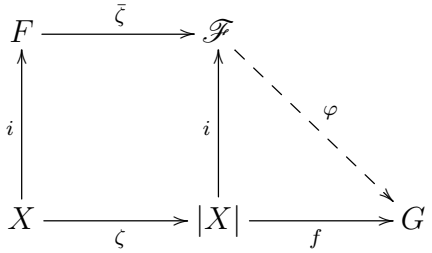
Por fim, como a função ζ é uma bijeção de X em $[X]$, podemos definir uma bijeção $\bar{\zeta} : F \to \mathscr{F}$ por $x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n} \mapsto |x_1^{\epsilon_1}| \circ |x_2^{\epsilon_2}| \circ ... \circ |x_n^{\epsilon_n}|$ com $\bar{\zeta}(X) = \zeta(X) = |X|$ e segue que F é um conjunto isomorfo a $\mathscr{F}$.

Para concluir a prova, observe que F é grupo com a operação $x * y := \bar{\zeta}(\bar{\zeta}^{-1}(x)\bar{\zeta}^{-1}(y)$. De fato,

$$\begin{aligned}(x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n}) * (y_1^{\eta_1}y_2^{\eta_2}...y_m^{\eta_m}) &= \bar{\zeta}(\bar{\zeta}^{-1}(x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n})\bar{\zeta}^{-1}(y_1^{\eta_1}y_2^{\eta_2}...y_m^{\eta_m}) \\ &= \bar{\zeta}(|x_1^{\epsilon_1}| \circ |x_2^{\epsilon_2}| \circ ... \circ |x_n^{\epsilon_n}| \circ |y_1^{\eta_1}| \circ |y_2^{\eta_2}| \circ ... \circ |y_n^{\eta_n}|)\end{aligned}$$

Assim, $(x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n})^{-1} = x_n^{-\epsilon_n}...x_2^{-\epsilon_2}x_1^{-\epsilon_1}$.

O seguinte diagrama resume a demonstração:



Como a função ζ é uma bijeção de X em $[X]$, podemos definir uma bijeção $\bar{\zeta} : F \to \mathscr{F}$ por $x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n} \mapsto |x_1^{\epsilon_1}| \circ |x_2^{\epsilon_2}| \circ ... \circ |x_n^{\epsilon_n}|$ com $\bar{\zeta}(X) = \zeta(X) = |X|$ □

Corolário 2.8 *Todo grupo G é um quociente de um grupo livre.*

Prova: Construa um conjunto $X = \{x_g : g \in G\}$ tal que $f : x_g \mapsto g$ é uma bijeção. Considere F como sendo o grupo livre com base X, então existe um homomorfismo $\varphi : F \to G$

estendendo f. Além do mais, φ é sobrejetora, pois f é. Então, pelo Teorema do Isomorfismo, $G \cong {}^{F}/_{Ker(\varphi)}$.

□

Garantida a existência de um grupo livre gerado por um conjunto dado, podemos definir um grupo livre que satisfaça determinadas condições.

Definição 2.9 *Sejam X um conjunto e Δ uma família de palavras em X. Um grupo G tem* ***geradores*** *X e* ***relações*** *Δ se $G \cong {}^{F}/_{R}$, onde F é grupo livre com base X e R é o subgrupo normal de F gerado por Δ. O par ordenado $(X|\Delta)$ é chamado de* ***apresentação*** *de G.*

Outra forma de descrever uma relação $r \in R$, no grupo quociente G sendo apresentado, é pela equação $r = 1$. Definimos R como um subgrupo normal de F gerado por Δ pois, se $r \in \Delta$ e $w \in F$, então $r = 1$ em G implica que $wrw^{-1} = 1$ em G e também porque queremos formar um grupo quociente.

A seguir, veremos vários exemplos de grupos livres com geradores e relações.

Exemplo 2.10 *O grupo com único gerador x e relação $x^n = 1$ é (isomorfo a) $\mathbb{Z}_n$.*

Observe que, nesse caso, temos $F = \langle x \rangle$ e portanto o subgrupo normal R de F gerado pela relação $r = x^n$ é $\langle x^n \rangle$. Portanto, $G \cong {}^{F}/_{R} = {}^{\langle x \rangle}/_{\langle x^n \rangle} \cong \mathbb{Z}_n$.

Exemplo 2.11 *No caso específico de $G = \mathbb{Z}_6$, também temos a apresentação $\mathbb{Z}_6 = (x, y|x^3 = 1, y^2 = 1, xyx^{-1}y^{-1} = 1)$.*

Note que teremos $F = \{1, x, x^2(= x^{-1}), y(= y^{-1}), xy, ...\}$ e que da expressão do comutador $xyx^{-1}y^{-1} = 1$, segue que no quociente ${}^{F}/_{R}$, teremos $xy = yx$. Portando

$$ {}^{F}/_{R} = \left\{\bar{1}, \bar{x}, \bar{x^2}, \bar{y}, \bar{xy}, \bar{x^2y}\right\}$$

Exemplo 2.12 *O grupo diedral D_{2n} tem a apresentação*

$$D_{2n} = (x, y|x^n = 1, y^2 = 1, yxy = x^{-1})$$

Aqui, observa-se primeiro que escrevemos a relação $yxy = x^{-1}$ ao invés de $yxyx = 1$, o que diferencia este exemplo do caso anterior, $\mathbb{Z}_6$.

Pela definição, D_{2n} tem ordem $2n$, tendo geradores S e T satisfazendo as equações dadas. Se $G = {}^{F}/_{R}$, onde F é um grupo livre com base $\{x, y\}$ e R é o subgrupo normal gerado

por $\{x^n, y^2, xyxy\}$, então resta verificar que G tem ordem $2n$. Com efeito, a definição de grupo livre dá o homomorfismo sobrejetor $\varphi : F \to D_{2n}$, com $\varphi(x) = S$ e $\varphi(y) = T$. Além disso, $R \leq Ker(\varphi)$, pois S e T satisfazem as relações, então, pelo 3^o teorema dos isomorfismos, temos a "sobrejeção" ${}^{F}/_{R} \to {}^{F}/_{Ker(\varphi)}$, isto é, há uma sobrejeção $G = {}^{F}/_{R} \to D_{2n}$. Daqui, $|G| \geq 2n$. A inequação inversa também vale pois, para cada elemento em G, temos a fatoração $x^i y^j R$ com $0 \leq i < n$ e $0 \leq j < 2$. Então, $|G| = 2n$, portanto $G \cong D_{2n}$.

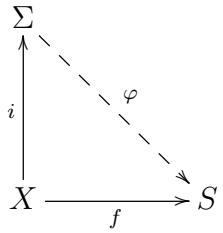
Exemplo 2.13 *Outro exemplo seria do grupo dos quatérnios, que tem apresentação $Q = (a, b|a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1})$ e $Q = (x, y|xyx = y, x^2 = y^2)$*

Em cada um dos casos, basta verificar que o grupo apresentado tem ordem 8.

2.2 Semigrupos Livres

Contruiremos, agora, semigrupos livres. Como é se de esperar, a definição formal é basicamente a mesma para grupos, no entanto a garantia da existência do semigrupo livre é mais simples.

Definição 2.14 *Se X é um subconjunto de um semigrupo Σ, então Σ é um **semigrupo livre** com **base** X se, para cada semigrupo S e cada função $f : X \to S$, existe um único homomorfismo $\varphi : \Sigma \to S$ estendendo f. Ou seja, o seguinte diagrama comuta:*



Definição 2.15 *Uma palavra w em X é **positiva** se $w = 1$ ou $w = x_1^{\epsilon_1} x_2^{\epsilon_2} ... x_n^{\epsilon_n}$, onde todos os expoentes $\epsilon_i > 0$.*

O conjunto Σ de todas as palavras positivas em X é um semigrupo livre com base X. Observe que o produto de palavras positivas é positiva e, como não há possibilidade de cancelamento, é fácil de ver que o produto é associativo. De qualquer maneira, apresentaremos tal resultado por meio de um teorema:

Teorema 2.16 *Sejam X um conjunto não vazio, Σ o conjunto de todas as palavras positivas de X e S um semigrupo. Se $f : X \to S$ é uma função qualquer, então existe um único homomorfismo $\varphi : \Sigma \to S$ tal que $\varphi|_X = f$.*

Prova: Defina $\varphi(x_1x_2...x_n) = f(x_1)f(x_2)...f(x_n)$. Segue direto da definição de φ que o mesmo é homomorfismo e estende f. A unicidade pode ser provada observando que se existe outro homomorfismo ψ que estende f, teremos

$$\psi(x_1x_2...x_n) = \psi(x_1)\psi(x_2)...\psi(x_n) = f(x_1)f(x_2)...f(x_n) = \varphi(x_1x_2...x_n).$$

□

Daí segue que cada semigrupo é imagem homomórfica de um semigrupo livre.

Para podermos definir apresentação de semigrupo, precisamos de alguns conceitos preliminares.

Relembre que uma congruência em um semigrupo S é uma relação de equivalência $\equiv$ em S tal que

$$a \equiv a' \text{ e } b \equiv b' \Rightarrow ab \equiv a'b'$$

E que se $\equiv$ é uma congruência em um semigrupo S, então o **semigrupo quociente** é o conjunto de todas as classes de equivalência, denotado por ${}^{S}/_{\equiv}$, com a operação

$$[a][b] = [ab]$$

onde $[a]$ denota a classe de equivalência de a em S.

A construção de congruência pode se dar de duas formas diferentes. A primeira forma é por meio de um homomorfismo $\varphi : S \to T$ de semigrupos. Neste caso, defina $a \equiv b$ se $\varphi(a) = \varphi(b)$. Chamamos esta congruência de $Ker(\varphi)$, e com ela podemos enunciar os seguintes teoremas:

Teorema 2.17 ***(Teorema do Isomorfismo)*** *Sejam S e T semigrupos com $\varphi : S \to T$ um homomorfismo. Então*

$${}^{S}/_{Ker(\varphi)} \cong im\varphi.$$

Prova: Existe ψ pelo teorema **??**: basta tomar $\tilde{\phi}$ e considerar a "restrição do contradominio" à imagem de φ. Da definição de Ker como congruência, segue que essa aplicação é injetora e, portanto, é bijetora. □

Relembre que uma congruência ρ é uma relação de equivalência compatível. Ou seja, é uma relação de equivalência que, se $(s,t),(s',t') \in \rho$, então $(ss',tt') \in \rho$ para todo $s,s',t,t' \in S$.

A segunda construção se baseia no seguinte fato. Como qualquer relação em S, uma congruência é um subconjunto de $S \times S$. É facil de ver que qualquer interseção de congruências também é congruência. Se S é um semigrupo, pode-se assim definir a congruência gerada por um subconjunto E de $S \times S$ como a interseção de todas as congruências contendo E.

Se Σ é um semigrupo livre com base X e se $\{w_i = u_i : i \in I\}$ é uma família de equações, onde $w_i, u_i \in \Sigma$, entao defina $\equiv$ como sendo a congruência gerado por $\{(w_i, u_i) : i \in I\} \subset \Sigma \times \Sigma$.

Finalmente, o semigrupo quociente ${}^{\Sigma}/_{\equiv}$ é dito ter a **apresentação**

$$(X|w_i = u_i \forall i \in I).$$

2.3 Semigrupo de Exel

Agora, definiremos o Semigrupo de Exel, que será vital no decorrer deste trabalho. Além do mais, veremos algumas de suas propriedades. Conforme mencionado no início deste capítulo, utilizamos [5] como principal referência nesta parte, porém mais detalhes podem ser encontrados em [3], [6], [9] e [10].

Definição 2.18 *Seja G um grupo, o **Semigrupo de Exel** $S(G)$ é o semigrupo definido por geradores e relações como segue.*

1. *A cada $g \in G$ associa-se o gerador $[g]$.*
2. *Para cada par $g, h \in G$ considera-se as relações:*

   i) $[g^{-1}][g][h] = [g^{-1}][gh]$

   ii) $[g][h][h^{-1}] = [gh][h^{-1}]$

   iii) $[g][1_G] = [g]$

   iv) $[1_G][g] = [g]$

Obs. 2.19 *Note que o item iv pode ser obtido dos demais. Mas, a fim de clareza, ele aparece na definição. De fato,*

$$[1_G][g] = [gg^{-1}][g] \overset{ii}{=} [g][g^{-1}][g] \overset{i}{=} [g][g^{-1}g] = [g][1_G] \overset{iii}{=} [g]$$

Obs. 2.20 *Como $[g][g^{-1}][g] = [g][g^{-1}g] = [g]$, segue que $S(G)$ é um semigrupo regular. Veremos mais adiante que $S(G)$ é um semigrupo inverso.*

Exemplo 2.21 *Seja* $G = \mathbb{Z}_2 = \langle g | g^2 = 1_G \rangle$. *Então* $S(\mathbb{Z}_2) = \{[1_G], [g], [g][g]\}$.

Observe que, pela definição de Semigrupo de Exel, temos:

$$[1_G][g] = [g][1_G] = [g]$$

$$[1_G][g][g] = [g][g][1_G] = [g][g]$$

$$[g][g][g] = [g]$$

Com isso, podemos concluir que $[g]^{2k} = [g][g]$ *se* n *é par e* $[g]^{2k+1} = [g]$ *para* $k \geq 1$.

Teorema 2.22 *Seja* S *um semigrupo com apresentação por geradores e relações*

$$S = \langle X | u_i = w_i, i \in I \rangle ,$$

com

$$u_i = x_{1,i}x_{2,i}...x_{n_i,i}$$

$$w_i = y_{1,i}y_{2,i}...y_{m_i,i}$$

para cada $i \in I$, *onde cada* $x_{k,i}$ *e* $y_{l,i}$ *pertence a* X. *Dados um semigrupo* T *e uma função* $f : X \to T$ *tais que* $f(x_{1,i})f(x_{2,i})...f(x_{n_i,i}) = f(y_{1,i})f(y_{2,i})...f(y_{m_i,i})$. *Então existe uma única extensão de* f *a um homomorfismo de semigrupos* $F : S \to T$.

Prova: Dada $f : X \to T$, o teorema **??** garante que existe uma única extensão $\tilde{f} : \Sigma \to T$ de f ao semigrupo livre Σ, gerado por X, que é dada por

$$\tilde{f}(x_1x_2...x_n) = f(x_1)f(x_2)...f(x_n).$$

Pelas hipóteses, $\tilde{f}(u_i) = \tilde{f}(w_i)$ para cada i em I. De fato,

$$\begin{aligned}
\tilde{f}(u_i) &= \tilde{f}(x_{1,i}x_{2,i}...x_{n_i,i}) \\
&= f(x_{1,i})f(x_{2,i})...f(x_{n_i,i}) \\
&= f(y_{1,i})f(y_{2,i})...f(y_{m_i,i}) \\
&= \tilde{f}(y_{1,i}y_{2,i}...y_{m_i,i}) \\
&= \tilde{f}(w_i).
\end{aligned}$$

Portanto, o núcleo de $\tilde{f}$ contém a congruência $\equiv$ gerada pelas equações $u_i = w_i$ com $i \in I$, e o teorema **??** mostra que existe um único homomorfismo $F : S = \Sigma|_{\equiv} \to T$ tal que

$F \circ \pi = \tilde{f}$, onde $\pi : \Sigma \to S$ é a projeção canônica. □

Corolário 2.23 *Dado um monóide S, um grupo G e uma função $f : G \to S$ satisfazendo, para $g, h \in G$,*

i) $f(g^{-1})f(g)f(h) = f(g^{-1})f(gh)$

ii) $f(g)f(h)f(h^{-1}) = f(gh)f(h^{-1})$

iii) $f(g)f(1_G) = f(g)$

Então, existe um único morfismo $\tilde{f} : S(G) \to S$ tal que $\tilde{f}([g]) = f(g)$ para todo $g \in G$.

Prova: A proposição segue imediatamente da definição de semigrupo definido por geradores e relações e do teorema **??**. □

Uma função que satisfaz os itens i e ii da proposição anterior e $f(1_G) = 1_S$ é chamada de **homomorfismo parcial**.

Proposição 2.24 *Existe um antiautomorfismo involutivo $* : S(G) \to S(G)^{op}$ tal que $[g]^* = [g^{-1}]$, para todo $g \in G$.*

Prova: Seja $S(G)^{op}$ o semigrupo oposto, definido com mesmo conjunto que $S(G)$ porém com operação

$$\alpha \bullet \beta = \beta\alpha$$

Defina

$$\begin{array}{rccc} f: & G & \longrightarrow & S(G)^{op} \\ & g & \longmapsto & [g^{-1}]. \end{array}$$

Vejamos que f satisfaz as propriedades da proposição anterior:

i) $f(g^{-1}) \bullet f(g) \bullet f(h) = [g] \bullet [g^{-1}] \bullet [h^{-1}] = [h^{-1}][g^{-1}][g] = [(gh)^{-1}][g] = [g] \bullet [(gh)^{-1}] = f(g^{-1}) \bullet f(gh)$

ii) $f(g) \bullet f(h) \bullet f(h^{-1}) = [g^{-1}] \bullet [h^{-1}] \bullet [h] = [h][h^{-1}][g^{-1}] = [h][(gh)^{-1}] = f(gh) \bullet f(h^{-1})$

iii) $f(g) \bullet f(1_G) = [1_G][g^{-1}] = [g^{-1}] = f(g)$

Logo, f se estende a um homomorfismo $* : S(G) \to S(G)^{op}$, dado por $[g]^* = [g^{-1}]$, involutivo pois, $* \circ * = id_{S(G)}$. □

Proposição 2.25 *Seja G um grupo e, para cada $g \in G$, seja $\epsilon_g = [g][g^{-1}] \in S(G)$. Então, para $g, h \in G$.*

i) ϵ_g *é um idempotente autoadjunto, isto é,* $\epsilon_g^* = \epsilon_g = \epsilon_g^2$

ii) $[g]\epsilon_h = \epsilon_{gh}[g]$

iii) $\epsilon_g\epsilon_h = \epsilon_h\epsilon_g$

Prova:

i) $\epsilon_g^* = ([g][g^{-1}])^* = [g^{-1}]^*[g]^* = [g][g^{-1}] = \epsilon_g$,

$\epsilon_g\epsilon_g = [g][g^{-1}][g][g^{-1}] = [g][1_G][g^{-1}] = [g][g^{-1}] = \epsilon_g$

ii) $[g]\epsilon_h = [g][h][h^{-1}] = [gh][h^{-1}] = [gh][(gh)^{-1}][gh][h^{-1}] = [gh][(gh)^{-1}][ghh^{-1}] = [gh][(gh)^{-1}][g] = \epsilon_{gh}[g]$

iii) $\epsilon_g\epsilon_h = [g][g^{-1}]\epsilon_h = [g]\epsilon_{g^{-1}h}[g^{-1}] = \epsilon_{gg^{-1}h}[g][g^{-1}] = \epsilon_h\epsilon_g$

□

Proposição 2.26 *Seja $S(G)$ um Semigrupo de Exel. Então todo elemento $\alpha \in S(G)$ admite uma decomposição $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]$, onde $n \geq 0$ e $g_1, g_2, ..., g_n, h \in G$. Além disso, pode-se assumir $g_i \neq g_j$ se $i \neq j$, $g_i \neq h$ e $g_i \neq 1_G$, para todo $i = 1, ..., n$.*

Prova: Defina $S = \{\alpha : \alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]\}$. Note que, para $n = 0$, temos $[h] \in S$, para todo $h \in G$ e, para $[g][h] \in S(G)$, observe que, tomando $\epsilon_g[gh] \in S$, temos

$$\epsilon_g[gh] = [g][g^{-1}][gh] = [g][g^{-1}gh] = [g][h].$$

Vejamos agora que S é subsemigrupo de $S(G)$: tome $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h] \in S$ e $[t] \in S(G)$. Então,

$$[h][t] = [h][h^{-1}][h][t] = [h][h^{-1}][ht] = \epsilon_h[ht]$$

e

$$\alpha[t] = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h][t]$$

$$= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}\epsilon_h[ht]$$

Observe que, caso tenhamos $h = g_i$, para algum i, bastaria comutar os idempotentes e "excluir" um ϵ_h, usando novamente o fato dele ser idempotente. De fato, se $h = g_i$, então $\epsilon_{g_i} = [h][h^{-1}]$, logo

$$\begin{aligned}
\alpha &= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_i}...\epsilon_{g_n}[h] \\
&= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_{i-1}}\epsilon_{g_{i+1}}...\epsilon_{g_n}\epsilon_{g_i}[h] \\
&= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_{i-1}}\epsilon_{g_{i+1}}...\epsilon_{g_n}[h][h^{-1}][h] \\
&= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_{i-1}}\epsilon_{g_{i+1}}...\epsilon_{g_n}[h][h^{-1}][h] \\
&= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_{i-1}}\epsilon_{g_{i+1}}...\epsilon_{g_n}[h]
\end{aligned}$$

Como S é subsemigrupo de $S(G)$, $S(G)$ é gerado pelos elementos $[g]$ com $g \in G$, e cada $[g]$ está em S, segue que $S = S(G)$.

□

Definição 2.27 *Se $\alpha \in S(G)$ é escrito na forma $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]$, satisfazendo as propriedades da proposição anterior, dizemos que α está na* ***forma padrão****.*

Proposição 2.28 *Para cada $\alpha \in S(G)$, tem-se $\alpha\alpha^*\alpha = \alpha$ e $\alpha^*\alpha\alpha^* = \alpha^*$. Em Particular, $S(G)$ é um semigrupo regular.*

Prova: Para o primeiro caso, tome $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]$, então

$$\begin{aligned}
\alpha\alpha^*\alpha &= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h][h^{-1}]\epsilon_{g_n}...\epsilon_{g_2}\epsilon_{g_1}\epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h] \\
&= \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}\overbrace{[h][h^{-1}][h]}^{[h]} \\
&= \alpha
\end{aligned}$$

Por outro lado, como $\alpha\alpha^*\alpha = \alpha$, temos que $(\alpha\alpha^*\alpha)^* = \alpha^*$, de onde segue que $\alpha^*\alpha\alpha^* = \alpha^*$. □

2.4 Representações de S(G)

Nosso objetivo é mostrar a unicidade do elemento α^*, dado $\alpha \in S(G)$ e, consequentemente concluir que o Semigrupo de Exel é um semigrupo inverso. Para isso, precisamos das representações de $S(G)$.

Definição 2.29 *Sejam $S(G)$ o Semigrupo de Exel e T um semigrupo qualquer. Uma **representação de** $S(G)$ é um homomorfismo $\varphi : S(G) \to T$.*

Um exemplo de representação de $S(G)$ é a **função grau** $\delta : S(G) \to G$ definida por $[g] \mapsto g$. De fato δ é um homomorfismo pois, $\delta([gh]) = gh = \delta([g])\delta([h])$. Uma primeira aplicação da função grau é a descrição dos idempotentes de $S(G)$ conforme proposição abaixo.

Proposição 2.30 *Seja $S(G)$ um Semigrupo de Exel. $\beta \in S(G)$ é idempotente se, e somente se, β é da forma $\beta = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}$.*

Prova: Seja $\beta \in S(G)$ um idempotente. Como o grau é homomorfismo, de $\beta^2 = \beta$ segue que $\delta(\beta)^2 = \delta(\beta^2) = \delta(\beta)$. Como o único idempotente de um grupo G é seu elemento neutro, e $\delta(\beta) \in G$, segue que $\delta(\beta) = 1_G$ e, como $\delta(\epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]) = h$, segue que $h = 1_G$ e, portanto, $\beta = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}$.

Reciprocamente, se β tem a forma descrita acima, então segue da Proposição **??** que β é idempotente.

□

Relembre: No capítulo anterior definimos $P_{1_G} = \{A : A \subseteq G, 1_G \in A\}$. Tome $\mathscr{F}(P_{1_G}) = \{f : P_{1_G} \to P_{1_G} : \text{f é função}\}$. Além do mais, defina, para cada $g \in G$, as funções

$$\begin{array}{rccc} \phi_g : & P_{1_G} & \longrightarrow & P_{1_G} \\ & E & \longmapsto & gE \cup \{1_G, g\}\,. \end{array}$$

Proposição 2.31 *A função $\phi : G \to \mathscr{F}(P_{1_G}$, $g \mapsto \phi_g$ satisfaz os itens $i)$ a $iii)$ do corolário* **??** *e, portanto, existe uma única representação $\Lambda : S(G) \to \mathscr{F}(P_1(G))$ tal que $\Lambda([g]) = \phi_g$*

Prova:

i)

$$\phi_{g^{-1}}\phi_g\phi_h(E) = \phi_{g^{-1}}\phi_g(hE \cup \{h, 1_G\})$$

$$= \phi_{g^{-1}}(ghE \cup \{g, gh, 1_G\})$$
$$= hE \cup \left\{g^{-1}, h, 1_G\right\}$$

Por outro lado,

$$\phi_{g^{-1}}\phi_{gh}(E) = \phi_{g^{-1}}(ghE \cup \{gh, 1_G\})$$
$$= hE \cup \left\{g^{-1}, h, 1_G\right\}$$

ii)

$$\phi_g\phi_h\phi_{h^{-1}}(E) = \phi_g\phi_h(h^{-1}E \cup \left\{1_G, h^{-1}\right\})$$
$$= \phi_g(E \cup \{1_G, h\})$$
$$= gE \cup \{g, gh, 1_G\}$$

Por outro lado,

$$\phi_{gh}\phi_{h^{-1}}(E) = \phi_{gh}(h^{-1}E \cup \left\{h^{-1}, 1_G\right\})$$
$$= gE \cup \{g, gh, 1_G\}$$

iii) $\phi_g\phi_{1_G}(E) = \phi_g(E \cup \{1_G\}) = gE \cup \{g, 1_G\} = \phi_g(E)$

□

Obs. 2.32 *Note que* $\Lambda(\epsilon_g)(E) = \Lambda([g][g^{-1}])(E) = \phi_g\phi_{g^{-1}}(E) = \phi_g(g^{-1}E \cup \{g^{-1}, 1_G\}) = E \cup \{g, 1_G\}$. *Daí segue, para* $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]$ *que*

$$\Lambda(\alpha)(\{1_G\}) = \{1_G, g_1, g_2, ..., g_n, h\}$$

Proposição 2.33 *Todo* $\alpha \in S(G)$ *admite uma única decomposição* $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]$, *a menos da ordem dos* $g_i's$

Prova: Considere $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]$. Suponha que exista outra decomposição $\alpha = \epsilon_{h_1}\epsilon_{h_2}...\epsilon_{h_m}[k]$. Aplicando a função grau em ambos os casos, temos $\delta(\alpha) = h$ e $\delta(\alpha) = k$, o que implica $h = k$. Aplicando a função Λ temos, no primeiro caso

$$\Lambda(\alpha)(\{1_G\}) = \{1_G, g_1, g_2, ..., g_n, h\}$$

Já no segundo caso, obtemos

$$\Lambda(\alpha)(\{1_G\}) = \{1_G, h_1, h_2, ..., h_m, h\}$$

O que implica $\{g_1, g_2, ..., g_n\} = \{h_1, h_2, ..., h_m\}$ □

Teorema 2.34 *Seja G um grupo, então $S(G)$ é um semigrupo inverso.*

Prova: Suponha que α admita um outro inverso β, além de α^*, tal que $\alpha\beta\alpha = \alpha$ e $\beta\alpha\beta = \beta$. Considere $\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]$ e $\beta^* = \epsilon_{h_1}\epsilon_{h_2}...\epsilon_{h_m}[k]$, assim, $\beta = [k^{-1}]\epsilon_{h_1}\epsilon_{h_2}...\epsilon_{h_m}$. Então

$$h = \delta(\alpha) = \delta(\alpha\beta\alpha) = hk^{-1}h \Rightarrow h = k.$$

Também

$$\alpha = \alpha\beta\alpha = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h][h^{-1}]\epsilon_{h_1}\epsilon_{h_2}...\epsilon_{h_m}\epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h] = \epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}\epsilon_{h_1}\epsilon_{h_2}...\epsilon_{h_m}[h].$$

Da unicidade da decomposição padrão, obtêm-se $\{g_1, g_2, ..., g_n, h_1, h_2, ..., h_m\} = \{g_1, g_2, ..., g_n\}$. O que implica

$$\{h_1, h_2, ..., h_m\} \subseteq \{g_1, g_2, ..., g_n\}.$$

Analogamente, fazendo $\beta^*\alpha^*\beta^* = \beta^*$, obtêm-se

$$\{g_1, g_2, ..., g_n\} \subseteq \{h_1, h_2, ..., h_m\}.$$

E concluímos que $\beta = \alpha^*$ □

Antes de enunciarmos o próximo teorema, lembre que $\tilde{G}^R = \{(A, g) \in P_{1G} \times G : g \in A\}$ é monóide inverso com a operação $(A, g)(B, h) = (A \cup gB, gh)$.

Teorema 2.35 *Seja G um grupo. O Semigrupo de Exel $S(G)$ é isomorfo ao monóide $\tilde{G}^R$.*

Prova: Considere G um grupo e a seguinte função:

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \tilde{G}^R \\ & g & \longmapsto & (\{1_G, g\}, g). \end{array}$$

Note que $\varphi(1_G) = (\{1_G\}, 1_G) = 1_{\tilde{G}^R}$ e

$$\varphi(g)\varphi(h)\varphi(h^{-1}) = (\{1_G, g\}, g)(\{1_G, h\}, h)(\{1_G, h^{-1}\}, h^{-1})$$

$$= (\{1_G, g\}, g)(\{1_G, h\}, 1_G)$$
$$= (\{1_G, g, gh\}, g).$$

Por outro lado,

$$\varphi(gh)\varphi(h^{-1}) = (\{1_G, gh\}, gh)(\{1_G, h^{-1}\}, h^{-1})$$
$$= (\{1_G, g, gh\}, g).$$

Analogamente mostra-se que $\varphi(g^{-1})\varphi(g)\varphi(h) = \varphi(g^{-1})\varphi(gh)$. Portanto, existe um único homomorfismo $\phi : S(G) \to \tilde{G}^R$ que estende φ.

Daí,

$$\phi(\epsilon_g) = \phi([g])\phi([g^{-1}])$$
$$= (\{1_G, g\}, g)(\{1_G, g^{-1}\}, g^{-1})$$
$$= (\{1_G, g\}, 1_G).$$

- ϕ é injetora. De fato, seja $\epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h] \in S(G)$. Então,

$$\phi(\epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h]) = (\{1_G, g_1\}, 1_G)(\{1_G, g_2\}, 1_G)...(\{1_G, g_n\}, 1_G)(\{1_G, h\}, h) =$$
$$= (\{1_G, g_1, g_2, ..., g_n, h\}, h).$$

  Logo, se dois elementos de $S(G)$ possuem a mesma imagem por ϕ em $\tilde{G}^R$, então eles possuem a mesma forma padrão e, portanto, são iguais.

  Portanto, $\epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[h] = [1_G] = 1_{S(G)}$.

- ϕ é sobrejetora: Seja $(A, g) \in \tilde{G}^R$ com $A = \{1_G, g, g_1, g_2, ..., g_n\}$ Então,

$$(A, g) = \phi(\epsilon_{g_1}\epsilon_{g_2}...\epsilon_{g_n}[g]).$$

□

Outra demonstração desse resultado pode ser encontrado em [9].

2.5 Ações de Semigrupos Inversos e Ações Parciais de Grupos

Nessa seção, iremos mostrar um dos resultados mais importantes do trabalho, que relaciona ações parciais de um grupo G com ações do Semigrupo de Exel $S(G)$, obtido a partir do mesmo grupo. Para tal, como de praxe, precisamos de alguns resultados preliminares, em especial, precisamos começar dizendo o que é uma ação parcial.

Definição 2.36 *Uma **ação parcial** θ **de um grupo** G **em um conjunto** X é uma coleção de bijeções $\theta_g : D_{g^{-1}} \to D_g$, com D_g subconjunto de X, para todo $g \in G$, satisfazendo, para $g, h \in G$:*

(AP1) $D_{1_G} = X$ *e* θ_{1_G} *é a função identidade de* X

(AP2) $\theta_g(D_{g^{-1}} \cap D_h) = D_g \cap D_{gh}$

(AP3) $\theta_g \circ \theta_h = \theta_{gh}$ *em* $D_{h^{-1}} \cap D_{h^{-1}g^{-1}}$

Exemplo 2.37 *Toda ação (global) de um grupo G em um conjunto X é também uma ação parcial. Basta notar que, para todo $g \in G$, temos $D_g = X$ e $\theta_g(x) = g \cdot x$.*

Exemplo 2.38 *Se G age (globalmente) em X e Y é subconjunto de X, então G age parcialmente em Y.*

Considere uma ação de G em X. Para cada $g \in G$ associamos uma bijeção $\beta_g : X \to X$ definida por $\beta_g(x) = g \cdot x$.

Seja Y um subconjunto de X. Defina $\theta_g : \beta_{g^{-1}}(Y) \cap Y \to Y \cap \beta_g(Y)$ por $\theta_g = \beta_g$. Assim, G age parcialmente em Y.

De fato, provemos, como exemplo, a propriedade (AP2):

$$\begin{aligned}
\theta_g(D_{g^{-1}} \cap D_h) &= \beta_g((\beta_{g^{-1}}(Y) \cap Y) \cap (\beta_h(Y) \cap Y)) \\
&= (\beta_g\beta_{g^{-1}}(Y) \cap \beta_g Y) \cap (\beta_g\beta_h(Y) \cap \beta_g Y) \\
&= ((Y) \cap \beta_g Y) \cap (\beta_{gh}(Y) \cap \beta_g Y) \\
&= D_g \cap D_{gh}
\end{aligned}$$

Para mais detalhes veja [3] *e* [7].

Proposição 2.39 *Sejam G um grupo e X um conjunto. Uma função $\theta : G \to \mathscr{I}(X)$ define uma ação parcial de G em X se, e somente se, tem-se para todo $g, h \in G$*

i) $\theta_g\theta_h\theta_{h^{-1}} = \theta_{gh}\theta_{h^{-1}}$

ii) $\theta_{1_G} = id_X$

iii) $\theta_{g^{-1}}\theta_g\theta_h = \theta_{g^{-1}}\theta_{gh}$.

Prova: Para mostrar a volta do teorema, tome $g = h^{-1}$ em $i)$. Assim, $\theta_{h^{-1}}\theta_h\theta_{h^{-1}} = \theta_{1_G}\theta_{h^{-1}} = \theta_{h^{-1}}$. Trocando h por h^{-1}, obtemos $\theta_h\theta_{h^{-1}}\theta_h = \theta_h$. O que implica $\theta_{h^{-1}} = \theta_h^*$.

Agora, defina $D_h = im\theta_h$, então $dom\theta_h = im\theta_h^* = im\theta_{h^{-1}} = D_{h^{-1}}$. O que implica que θ_h é função de $D_{h^{-1}}$ em D_h

Para provar a propriedade $(AP2)$, tome $g, h \in G$. Como

$$\theta_{h^{-1}}\theta_{g^{-1}} = \theta_{h^{-1}}\theta_{g^{-1}}\theta_g\theta_{g^{-1}} = \theta_{h^{-1}g^{-1}}\theta_g\theta_{g^{-1}},$$

$$dom(\theta_{h^{-1}}\theta_{g^{-1}}) = \theta_g(D_{g^{-1}} \cap D_h)$$

e

$$dom(\theta_{h^{-1}g^{-1}}\overbrace{\theta_g\theta_{g^{-1}}}^{id_{D_g}}) = D_g \cap D_{gh},$$

vale a propriedade.

Note que as propriedades $(AP1)$ e $(AP3)$ são obtidas imediatamente de $ii)$ e $iii)$.

Já para mostrar a primeira parte do teorema, se $\theta = (\{D_g\}_{g\in G}, \{\theta_g : D_{g^{-1}} \to D_g\}_{g\in G})$ é ação parcial de G em X, para $g, h \in G$, temos

(AP1) $D_{1_G} = X$ e θ_{1_G} é a função id de X (o que prova, imediatamente, o item $ii)$)

(AP2) $\theta_g(D_{g^{-1}} \cap D_h) = D_g \cap D_{gh}$

(AP3) $\theta_g \circ \theta_h = \theta_{gh}$ em $D_{h^{-1}} \cap D_{h^{-1}g^{-1}}$

Com isso, provemos o item $i)$ (o item $iii)$ é análogo). Observe que $dom(\theta_g\theta_h) = \theta_h^{-1}[D_{g^{-1}} \cap D_h] = D_{h^{-1}} \cap D_{(gh)^{-1}}$

Daí, segue que

$$\begin{aligned} dom(\theta_g\theta_h\theta_{h^{-1}}) &= (\theta_{h^{-1}})^{-1}[dom(\theta_g\theta_h) \cap im\theta_{h^{-1}}] \\ &= \theta_h[D_{h^{-1}} \cap D_{(gh)^{-1}} \cap D_{h^{-1}}] \end{aligned}$$

$$= \theta_h[D_{h^{-1}} \cap D_{(gh)^{-1}}]$$
$$\overset{AP2}{=} D_h \cap D_{g^{-1}}$$

Por outro lado,

$$dom(\theta_{(gh)}\theta_{h^{-1}}) = (\theta_{h^{-1}})^{-1}[dom(\theta_{gh}) \cap im\theta_{h^{-1}}]$$
$$= \theta_h[D_{(gh)^{-1}} \cap D_{(h)^{-1}}]$$
$$\overset{AP2}{=} D_h \cap D_{h(gh)^{-1}}$$
$$= D_h \cap D_{g^{-1}}$$

Assim, tomando $x \in D_{h^{-1}} \cap D_{h^{-1}g^{-1}}$, temos $x = \theta_{h^{-1}}\theta_h(x) = \theta_{h^{-1}}(y)$, onde $y = \theta_h(x)$. Então,

$$\theta_g\theta_h\theta_{h^{-1}}(y) = \theta_g\theta_h\overbrace{\theta_{h^{-1}}\theta_h(x)}^{x} \overset{AP3}{=} \theta_{gh}\theta_{h^{-1}}(y),$$

o que implica $\theta_g\theta_h\theta_{h^{-1}} = \theta_{gh}\theta_{h^{-1}}$

□

Definição 2.40 *Uma **ação** de um semigrupo inverso S em um conjunto X é um homomorfismo $\pi : S \to \mathscr{I}(X)$.*

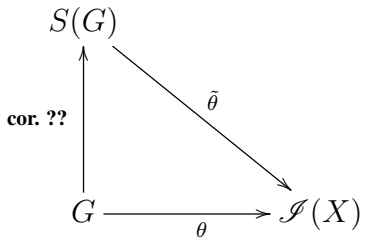
Agora, finalmente, podemos enunciar o importante teorema que relaciona ações parciais de G em X e ações de $S(G)$ em X.

Teorema 2.41 *Para todo grupo G e qualquer conjunto X, existe uma correspondência biunívoca*

$$\{\text{ações parciais de } G \text{ em } X\} \longleftrightarrow \{\text{ações de } S(G) \text{ em } X\}.$$

Prova:

Observe que o corolário **??** nos diz que homomorfismos de $S(G)$ em $\mathscr{I}(X)$ estão em correspondência bionívoca com funções de G em $\mathscr{I}(X)$, que satisfazem as propriedades $i)$ a $iii)$ da referida proposição. Logo, pela proposição anterior (**??**), tais funções correspondem à ações parciais de G em X. O diagrama abaixo ilustra tal resultado:



$$\updownarrow \textbf{prop. ??}$$

$$G \xrightarrow[\theta]{} \mathscr{I}(X)$$

□

2.6 Álgebra de Grupo

Nas próximas seções, mostraremos importantes resultados acerca de estruturas de módulos e anéis, ou álgebras, definidas a partir de um grupo. Tais resultados serão essenciais para a compreensão do capítulo seguinte. Inicialmente, temos por objetivo mostrar a conexão entre representações de grupo e álgebras de grupo para, depois, apresentar os resultados mencionados. No que segue, K denotará um anel comutativo qualquer e, quando estivermos falando de módulos sobre um anel, será sempre módulo à esquerda. Portanto, simplificaremos a linguagem chamando apenas por módulo.

Definição 2.42 *Seja G um grupo multiplicativo. Então, definimos a* ***álgebra de grupo*** *KG como segue. Seu grupo aditivo é o K-módulo livre tendo uma base formada por elementos de G. Assim, cada elemento tem uma expressão única na forma $\sum_{g\in G} a_g g$, onde $a_g \in K$ e somente um número finito de a_g pode ser não nulo. Se g e h são elementos da base, isto é, $g, h \in G$, defina seu produto em KG como sendo seu produto gh em G. O produto de dois elementos de KG é definido pela extensão por linearidade*

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{z\in G}\left(\sum_{gh=z} a_g b_h\right) z.$$

Vejamos que, assim definido, o produto em KG é K-bilinear, associativo e possui elemento neutro $1_{KG} \neq 0_G$ (onde $1_{KG} = 1_K 1_G$) tal que $1_{KG}a = a1_{KG} = a$ para todo $a \in KG$.

Antes, observe que a em KG é, na verdade, $a1_G$ e, assim, ga é uma abreviação de $(1_K g)(a1_G)$. Logo, pela definição $ga = (1_K g)(a1_G) = 1_K ag1_G = ag$.

K-bilinear:

$$\left(\alpha_1\left(\sum_{g\in G} a_g^1 g\right) + \alpha_2\left(\sum_{g\in G} a_g^2 g\right)\right)\left(\sum_{h\in G} b_h h\right) =$$

$$= \left(\left(\sum_{g\in G} \alpha_1 a_g^1 g\right) + \left(\sum_{g\in G} \alpha_2 a_g^2 g\right)\right)\left(\sum_{h\in G} b_h h\right) =$$

$$= \left(\sum_{g\in G}(\alpha_1 a_g^1 + \alpha_2 a_g^2)g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{z\in G}\left(\sum_{gh=z}(\alpha_1 a_g^1 + \alpha_2 a_g^2)b_h\right) z =$$

$$= \sum_{z\in G}\left(\left(\sum_{gh=z}\alpha_1 a_g^1 b_h\right) z + \left(\sum_{gh=z}\alpha_2 a_g^2 b_h\right)\right) z =$$

$$= \sum_{z\in G}\left(\sum_{gh=z}\alpha_1 a_g^1 b_h\right) z + \sum_{g\in G}\left(\sum_{gh=z}\alpha_2 a_g^2 b_h\right) z =$$

$$= \alpha_1 \sum_{z\in G}\left(\sum_{gh=z} a_g^1 b_h\right) z + \alpha_2 \sum_{z\in G}\left(\sum_{gh=z} a_g^2 b_h\right) z =$$

$$= \alpha_1\left(\sum_{g\in G} a_g^1 g\right)\left(\sum_{h\in G} b_h h\right) + \alpha_2\left(\sum_{g\in G} a_g^2 g\right)\left(\sum_{h\in G} b_h h\right)$$

Também,

$$\left(\sum_{g\in G} a_g g\right)\left(\beta_1\left(\sum_{h\in G} b_h^1 h\right) + \beta_2\left(\sum_{h\in G} b_h^2 h\right)\right) =$$

$$= \left(\sum_{g\in G} a_g g\right)\left(\left(\sum_{h\in G}\beta_1 b_h^1 h\right) + \left(\sum_{h\in G}\beta_2 b_h^2 h\right)\right) =$$

$$= \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G}(\beta_1 b_h^1 + \beta_2 b_h^2)h\right) = \sum_{g\in G}\left(\sum_{gh=z} a_g(\beta_1 b_h^1 + \beta_2 b_h^2)\right) z =$$

$$= \sum_{z\in G}\left(\sum_{gh=z} a_g\beta_1 b_h^1\right) z + \sum_{z\in G}\left(\sum_{gh=z} a_g\beta_2 b_h^2\right) z = \beta_1\sum_{z\in G}\left(\sum_{gh=z} a_g b_h^1\right) z + \beta_2\sum_{z\in G}\left(\sum_{gh=z} a_g b_h^2\right) z =$$

$$= \beta_1\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h^1 h\right) + \beta_2\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h^2 h\right)$$

Associativo:

$$\left(\sum_{g\in G} a_g g\right)\left(\left(\sum_{g\in G} b_h h\right)\left(\sum_{i\in G} c_i i\right)\right) = \left(\sum_{g\in G} a_g g\right)\left(\sum_{z\in G}\left(\sum_{hi=z} b_h c_i\right) z\right) =$$

$$= \sum_{w\in G}\left(\sum_{gz=w} a_g\left(\sum_{hi=z} b_h c_i\right)\right) w = \sum_{w\in G}\left(\sum_{g(hi)=w} a_g(b_h c_i)\right) w =$$

$$= \sum_{w\in G}\left(\sum_{(gh)i=w}(a_g b_h)c_i\right) w = \sum_{w\in G}\left(\sum_{z'i=w}\left(\sum_{gh=z'}(a_g b_h)c_i\right)\right) w =$$

$$= \left(\sum_{z'\in G}\left(\sum_{gh=z'} a_g b_h\right) z'\right)\left(\sum_{i\in G} c_i i\right) = \left(\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right)\right)\left(\sum_{i\in G} c_i i\right)$$

$\exists 1_{KG}$**:** Tome $1_{KG} = 1_K 1_G$. Então,

$$1_K 1_G \left(\sum_{g \in G} a_g g \right) = \left(\sum_{g \in G} 1_K a_g 1_G g \right) = \left(\sum_{g \in G} a_g g \right).$$

E,

$$\left(\sum_{g \in G} a_g g \right) 1_K 1_G = \left(\sum_{g \in G} a_g 1_K g 1_G \right) = \left(\sum_{g \in G} a_g g \right).$$

Proposição 2.43 *Sejam G um grupo, A uma K-álgebra, e $U(A)$ o grupo multiplicativo dos elementos invertíveis de A. Todo homomorfismo de grupos $\phi : G \to U(A)$ possui uma única extensão a um homomorfismo de K-álgebras $\Phi : KG \to A$.*

Prova: Se existe tal Φ, então

$$\Phi(\sum_{g \in G} k_g g) = \sum_{g \in G} k_g \Phi(g) = \sum_{g \in G} k_g \phi(g).$$

Isso mostra a unicidade de Φ.

Agora, defina Φ pela expressão obtida acima, isto é,

$$\Phi(\sum_{g \in G} k_g g) = \sum_{g \in G} k_g \phi(g).$$

Esta Φ é K-linear pois é a única extensão K-linear da aplicação da base G no K-módulo A que leva g em $\phi(g)$.

É fácil de ver que Φ preserva o produto e é claro que preserva a unidade. □

Corolário 2.44 *Um homomorfismo de grupos $\phi : G \to G'$ se estende de modo único a um morfismo de K-álgebras $\Phi : KG \to KG'$.*

Prova: Como G' está contido em $U(KG')$, segue direto da proposicao anterior. □

Definição 2.45 *Seja K um corpo. Então, uma K-**representação** de um grupo G é um homomorfismo*

$$\sigma : G \to GL(V)$$

onde V é um espaço vetorial sobre um corpo K.

Proposição 2.46 *Cada K-representação $\sigma : G \to GL(V)$ fornece a V a estrutura de um KG-módulo. Reciprocamente, cada KG-módulo V determina uma K-representação.*

Prova: Para mostrar a primeira parte da proposição, considere $\sigma : G \to GL(V)$ um homomorfismo, denote $\sigma(g) : V \to V$ por σ_g e defina uma ação $KG \times V \to V$ por $\left(\sum_{g\in G} a_g g\right) v = \left(\sum_{g\in G} a_g \sigma_g(v)\right)$. Observe que de fato esta função é uma ação pois $(1_{KG})v = \sigma_{1_{KG}}(v) = Id_V(v) = v$ e também

$$\sum_{g\in G} a_g g \left(\left(\sum_{h\in G} b_h h\right) v\right) = \sum_{g\in G} a_g g \left(\sum_{h\in G} b_h \sigma_h(v)\right) = \sum_{z\in G} \left(\sum_{gh=z} a_g b_h\right) \sigma_z(v).$$

Por outro lado,

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) v = \left(\sum_{z\in G}\left(\sum_{gh=z} a_g b_h\right) z\right) v = \sum_{z\in G}\left(\sum_{gh=z} a_g b_h\right)\sigma_z(v).$$

Logo, $\sum_{g\in G} a_g g \left(\left(\sum_{h\in G} b_h h\right) v\right) = \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) v$.

Para verificar que V é um KG-módulo, basta verificar as propriedades relacionadas ao produto por escalar em KG, uma vez que as propriedades da adição são imediatas por ser V um espaço vetorial sobre K.

i) $1_{KG}v = v$ é imediato da ação definida, bem como a próxima propriedade.

ii) $\left(\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right)\right) v = \left(\sum_{g\in G} a_g g\right)\left(\left(\sum_{h\in G} b_h h\right) v\right)$

iii)

$$\left(\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right)\right) v = \left(\sum_{g\in G}(a_g + b_g) g\right) v = \sum_{ginG}(a_g + b_g) g\sigma_g(v) =$$

$$= \sum_{g\in G} a_g\sigma_g(v) + \sum_{h\in G} b_h\sigma_h(v) = \left(\sum_{g\in G} a_g g\right) v + \left(\sum_{h\in G} b_h h\right) v$$

iv)

$$\left(\sum_{g\in G} a_g g\right)(v_1 + v_2) = \sum_{g\in G} a_g\sigma_g(v_1 + v_2) =$$

$$= \sum_{g\in G} a_g\sigma_g(v_1) + \sum_{g\in G} a_g\sigma_g(v_2) = \left(\sum_{g\in G} a_g g\right) v_1 + \left(\sum_{g\in G} a_g g\right) v_2$$

Já para verificarmos a outra parte do teorema, suponha V um KG-módulo. Se $g \in G$, então $v \mapsto gv$ define uma transformação linear $T_g : V \to V$. De fato,

$$T_g(av_1 + v_2) = g(av_1 + v_2) = gav_1 + gv_2 =$$

$$= agv_1 + gv_2 = aT_g v_1 + T_g v_2.$$

Claramente $(T_g)^{-1} = T_{g^{-1}}$. Defina

$$\begin{array}{rccc} \sigma: & G & \longrightarrow & GL(V) \\ & g & \longmapsto & T_g \end{array}$$

Então, σ é uma K-representação. Com efeito, $\sigma(gh)(v) = T_{gh}(v) = gh(v) = gT_h(v) = T_g T_h(v)$ para todo $v \in V$. Logo $T_{gh} = T_g T_h$, o que implica $\sigma(gh) = \sigma(g)\sigma(h)$. □

2.7 Álgebra de Monóide

Definição 2.47 *Seja S um monóide. Então, definimos a **álgebra de monóide** KS como segue. Seu grupo aditivo é o K-módulo livre tendo uma base formada por elementos de S. Assim, cada elemento tem uma expressão única na forma $\sum_{s\in S} a_s s$, onde $a_s \in K$ e somente um número finito de a_s pode ser não nulo. Se s e t são elementos da base, isto é, $s, t \in S$, defina seu produto em KS como sendo seu produto st em S. O produto de dois elementos de KS é definido pela extensão por linearidade*

$$\left(\sum_{s\in S} a_s s\right)\left(\sum_{t\in S} b_t t\right) = \sum_{u\in S}\left(\sum_{st=u} a_s b_t\right) u.$$

A prova de que KS é uma K-álgebra é idêntica à feita para KG, já que, naquela prova, os inversos dos elementos de G não são usados.

As provas da proposição e do corolário que seguem são análogas as provas da proposição **??** e corolário **??**.

Proposição 2.48 *Sejam S um monóide e A uma K-álgebra. Considerando A como monóide multiplicativo, todo homomorfismo de monóides $\phi : S \to A$ possui uma única extensão a um homomorfismo de K-álgebras $\Phi : KS \to A$.*

Corolário 2.49 *Se S e S' são monóides e $\phi : S \to S'$ é um homomorfismo, então existe uma única extensão a um homomorfismo de K-álgebras $\Phi : KS \to KS'$.*

2.8 Álgebra de Grupo Semissimples

Definição 2.50 *Um R-módulo M é **simples** se $M \neq \{0\}$ e M não tem submódulos próprios não nulos, ou seja, os únicos submódulos de M são $\{0\}$ e M.*

Definição 2.51 *Seja R um anel, possivelmente não-comutativo. Um R-módulo é **semissimples** se ele é uma soma direta de módulos simples. Um anel R é **semissimples** se ele é soma direta de ideais minimais (à esquerda), ou seja, se R é um R-módulo semissimples.*

Proposição 2.52 *Um R-módulo é semissimples se, e somente se, cada submódulo de M é um somando direto.*

Prova: Veja [12]. □

Teorema 2.53 ***(Maschke)*** *Sejam G um grupo finito e K um corpo cuja característica não divide $|G|$. Então KG é um anel semissimples.*

Prova: Precisamos mostrar que cada ideal I de KG é um somando direto. Como K é um corpo, KG é um espaço vetorial sobre K e I é um subespaço. Então, I é um somando direto enquanto espaço vetorial, logo existe um subespaço V, que pode não ser um ideal de KG, com $KG = I \oplus V$. Logo, existe uma transformação K-linear $d : KG \to I$ com $d(b) = b$ para todo $b \in I$ e com $Ker(d) = V$. Assim, cada $u \in KG$ tem uma expressão única na forma $u = b + v$, onde $b \in I$ e $v \in V$, e $d(u) = b$. Segue que I é um somando direto de KG se, e somente se, é um retrato, isto é, se, e somente se, existe um KG-homomorfismo $D : KG \to I$ com $D(u) = u$ para todo $u \in I$. Defina $D : KG \to KG$ por

$$D(u) = \frac{1}{|G|} \sum_{x \in G} xd(x^{-1}u)$$

para todo $u \in KG$. Note que $|G| \neq 0$ em K. É óbvio que D é um K-homomorfismo pois d é K-homomorfismo. Além do mais,

i) $imD \subseteq I$:

Se $u \in KG$ e $x \in G$, então $d(x^{-1}u) \in I$ pois $imd \subseteq I$, e $xd(x^{-1}u) \in I$ pois I é um ideal. Portanto $D(u) \in I$, para cada termo da soma na definição de $D(u)$.

ii) Se $b \in I$, então $D(b) = b$:

Se $b \in I$, para $x^{-1}b$, temos $d(x^{-1}b) = x^{-1}b$, pois $x^{-1}b \in I$ por ser I um ideal. Portanto, $xd(x^{-1}b) = xx^{-1}b = b$ e

$$D(b) = \frac{1}{|G|}\sum_{x\in G} xd(x^{-1}b) = \frac{b}{|G|}\sum_{x\in G} 1 = \frac{b}{|G|}|G| = b$$

iii) D é um KG-homomorfismo:

Como d é um K-homomorfismo, $D(u+u') = D(u) + D(u')$ verifica-se trivialmente, bem como $D(ku) = kD(u)$ para todo $k \in K$ e todo $u \in KG$. Resta, portanto, provar que $D(gu) = gD(u)$ para todo $g \in G$ e todo $u, u' \in KG$:

$$gD(u) = \frac{g}{|G|}\sum_{x\in G} xd(x^{-1}u) = \frac{1}{|G|}\sum_{x\in G} gxd(x^{-1}u) =$$

$$= \frac{1}{|G|}\sum_{x\in G} gxd(x^{-1}g^{-1}gu) = \frac{1}{|G|}\sum_{y=gx\in G} yd(y^{-1}gu) = D(gu)$$

□

Teorema 2.54 ***(Wedderburn-Artin I)*** *Um anel R é semissimples se, e somente se, R é isomorfo a um produto direto de anéis de matrizes sobre anéis de divisão.*

Prova: Para a demonstração deste teorema, bem como do próximo, e para mais detalhes, veja [12]. □

Teorema 2.55 ***(Wedderburn-Artin II)*** *Cada anel R semissimples é um produto direto*

$$R \cong Mat_{n_1}(\Delta_1) \times Mat_{n_2}(\Delta_2) \times ... \times Mat_{n_m}(\Delta_m)$$

onde $n_i \geq 1$, Δ_i é um anel de divisão e os números m e $n_i's$, assim como os anéis de divisão $\Delta_i's$, são unicamente determinados por R.

Teorema 2.56 ***(Molien)*** *Seja G um grupo finito e K um corpo algebricamente fechado cuja característica não divide a ordem de G. Então*

i) $KG \cong Mat_{n_1}(K) \times Mat_{n_2}(K) \times ... \times Mat_{n_k}(K)$

ii) $|G| = n_1^2 + n_2^2 + ... + n_k^2$

para algum $k \in \mathbb{Z}$.

Prova: Seja KG uma K-álgebra de grupo que tem dimensão finita pois G é finito. Pelo teorema de Wedderburn-Artin II, temos que

$$KG \cong \prod_{i=1}^{n} Mat_{n_i}(\Delta_i)$$

com Δ_i sendo K-álgebra. Aceitando que cada Δ_i é K-álgebra, podemos identificar K com a subálgebra $K1_{\Delta_i}$, e com essa identificação queremos mostrar que $\Delta_i = K$. Temos que $dim(\Delta_i) \leq dim(KG) \leq \infty$ para todo $i = 1, 2, ..., n$. Então, para todo i, $\Delta_i = K$ como álgebras (Nesse caso, K identifica a álgebra $K1_{\Delta_i}$).

De fato, suponha por absurdo que $K \subsetneq \Delta_i$, tome $\alpha \in \Delta_i \setminus K$ para todo $i = 1, 2, ..., n$.

Então, para

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[\alpha] \right\},$$

temos que

$$K \subseteq K(\alpha) \subseteq \Delta_i,$$

o que implica $dim(K(\alpha)) \leq dim(\Delta_i) \leq \infty$.

Agora, suponha $dim(K(\alpha)) = n$. O conjunto $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ possui $n+1$ elementos, logo é um conjunto linearmente dependente. Então, existem $a_0, a_1, ..., a_n \in K$, com pelo menos um a_i não nulo, tais que

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0.$$

Então α é raíz do polinômio não nulo $\sum_{i=0}^{n} a_i x^i \in K[x]$. Mas K é algebricamente fechado, logo $\alpha \in K$, uma contradição. O que prova o item $i)$.

Já o item $ii)$ verifica-se imediatamente usando as dimensões das K-álgebras.

□

2.9 Módulos Simples da Álgebra $Mat_{n_1}(\mathbb{C}) \times ... \times Mat_{n_k}(\mathbb{C})$

Nessa seção, restringiremos o corpo que estamos trabalhando ao corpo dos complexos $\mathbb{C}$, pois temos por objetivo entender melhor os módulos simples de uma álgebra semissimples da forma $R = Mat_{n_1}(\mathbb{C}) \times ... \times Mat_{n_k}(\mathbb{C})$.

Lema 2.57 ***(de Schur)*** *Qualquer homomorfismo não nulo entre dois R-módulos simples é um isomorfismo.*

Prova: Sejam M e N R-módulos simples e seja $\Phi : M \to N$ um homomorfismo. Como $Ker(\Phi)$ é um submódulo de M e diferente de M pois $\Phi \neq 0$, temos, por ser M simples, que $Ker(\Phi) = 0$. Analogamente temos $im\Phi = N$. □

Proposição 2.58 *Seja R um anel semissimples tal que*

$$R = S_1 \oplus S_2 \oplus ... \oplus S_n$$

com S_i R-módulo simples para $i = 1, ..., n$, podendo haver repetições entre os S_i's. Então, se S é R-módulo simples, $S \cong S_i$ para algum i.

Prova: Seja $x \in S$ não nulo. Então $S = Rx$. De fato, claramente $Rx \subseteq S$ pois S é R-módulo e, como S é simples, temos $Rx = S$. Considere

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & S \\ & r & \longmapsto & rx \end{array}$$

então φ é um epimorfismo, pois é linear e sobrejetora.

Temos $Hom_R(R, S) \cong \bigoplus_{i=1}^{n} Hom(S_i, S)$. Como φ é epimorfismo, $Hom_R(R, S) \neq 0$. Logo, existe i tal que $Hom(S_i, S) \neq 0$. Portanto, Pelo Lema de Schur, $S \cong S_i$. □

No que segue, e_{ij} denota a matriz elementar que possui o elemento 1 na entrada ij e 0 nas demais entradas.

Agora, vejamos quais são os módulos de $Mat_n(\mathbb{C})$. Claramente podemos escrever $Mat_n(\mathbb{C})$ como soma direta de $\mathbb{C}$-subespaços:

$$Mat_n(\mathbb{C}) = C_1 \oplus C_2 \oplus ... \oplus C_n,$$

onde

$$C_j = \langle e_{ij} : i = 1, 2, ...n \rangle = \begin{pmatrix} 0 & \dots & 0 & a_{1j} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2j} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nj} & 0 & \dots & 0 \end{pmatrix}$$

onde $a_{ij} \in \mathbb{C}$ para todo $i, j = 1, 2, ..., n$. Observe também que cada C_j é um ideal à esquerda e, portanto, essa decomposição é em soma direta de $Mat_n(\mathbb{C})$-submódulos.

Proposição 2.59 *A aplicação*

$$\begin{array}{rccc} \theta_{j,k}: & C_j & \longrightarrow & C_k \\ & \sum_{l=1}^{n} b_l e_{lj} & \longmapsto & \sum_{l=1}^{n} b_l e_{lk} \end{array}$$

é um isomorfismo de $Mat_n(\mathbb{C})$-módulos entre C_j e C_k.

Prova: $\theta_{j,k}$ é um homomorfismo entre C_j e C_k com inversa $(\theta_{j,k})^{-1} = \theta_{k,j}$. Portanto é um isomorfismo. De fato, primeiro observe que

$$\begin{aligned} \sum_{k,l=1}^{n} a_{kl}e_{kl}.\sum_{i=1}^{n} b_i e_{ij} &= \sum_{l,k,i=1}^{n} a_{kl}b_i e_{kl}e_{ij} \\ &= \sum_{l,k,i=1}^{n} a_{kl}b_i\delta_{l,i}e_{kj} \\ &= \sum_{l,k=1}^{n} a_{ki}b_i e_{kj} \end{aligned}$$

Assim,

$$\begin{aligned} \theta_{j,k}(\sum_{p,q=1}^{n} a_{pq}e_{pq}.\sum_{l=1}^{n} b_i e_{ij}) &= \theta_{j,k}(\sum_{l,p=1}^{n} a_{pi}b_i e_{pj}) \\ &= \sum_{l,p=1}^{n} a_{pi}b_i e_{pk} \end{aligned}$$

Também,

$$\begin{aligned} (\sum_{p,q=1}^{n} a_{pq}e_{pq}).\theta_{j,k}(\sum_{l=1}^{n} b_i e_{ij}) &= (\sum_{p,q=1}^{n} a_{pq}e_{pq}).\sum_{l=1}^{n} b_i e_{ik} \\ &= \sum_{l,i=1}^{n} a_{pi}b_i e_{pk} \end{aligned}$$

□

Proposição 2.60 *Cada $Mat_n(\mathbb{C})$-módulo C_j é simples.*

Prova: Como todos C_j's são isomorfos entre si, basta provar somente para um deles. Neste caso, seja M um submódulo não trivial de C_j. Então M possui um vetor v não nulo na forma $v = \sum_{l=1}^{n} c_l e_{lj}$, onde pelo menos um dos c_l's é não nulo, digamos c_k. Temos

$$c_k^{-1}e_{ik}v = e_{ij} \in M.$$

Como isto vale para qualquer i e os elementos na forma e_{ij} geram C_j, temos que $M = C_j$ $\square$

Considere $R = Mat_{n_1}(\mathbb{C}) \times Mat_{n_2}(\mathbb{C}) \times ... \times Mat_{n_m}(\mathbb{C})$ com $n_i \geq 1$. Quando $n = 1$, podemos, como anéis, identificar $Mat_1(\mathbb{C})$ por $\mathbb{C}$.

Seja $I_j^k = \{0\} \times ... \times \{0\} \times C_k^{n_j} \times \{0\} \times ... \times \{0\}$ onde

$$C_k^{n_j} = \begin{pmatrix} 0 & \dots & 0 & a_{1j} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2j} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nj} & 0 & \dots & 0 \end{pmatrix} \subseteq Mat_{n_k}(\mathbb{C}).$$

para $k = 1, ..., m$.

Então, I_j^k é ideal à esquerda de R e, pela proposição **??**, é simples. Daí, temos

$$R = \bigoplus_{k=1}^{m} \bigoplus_{j=1}^{n_k} I_j^k$$

onde, pela proposição **??**, $I_j^k \cong I_{j'}^k$, para todo $1 \neq k, k', n_k$.

Portanto, pela proposição **??**, R tem exatamente m módulos simples distintos, isomorfos à $I_1^1, I_1^2, ..., I_1^k$.

Exemplo 2.61 ***(Proposição:)*** *Se G é um grupo abeliano de ordem m então $\mathbb{C}G \cong \mathbb{C}^m$.*

Pelo teorema de Molien, $\mathbb{C}G \cong Mat_{n_1}(\mathbb{C}) \times ... \times Mat_{n_k}(\mathbb{C})$. Como G é abeliano, $\mathbb{C}G$ é uma álgebra comutativa. Como $Mat_n(\mathbb{C})$ só é comutativa se $n = 1$ (e neste caso $Mat_n(\mathbb{C})$ é isomorfa a $\mathbb{C}$), segue que $n_1 = n_2 = ... = n_k = 1$. Pelo segundo item do teorema de Molien, $k = m$.

Exemplo 2.62 *Vejamos qual é a álgebra de grupo $\mathbb{C}S_3$ do grupo de permutacões S_3.*

Pela segunda parte do teorema de Molien, se $\mathbb{C}S_3 \cong Mat_{n_1}(\mathbb{C}) \times ... \times Mat_{n_k}(\mathbb{C})$, então $6 = |S_3|$ é a soma dos quadrados dos n_i. Neste caso, só existem duas soluções: ou temos $k = 6$ e $n_i = 1$ para todo i, ou temos $k = 3$ e $n_1 = n_2 = 1, n_3 = 2$ (supondo que tomemos sempre a seq $n_1, n_2, ...$ crescente). A primeira solução nos mostra que $\mathbb{C}S_3 \cong \mathbb{C}^6$. Mas $\mathbb{C}^6$ é uma álgebra comutativa e $\mathbb{C}S_3$ não é. Portanto, essa solução não está correta. Sobra, então, a segunda solução, e temos

$$\mathbb{C}S_3 \cong \mathbb{C} \times \mathbb{C} \times Mat_2(\mathbb{C}).$$

Capítulo 3

Álgebra Parcial de Grupo

Neste capítulo, estudaremos as álgebras parciais de grupos finitos, que, para um grupo G é denotada por $K_{par}(G)$.

Vimos no capítulo anterior que, se G e G' são isomorfos, então KG e KG' são algebras isomorfas, mas, em geral, a recíproca é falsa. No caso de grupos abelianos finitos (de ordem n) e de $K = \mathbb{C}$, tudo o que $\mathbb{C}G$ mantém de informação de G é a sua ordem, pois $\mathbb{C}G \simeq \mathbb{C}^n$. Neste sentido, a álgebra parcial de um grupo, torna-se uma ferramenta mais fina para dizer quando dois grupos não são isomorfos. Ou seja, se $G \neq G'$, então $K_{par}(G) \ncong K_{par}(G')$. Veremos alguns exemplos adiante, mas antes precisamos introduzir uma série de definições e resultados.

No decorrer, salve menção contrária, G é grupo finito, K é um corpo e 1_G é a identidade de G. Além do mais, padronizaremos as seguintes notações: $H \leq G$ indica que H é subgrupo de G e $H < G$ indica que H é subgrupo próprio de G, isto é, $H \leq G$ e $H \neq G$. Também usaremos as notações $(G : H)$ para denotar o índice de H em G, $[G : G]$ para o comutador de G e $\mathscr{N}(H)$ para o normalizador de H em G, ou seja,

$$[G : G] = \left\{g^{-1}h^{-1}gh \in G : g, h \in G\right\}$$

e

$$\mathscr{N}(H) = \{g \in G : gH = Hg\}.$$

A referência desse capítulo é o artigo [4], por conta disso, usaremos o mesmo conceito de soma direta de K-álgebras que os autores do mesmo:

Definição 3.1 *Se K é um corpo e $A_1, A_2, ..., A_n$ são K-álgebras, então sua **soma direta** é o K-espaço vetorial*

$$A_1 \oplus A_2 \oplus ... \oplus A_n$$

com a multiplicação

$$(a_1 + a_2 + ... + a_n)(b_1 + b_2 + ... + b_n) = (a_1b_1 + a_2b_2 + ... + a_nb_n).$$

É fácil ver que $A_1 \oplus A_2 \oplus ... \oplus A_n$ *é isomorfo ao produto direto de anéis* $A_1 \times A_2 \times ... \times A_n$ *utilizado nos capítulos anteriores. Em particular, se* A *é uma* K*-álgebra e* n *é um inteiro positivo,* nA *indicará a soma direta* $A \oplus A \oplus ... \oplus A$ *(com* n *termos), que é isomorfa ao produto* A^n*.*

3.1 Grupoides

Nesta seção, utilizaremos a definição de grupoide apresentada em [7] (mais detalhes à respeito de grupoides podem ser encontrados também em [11]), mas logo em seguida, mostraremos que esta definição é equivalente a uma definição categórica mais geral.

Definição 3.2 *Um* ***grupoide*** *é um conjunto não-vazio* Γ *munido com uma operação binária parcialmente definida, denotada por concatenação, para a qual, os axiomas usuais de um grupo valem sempre que tal operação faz sentido. Ou seja:*

i) Para cada $g, h, l \in \Gamma$*,* $g(hl)$ *existe se, e somente se,* $(gh)l$ *existe e, neste caso, eles são iguais.*

ii) Para cada $g, h, l \in \Gamma$*,* $g(hl)$ *existe se, e somente se,* gh *e* hl *existem.*

iii) Para cada $g \in \Gamma$*, existem elementos (únicos)* $d(g), i(g) \in \Gamma$ *tais que* $gd(g)$ *e* $i(g)g$ *existem e* $gd(g) = g = i(g)g$*.*

iv) Para cada $g \in \Gamma$*, existe um elemento* $g^{-1} \in \Gamma$ *tal que* $d(g) = g^{-1}g$ *e* $i(g) = gg^{-1}$*.*

Denotamos por $\Gamma^{(2)}$ *o subconjunto dos pares* $(g, h) \in \Gamma \times \Gamma$ *tais que os elementos* gh *existem.*

Um elemento $e \in \Gamma$ *é chamado uma* ***identidade*** *de* Γ *se* $e = d(g) = i(g^{-1})$*, para algum* $g \in \Gamma$*. Neste caso,* e *é chamado a* ***identidade domínio*** *de* g *e a* ***identidade imagem*** *de* g^{-1}*. Denotamos por* Γ_0 *o conjunto de todas as identidades de* Γ *e denotamos por* Γ_e *o conjunto de todos os* $g \in \Gamma$ *tais que* $d(g) = i(g) = e$*. Claramente* Γ_e *é um grupo, chamado de* ***grupo de isotropia*** *associado a* e*.*

Exemplo 3.3 *Considere o grupoide* $\Gamma(G) = \Gamma$ *cujos elementos são pares* (A, g)*, onde* $g \in G$ *e* A *é um subconjunto de* G *que contém os elementos* 1_G *e* g^{-1}*. Observe que* $1_G, g \in gA$*.*

A multiplicação de pares $(A,g)(B,h)$ *em* Γ *está definida para pares tais que* $A = hB$ *e, nesse caso, temos*

$$(hB,g)(B,h) = (B,gh).$$

O inverso do par (A,g) *é* (gA,g^{-1}) *e o domínio e imagem em* Γ *são, respectivamente* $d(A,g) = (A,1_G)$ *e* $i(A,g) = (gA,1_G)$.

Vejamos que as propriedades de grupoide são, de fato, satisfeitas:

Para cada $(A,g),(B,h),(C,i) \in \Gamma$. *Como* $h^{-1} \in B$ *e* $i^{-1} \in C$*:*

i) $((A,g),((B,h)(C,i))) \in \Gamma^{(2)} \Leftrightarrow B = iC$ *e* $A = hB \Leftrightarrow A = hiC \Leftrightarrow A = hB$ *e* $B = hC \Leftrightarrow (((A,g)(B,h)),(C,i)) \in \Gamma^{(2)}$

ii) $((A,g),((B,h)(C,i))) \in \Gamma^{(2)} \Leftrightarrow A = hB$ *e* $B = iC \Leftrightarrow A = hiC = hB$ *e* $B = iC \Leftrightarrow ((A,g),(B,h)),((B,h)(C,i)) \in \Gamma^{(2)}$

iii) $(gA,1_G)(A,g) = (A,g)\ (A,g)(A,1_G) = (A,g)$

iv) $(gA,g^{-1})(A,g) = (A,1_G)$

$(A,g)(gA,g^{-1}) = (gA,1_G)$

Observe que $(A,g) = (g^{-1}gA,g)$ *e que a unicidade é imediata para que o produto esteja definido e dê o resultado esperado.*

O lema a seguir lista algumas propriedades básicas de grupoides que utilizaremos neste trabalho. A prova pode ser encontrada em [7] e [11].

Lema 3.4 *Seja* Γ *um grupoide, então:*

i) Para cada $g \in \Gamma$*, o elemento* g^{-1} *é único satisfazendo* $g^{-1}g = d(g)$ *e* $gg^{-1} = i(g)$

ii) Para cada $g \in \Gamma$*,* $d(g^{-1}) = i(g)$ *e* $i(g^{-1}) = d(g)$

iii) Para cada $g \in \Gamma$*,* $(g^{-1})^{-1} = g$

iv) Para cada $g,h \in \Gamma$*,* $(g,h) \in \Gamma^{(2)}$ *se, e somente se,* $d(g) = i(h)$

v) Para cada $g,h \in \Gamma$*,* $(h^{-1},g^{-1}) \in \Gamma^{(2)}$ *se, e somente se,* $(g,h) \in \Gamma^{(2)}$ *e, neste caso,* $(gh)^{-1} = h^{-1}g^{-1}$

vi) Para cada $(g,h) \in \Gamma^{(2)}$*,* $d(gh) = d(h)$ *e* $i(gh) = i(g)$

vii) Para cada $e \in \Gamma_0$, $d(e) = i(e) = e$ *e* $e^{-1} = e$

viii) Para cada $(g, h) \in \Gamma^{(2)}$, $gh \in \Gamma_0$ *se, e somente se,* $g = h^{-1}$

ix) Para cada $g, h \in \Gamma$, *existe* $l \in \Gamma$ *tal que* $g = hl$ *se, e somente se,* $i(g) = i(h)$

x) Para cada $g, h \in \Gamma$, *existe* $l \in \Gamma$ *tal que* $g = lh$ *se, e somente se,* $d(g) = d(h)$

Teorema 3.5 *A definição de grupoide acima é equivalente à noção categórica de grupoide, isto é,* Γ *é grupoide (como definido acima) se, e somente se, é uma categoria pequena (ou seja, cujos elementos são conjuntos) na qual seus morfismos são isomorfismos.*

Prova: Para mostrar a primeira parte do teorema, suponha que Γ é um grupoide conforme a definição apresentada. Vejamos que $\mathscr{C}(\Gamma)$ é categoria pequena cujos morfismos são isomorfismos.

Considere $\mathscr{C}(\Gamma)_0 = \Gamma_0$, $\mathscr{C}(\Gamma)(x, y) = \{f \in \Gamma : d(f) = x, i(f) = y\}$ e a composição em $\mathscr{C}(\Gamma)$ como sendo a operação de Γ, ou seja, $f \circ g = fg$. Assim, dados $x, y, z \in \mathscr{C}(\Gamma)_0$, considere

$$\begin{array}{rccc} \cdot : & \mathscr{C}(\Gamma)(y,z) \times \mathscr{C}(\Gamma)(x,y) & \longrightarrow & \mathscr{C}(\Gamma)(x,z) \\ & (g : y \mapsto z) \times (f : x \mapsto y) & \longmapsto & (g \circ f : x \mapsto z) = g \cdot f \end{array}$$

$g \circ f$ está bem definida pelo item $iv)$ do lema anterior. Do item $i)$ da definição de grupoide, segue que a composição é associativa e, dado $x \in \mathscr{C}(\Gamma)_0$ e $f \in \mathscr{C}(\Gamma)(x, x)$, tome $x = 1_x = id_x : x \mapsto x$ em Γ. Assim, $f \circ 1_x = f$ e $1_x \circ g = g$, para todos f, g caso tais operações estajem definidas.

Para verificarmos a outra parte do teorema, suponha que $\mathscr{C}$ é uma categoria cujos objetos são conjuntos e seus morfismos são isomorfismos. Sejam $\mathscr{C}(x, y)$ o conjunto dos morfismos entre x e y pertencentes a $\mathscr{C}_0$.

Defina $\Gamma(\mathscr{C}) = \bigcup_{x,y \in \mathscr{C}_0} \mathscr{C}(x, y)$. Considere o produto $(f, g) \mapsto fg$, onde fg é dado por $fg = f \circ g$ onde $\circ$ é a composição em $\mathscr{C}$, definido quando $d(f) = i(g)$.

Desta forma, $\Gamma(\mathscr{C})^2 \subseteq \Gamma(\mathscr{C}) \times \Gamma(\mathscr{C})$ é o conjunto dos pares (f, g) tais que $d(f) = i(g)$, com inverso de f em $\Gamma(\mathscr{C})$ dado pelo inverso f^{-1} de f em $\mathscr{C}$.

Assim, temos que $d(f : x \mapsto y) = id_x$ e $i(f : x \mapsto y) = id_y$ e as propriedades $i), ii), iii)$ e $iv)$ da definição de grupoide são trivialmente satisfeitas. □

Assim como fizemos para grupos e semigrupos, podemos definir a álgebra de um grupoide Γ conforme definição seguinte.

Definição 3.6 *Seja Γ um grupoide com Γ_0 finito. A **álgebra de grupoide** $K\Gamma$ é definida como segue. Considere $K\Gamma$ o K-módulo livre gerado por Γ e a seguinte multiplicação:*

$$\begin{array}{rccl} m: & \Gamma\times\Gamma & \longrightarrow & K\Gamma \\ & (g,h) & \longmapsto & m(g,h)=\begin{cases} gh, & se\ (g,h)\in\Gamma^{(2)} \\ 0, & c.c. \end{cases} \end{array}$$

A partir dessa multiplicação, restrita aos elementos da base de $K\Gamma$, podemos estender m da seguinte forma:

$$\begin{array}{rccl} m': & K\Gamma\times K\Gamma & \longrightarrow & K\Gamma \\ & \left(\sum\limits_{g\in\Gamma} a_g g, \sum\limits_{h\in\Gamma} b_h h\right) & \longmapsto & \sum\limits_{g,h\in\Gamma} a_g b_h m(g,h) \end{array}$$

Assim, a álgebra do grupoide Γ é o K-módulo livre $K\Gamma$ com o produto m' definido acima.

Para mostrar que $K\Gamma$ é uma álgebra, é fácil de ver que m' é K-bilinear. Além disso, m' é associativo e possui elemento neutro. A associativa é imediata da propriedade $i)$ da definição de grupoide e o elemento neutro é $1_{K\Gamma}=\sum\limits_{e\in\Gamma_0} e$. De fato,

$$\left(\sum_{e\in\Gamma_0} e\right) g = \sum_{\substack{e\in\Gamma_0 \\ e\neq i(g)}} eg + eg = g.$$

(O outro lado é análogo.)

3.2 Representação Parcial e Álgebra Parcial

Definição 3.7 *Uma **representação parcial** de G em uma K-álgebra A é uma função $\pi: G\to A$ tal que, para todos $s,t\in G$, temos*

i) $\pi(s)\pi(t)\pi(t^{-1})=\pi(st)\pi(t^{-1})$

ii) $\pi(s^{-1})\pi(s)\pi(t)=\pi(s^{-1})\pi(st)$

iii) $\pi(1_G)=1_A$

*Desta forma, uma função $\pi: G\to End(V)$, onde V é um espaço vetorial, satisfazendo $i), ii)$ e $iii)$ é dita uma **representação parcial** de G em V.*

Obs. 3.8 *Note que, claramente, toda K-representação de G também é uma representação parcial de G. Observe também que se H é subgrupo de G e $\pi : G \to End(V)$ é uma representação parcial de G, então a restrição de π a H é uma representação parcial de H.*

Se H é um subgrupo de G e $\pi : H \to End(V)$ é uma representação parcial de H, então a função $\tilde{\pi} : G \to End(V)$ dada por

$$\tilde{\pi}(g) = \begin{cases} \pi(g), & se\ g \in H \\ 0, & c.c. \end{cases}$$

define uma representação parcial de G.

De fato, provemos a propriedade $i)$ da definição de representação parcial (a propriedade $ii)$ é análoga e a propriedade $iii)$ é imediata):

Para verificarmos que $\tilde{\pi}(s)\tilde{\pi}(t)\tilde{\pi}(t^{-1}) = \tilde{\pi}(st)\tilde{\pi}(t^{-1})$, precisamos divir em três casos:

1. Se $s, t \in H$, então a igualdade é claramente satisfeita pois recai em π.

2. Se $t \notin H$, então $t^{-1} \notin H$, por ser H subgrupo de G, e $\tilde{\pi}(t) = \tilde{\pi}(t^{-1}) = 0$. Logo, ambos os lados da equação se anulam e vale a igualdade.

3. Se $s \notin H$, o lado esquerdo, claramente, se anula e o lado direito também. Com efeito, suponha por absurdo que $\tilde{\pi}(st)\tilde{\pi}(t^{-1}) \neq 0$. Então, $\tilde{\pi}(st)$ e $\tilde{\pi}(t^{-1})$ são não nulos. Em particular, $\tilde{\pi}(st) = \pi(st)$ e $\tilde{\pi}(t) = \pi(t)$, o que implica $st, t \in H$. Logo, $t^{-1} \in H$ e $stt^{-1} = s \in H$, uma contradição.

Proposição 3.9 *Seja $\pi : G \to A$ uma representação parcial. Se $\phi : A \to B$ é um morfismo de álgebras, então $\phi \circ \pi : G \to B$ é uma representação parcial.*

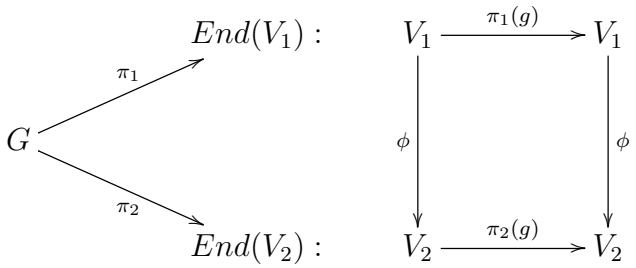
Prova: *Seja $\varphi = \phi \circ \pi$*

$$\begin{aligned} \varphi(s)\varphi(t)\varphi(t^{-1}) &= \phi \circ \pi(s)\phi \circ \pi(t)\phi \circ \pi(t^{-1}) = \phi(\pi(s)\pi(t)\pi(t^{-1})) \\ &= \phi(\pi(st)\pi(t^{-1})) = \phi \circ \pi(st)\phi \circ \pi(t^{-1}) \\ &= \varphi(st)\varphi(t^{-1}). \end{aligned}$$

$\varphi(1_G) = \phi \circ \pi(1_G) = \phi(1_A) = 1_B$

E o outro caso é análogo ao primeiro. □

Definição 3.10 *Sejam $\pi_1 : G \to End(V_1)$ e $\pi_2 : G \to End(V_2)$ duas representações parciais do grupo G. Dizemos que π_1 é **equivalente** à π_2 se existe um isomorfismo (de espaço vetorial) $\phi : V_1 \to V_2$ tal que $\phi \circ \pi_1(g) = \pi_2(g) \circ \phi$ para todo $g \in G$.*



Podemos, agora, apresentar uma definição de álgebra parcial de grupo. Esta, resume-se a definir $K_{par}(G)$ como a álgebra cujos módulos estão em correspondência uma-a-uma com as representações parciais de G.

Definição 3.11 *Sejam G um grupo e K um corpo. A K-**álgebra parcial de grupo** $K_{par}(G)$ é a K-álgebra livre com unidade 1 gerada pelo conjunto de símbolos $\{[g] : g \in G\}$ com relações:*

1) $[e] = 1$

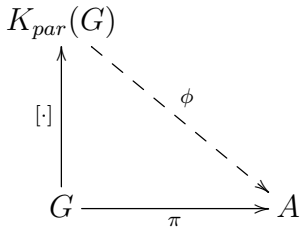
2) $[s^{-1}][s][t] = [s^{-1}][st]$

3) $[s][t][t^{-1}] = [st][t^{-1}]$

para todos $s, t \in G$.

Observe que, por construção, $K_{par}(G) = KS(G)$. Então, se A é uma K-algebra e $\pi : G \to A$ é uma representação parcial de G em A, pela propriedade universal de $S(G)$, existe um único homomorfismo de monóides $\varphi : S(G) \to A$ que estende π. Agora, pela proposição **??**, existe um único homomorfismo de K-álgebras $\Pi : K_{par}(G) = KS(G) \to A$, que estende φ e, portanto, estende π.

Note também que a aplicação que leva $g \in G$ em $[g] \in K_{par}(G)$ é uma representação parcial de G, com isto, qualquer representação parcial de G em A é composição dessa representação com um homomorfismo de álgebras de $K_{par}(G)$ em A.



Por outro lado, se $\phi : K_{par}(G) \to A$ é um homomorfismo de K-álgebras, então $\pi(t) = \phi([t])$ dá uma representação parcial de G em A.

No entanto, para o caso de grupo finito, torna-se mais rico construir a álgebra parcial de grupo de maneira diferente. No que segue, apresentaremos outra construção que acaba sendo mais eficiente do ponto de vista prático para construir a álgebra parcial de um grupo dado.

Para tal construção, considere o já visto grupoide $\Gamma(G) = \Gamma$, cujos elementos são pares (A, g), onde $g \in G$ e A é um subconjunto de G que contém os elementos 1_G e g^{-1} com a multiplicação de pares $(A, g)(B, h)$ em Γ definida para pares tais que $A = hB$ dada por:

$$(hB, g)(B, h) = (B, gh).$$

Relembre que o inverso do par (A, g) é (gA, g^{-1}) e o domínio e imagem em Γ são, respectivamente $d(A, g) = (A, 1_G)$ e $i(A, g) = (gA, 1_G)$.

Teorema 3.12 *Seja $K\Gamma(G)$ a álgebra do grupoide $\Gamma(G)$, com $|G| = n$ a cardinalidade de G. Então, a dimensão de $K\Gamma(G)$ é dada pela fórmula*

$$dim(K\Gamma(G)) = \sum_{k=0}^{n-1}(k+1)\binom{n-1}{k} = 2^{n-2}(n+1).$$

Prova: Note que a dimensão de $K\Gamma(G)$ é igual a cardinalidade de $\Gamma(G)$, que é o número de pares (A, g). Podemos calcular o número de pares (A, g) da seguinte forma:

Fixando o nível $k + 1$. Para o conjunto A temos que ter $k + 1$ elementos dentre n possíveis, mas o elemento 1_G deve pertencer a A. Logo, as possíbilidades para A são calculadas por $\binom{n-1}{k}$. Como, para cada par (A, g), podemos ter $k + 1$ possibilidades para g, no nível $k + 1$ há $(k + 1)\binom{n-1}{k}$ elementos. Assim, o número total será a soma

$$\sum_{k=0}^{n-1}(k+1)\binom{n-1}{k}.$$

Daí segue que

$$\begin{aligned}
\sum_{k=0}^{n-1}(k+1)\binom{n-1}{k} &= (n-1)\sum_{k=1}^{n-1}\frac{(n-2)!}{(k-1)!((n-2)-(k-1))!} + \sum_{k=0}^{n-1}\frac{(n-1)!}{k!((n-1)-k)!} \\
&= (n-1)\sum_{l=0}^{n-2}\frac{(n-2)!}{l!((n-2)-l)!} + 2^{n-1} \\
&= (n-1)2^{n-2} + 2.2^{n-2} \\
&= (n+1)2^{n-2}.
\end{aligned}$$

□

Corolário 3.13 *Sejam G e H grupos finitos tais que $K\Gamma(G) \cong K\Gamma(H)$. Então $|G| = |H|$.*

Prova: Sejam n e n' as ordens de G e H respectivamente. Então, como $K\Gamma(G) \cong K\Gamma(H)$, temos que $dim(K\Gamma(G)) = dim(K\Gamma(H))$. Logo, $2^{n-2}(n+1) = 2^{n'-2}(n'+1)$. Observe que a equação do teorema anterior é uma função estritamente crescente em n, pois

$$\frac{\delta}{\delta n}(2^{n-2}(n+1)) = 2^{n-2}ln2(n+1) + 2^{n-2} > 0.$$

Daí, segue que $n = n'$. □

Para finalizar a construção de $K_{par}(G)$ como sendo $K\Gamma(G)$, observe que os elementos na forma $(A, 1_G)$ são idempotentes em $K\Gamma(G)$, são mutuamente ortogonais e sua soma é a identidade de $K\Gamma(G)$, ou seja $\sum_{A \ni 1_G} (A, 1_G) = 1_{K\Gamma(G)}$. Com efeito, para $(A, 1_G), (A', 1_G), (B, g) \in K\Gamma(G)$,

$$(A, 1_G)^2 = (A, 1_G)(A, 1_G) = (1_G A, 1_G)(A, 1_G) = (A, 1_G 1_G) = (A, 1_G)$$

(Note também que um elemento (A, g) de $K\Gamma(G)$, para ser idempotente, precisam ser da forma $(A, 1_G)$ pois 1_G é o único idempotente em G),

$(A, 1_G)(A', 1_G) = 0$ se $A \neq A'$ e

$$\left(\sum_{A \ni 1_G} (A, 1_G)\right)(B, g) = \sum_{A \ni 1_G} (A, 1_G)(B, g) = (gB, 1_G)(B, g) = (B, g)$$

Por fim, defina a função $\lambda_p : G \to K\Gamma(G)$ por $\lambda_p(g) = \sum_{A \ni g^{-1}} (A, g)$. Então, λ_p é uma representação parcial de G. De fato, sejam $g, h \in G$,

$$\begin{aligned} \lambda_p(g^{-1})\lambda_p(g)\lambda_p(h) &= \sum_{\substack{A \ni g \\ B \ni g^{-1} \\ C \ni h^{-1}}} (A, g^{-1})(B, g)(C, h) \\ &= \sum_{\substack{C \ni h^{-1} \\ hC \ni g^{-1}}} (ghC, g^{-1})(hC, g)(C, h) \end{aligned}$$

$$= \sum_{\substack{C\ni h^{-1}\\ C\ni h^{-1}g^{-1}}} (C,h).$$

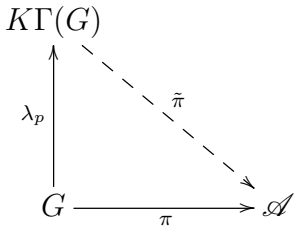
Por outro lado,

$$\begin{aligned}\lambda_p(g^{-1})\lambda_p(gh) &= \sum_{\substack{A\ni g\\ C\ni h^{-1}g^{-1}}} (A,g^{-1})(C,gh)\\ &= \sum_{\substack{ghC\ni g\\ C\ni h^{-1}g^{-1}}} (C,h)\\ &= \sum_{\substack{C\ni h^{-1}\\ C\ni h^{-1}g^{-1}}} (C,h).\end{aligned}$$

O outro item é similar e, claramente, $\lambda_p(1_G) = \sum_{A\ni 1_G} (A,1_G) = 1_{K\Gamma(G)}$.

Com isso, podemos apresentar os dois resultados mais significativos dessa seção, que, de fato, mostram que a construção feita é da álgebra parcial de grupo.

Teorema 3.14 *Existe uma correspondência biunívoca entre as representações parciais de G e as representações de $K\Gamma(G)$. Mais precisamente, se $\mathscr{A}$ é uma álgebra, então $\pi : G \to \mathscr{A}$ é uma representação parcial de G se, e somente se, existe um único homomorfismo de álgebra $\tilde{\pi} : K\Gamma(G) \to \mathscr{A}$ tal que $\pi = \tilde{\pi} \circ \lambda_p$, ou seja, o diagrama seguinte comuta:*



Prova: Para mostrar a primeira parte do teorema, suponha que $\pi : G \to \mathscr{A}$ é uma representação parcial de G. Para todo $r \in G$, denotemos por $\epsilon(r)$ o elemento de $\mathscr{A}$ dado por $\pi(r)\pi(r^{-1})$.

Observe que os elementos $\epsilon(r)$'s são idempotentes que comutam entre si:

Primeiro observe que

$$\pi(s)\epsilon(r) = \epsilon(sr)\pi(s). \tag{3.1}$$

pois

$$\pi(s)\epsilon(r) = \pi(s)\pi(r)\pi(r^{-1}) = \pi(sr)\pi(r^{-1})$$

$$\begin{aligned} &= \pi(sr)\pi(r^{-1}s^{-1})\pi(sr)\pi(r^{-1}) = \pi(sr)\pi(r^{-1}s^{-1})\pi(s) \\ &= \epsilon(sr)\pi(s). \end{aligned}$$

Então,

$$\begin{aligned} \epsilon(s)\epsilon(r) &= \pi(s)\pi(s^{-1})\epsilon(r) = \pi(s)\epsilon(s^{-1}r)\pi(s^{-1}) \\ &= \epsilon(r)\pi(s)\pi(s^{-1}) \\ &= \epsilon(r)\epsilon(s). \end{aligned}$$

para todo $s, r \in G$. Similarmente

$$\epsilon(r)\pi(s) = \pi(s)\epsilon(s^{-1}r). \tag{3.2}$$

Agora, considere a aplicacao $\tilde{\pi} : K\Gamma(G) \to \mathscr{A}$ que é definida em cada (A, g) de $\Gamma(G)$ por

$$\tilde{\pi}(A, g) = \pi(g)\left(\prod_{r\in A}\epsilon(r)\right)\left(\prod_{s\notin A}(1-\epsilon(s))\right)$$

Para (A, g) e (B, h) em $\Gamma(G)$, temos:

$$\begin{aligned} \tilde{\pi}(A, g)\tilde{\pi}(B, h) &= \pi(g)\prod_{r\in A}\epsilon(r)\prod_{s\notin A}(1-\epsilon(s))\pi(h)\prod_{t\in B}\epsilon(t)\prod_{v\notin B}(1-\epsilon(v)) \\ &= \pi(g)\pi(h)\prod_{r\in A}\epsilon(h^{-1}r)\prod_{s\notin A}(1-\epsilon(h^{-1}s))\prod_{t\in B}\epsilon(t)\prod_{v\notin B}(1-\epsilon(v)) \\ &= \pi(g)\pi(h)\prod_{r\in h^{-1}A}\epsilon(r)\prod_{s\in h^{-1}A}(1-\epsilon(s))\prod_{t\in B}\epsilon(t)\prod_{v\notin B}(1-\epsilon(v)). \end{aligned}$$

Agora, observe que, se $h^{-1}A \neq B$, ou seja, se $A \neq hB$, então existe um elemento r pertencente a $h^{-1}A$ mas que não pertence a B ou o contrário, r pertence a B mas não pertence a $h^{-1}A$. Em ambos os casos, o produto $\tilde{\pi}(A, g)\tilde{\pi}(B, h)$ contém o fator $\epsilon(r)(1-\epsilon(r)) = 0$ e, então, o produto é nulo.

Já se $h^{-1}A = B$, então, como $h^{-1} \in h^{-1}A$, o produto $\tilde{\pi}(A, g)\tilde{\pi}(B, h)$ é

$$\tilde{\pi}(A, g)\tilde{\pi}(B, h) = \pi(g)\pi(h)\prod_{r\in h^{-1}A}\epsilon(r)\prod_{s\notin h^{-1}A}(1-\epsilon(s))$$

$$\begin{aligned} &= \pi(g)\pi(h)\pi(h^{-1})\pi(h) \prod_{\substack{r\in h^{-1}A \\ r\neq h^{-1}}} \epsilon(r) \prod_{s\notin h^{-1}A} (1-\epsilon(s)) \\ &= \pi(gh) \prod_{r\in h^{-1}A} \epsilon(r) \prod_{s\notin h^{-1}A} (1-\epsilon(s)) \\ &= \tilde{\pi}(B, gh) = \tilde{\pi}((A,g)(B,h)). \end{aligned}$$

Com isto, provamos que $\tilde{\pi}$ preserva o produto de elementos da base de $K\Gamma(G)$ e, por isso, preserva produtos de dois elementos quaisquer de $K\Gamma(G)$.

Veja que, se $A \neq hB$, então o produto $(A,g)(B,h)$ não está definido em $\Gamma(G)$, mas é nulo em $K\Gamma(G)$. Com isso, a extensão linear a $K\Gamma(G)$ será um homomorfismo entre as álgebras $K\Gamma(G)$ e $\mathscr{A}$.

Agora, vejamos que $\tilde{\pi}$ leva unidade em unidade. Observe que $\pi(1_G) = 1_{\mathscr{A}}$ e, dado $S \subseteq G$, denote por P_S o elemento em $\mathscr{A}$ dado por

$$P_S = \prod_{s\in S} \epsilon(s) \prod_{s\notin S} (1_{\mathscr{A}} - \epsilon(s))$$

Como $\pi(t)\epsilon(s) = \epsilon(ts)\pi(t)$, temos $\pi(t)P_S = P_{tS}\pi(t)$. Note que, como $\epsilon(1_G) = 1_{\mathscr{A}}$, P_S é zero a menos que S contenha a identidade 1_G de G. Além disso, se $t \notin S$, então $P_S\pi(t) = 0$, pois $\epsilon(t)\pi(t) = \pi(t)$. Daí segue que

$$\sum_{\substack{S\subseteq G \\ S\ni 1_G}} P_S = \sum_{S\subseteq G} P_S = 1_{\mathscr{A}}.$$

De fato, observe que, uma vez que os ϵ's comutam, temos:

$$1_{\mathscr{A}} = \prod_{s\in G} 1_{\mathscr{A}} = \prod_{s\in G} (1_{\mathscr{A}} - \epsilon(s) + \epsilon(s)) =$$

$$= \sum_{S\subseteq G} \left[\left(\prod_{t\in S} \epsilon(t) \right) \left(\prod_{t\notin S} (1_{\mathscr{A}} - \epsilon(t) \right) \right] = \sum_{S\subseteq G} P_S.$$

Logo,

$$\begin{aligned}\tilde{\pi}(1_{K\Gamma(G)}) &= \tilde{\pi}\left(\sum_{A\ni 1_G}(A,1_G)\right) = \sum_{A\ni 1_G}\tilde{\pi}(A,1_G) = \sum_{A\ni 1_G}\prod_{r\in A}\epsilon(r)\prod_{s\notin A}(1_{K\Gamma(G)}-\epsilon(s)) \\ &= \sum_{A\ni 1_G}P_A = \sum_{A\subseteq G}P_A = 1_{\mathscr{A}}.\end{aligned} \tag{3.3}$$

Além disso, temos

$$\begin{aligned}\tilde{\pi}\circ\lambda_p(g) &= \tilde{\pi}\left(\sum_{A\ni g^{-1}}(A,g)\right) = \sum_{A\ni g^{-1}}\tilde{\pi}(A,g) = \\ &= \pi(g)\sum_{A\ni g^{-1}}\prod_{r\in A}\epsilon(r)\prod_{s\notin A}(1_{\mathscr{A}}-\epsilon(s)) = \\ &= \pi(g)\pi(g^{-1})\pi(g)\sum_{A\ni g^{-1}}\prod_{r\in A\setminus\{g^{-1}\}}\epsilon(r)\prod_{s\notin A}(1_{\mathscr{A}}-\epsilon(s)) = \\ &= \pi(g)\sum_{A\ni g^{-1}}(\epsilon(g^{-1})+1-\epsilon(g^{-1}))\prod_{r\in A\setminus\{g^{-1}\}}\epsilon(r)\prod_{s\notin A}(1_{\mathscr{A}}-\epsilon(s)) = \\ &= \pi(g)\sum_{B}\prod_{r\in B}\epsilon(r)\prod_{s\notin B}(1_{\mathscr{A}}-\epsilon(s)) = \\ &= \pi(g)\tilde{\pi}\left(\sum_{B}(B,e)\right) = \pi(g)\tilde{\pi}(1_{K\Gamma(G)}) = \pi(g).\end{aligned}$$

Por fim, falta mostrar a unicidade do homomorfismo $\tilde{\pi}$ satisfazendo $\tilde{\pi}\circ\lambda_p = \pi$. Para mostrar isto, é suficiente provar que o conjunto $\lambda_p(G)$ gera toda a álgebra $K\Gamma(G)$. Para tal, considere (B,h) um elemento arbitrário de $\Gamma(G)$, onde

$$B = \left\{b_1^{-1}, b_2^{-1}, ..., b_{k-1}^{-1}, h^{-1}\right\}$$

é um subconjunto de G contendo a identidade. O conjunto de tais pares (B,h) formam uma base do espaço vetorial $K\Gamma(G)$.

Com efeito, denote por $\mathbb{A}$ a subálgebra de $K\Gamma(G)$ gerada por $\lambda_p(G)$. Seja $\{g_1, g_2, ..., g_k\}$ uma família de elementos de G definida por:

$$g_1 = b_1, g_2g_1 = b_2, g_3g_2g_1 = b_3, ...,$$

$$g_{k-1}g_{k-2}...g_1 = b_{k-1}, g_kg_{k-1}...g_1 = h.$$

Considere o elemento em $\mathbb{A}$ dado pelo produto $\lambda_p(g_k)\lambda_p(g_{k-1})...\lambda_p(g_1)$:

$$\lambda_p(g_k)\lambda_p(g_{k-1})...\lambda_p(g_1) = \sum_{\substack{A_1 \ni g_1^{-1} \\ A_2 \ni g_2^{-1} \\ \vdots \\ A_k \ni g_k^{-1}}} (A_k, g_k)(A_{k-1}, g_{k-1})...(A_1, g_1).$$

Usando as regras de multiplicação em $\Gamma(G)$, é fácil de ver que esta soma é igual a:

$$\sum_{\substack{A_1 \ni g_1^{-1} \\ g_1 A_1 \ni g_2^{-1} \\ \vdots \\ g_{k-1}g_{k-2}...g_1 A_1 \ni g_k^{-1}}} (A_1, g_k g_{k-1}...g_1) \sum_{A_1 \supseteq B} (A_1, h).$$

Consequentemente, para cada $(B, h) \in \Gamma(G)$, $\mathbb{A}$ contém o elemento

$$\sum_{A \supseteq B} (A, h).$$

Agora, suponha que $G \setminus B = \{x_1, x_2, ..., x_N\}$. Temos

$$\sum_{A \supseteq B} (A, h) - \sum_{A \supseteq B \cup \{x_1\}} (A, h) = \sum_{\substack{A \supseteq B \\ A \not\ni x_1}} (A, h)$$

o que significa que, para cada $(B, h) \in \Gamma(G)$ e cada $x \notin B$, $\mathbb{A}$ contém todos os elementos na forma

$$\sum_{\substack{A \supseteq B \\ A \not\ni x}} (A, h).$$

Agora,

$$\sum_{\substack{A \supseteq B \\ A \not\ni x_1}} (A, h) - \sum_{\substack{A \supseteq B \cup \{x_1\} \\ A \not\ni x_1}} (A, h) = \sum_{\substack{A \supseteq B \\ A \not\ni x_1, x_2}} (A, h)$$

Então, para cada $x_1, x_2 \notin B$, $\mathbb{A}$ contém o elemento $\sum_{\substack{A \supseteq B \\ A \not\ni x_1, x_2}} (A, h)$.

Repetindo o argumento, usando indução, prova-se que $\mathbb{A}$ contém todos elementos na forma

$$\sum_{\substack{A \supseteq B \\ A \not\ni x_1, ..., x_N}} (A, h) = (B, h),$$

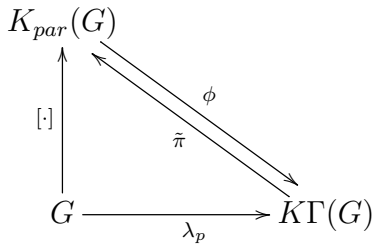
o que concui a prova que $\mathbb{A} = K\Gamma(G)$.

Já a segunda parte, segue da Proposição **??** uma vez que $\pi = \tilde{\pi} \circ \lambda_p$ é uma representação parcial de G. □

Corolário 3.15 *A álgebra de grupoide $K\Gamma(G)$ é isomorfa à álgebra parcial de grupo $K_{par}(G)$.*

Prova: Primeiro, observe que as funções $[\cdot] : G \to K_{par}(G)$, dada por $g \mapsto [g]$, e $\lambda_p : G \to K\Gamma(G)$ são representações parciais de G.

Pela propriedade universal das duas álgebras $K_{par}(G)$ e $K\Gamma(G)$, existem homomorfismos de K-álgebras $\tilde{\pi} : K\Gamma(G) \to K_{par}(G)$ e $\phi : K_{par}(G) \to K\Gamma(G)$ tais que $\tilde{\pi}(\lambda_p(g)) = [g]$ e $\phi([g]) = \lambda_p(g)$, para todo $g \in G$, ou seja, o seguinte diagrama comuta:



Daí segue, que $\tilde{\pi} \circ \phi = 1_{K_{par}(G)}$ e $\phi \circ \tilde{\pi} = 1_{K\Gamma(G)}$. Com efeito, para todo $g \in G$,

$$\tilde{\pi} \circ \phi([g]) = \tilde{\pi}(\lambda_p(g)) = [g]$$

e

$$\phi \circ \tilde{\pi}(\lambda_p(g)) = \phi([g]) = \lambda_p(g).$$

Assim, $K_{par(G)} \cong K\Gamma(G)$. □

3.3 Estrutura da Álgebra Parcial de Grupo

Nesta seção, provaremos que $K\Gamma(G)$ é soma direta de álgebras de matrizes sobre anéis KH, onde H é algum subgrupo de G, compreendendo assim um pouco melhor a estrutura de $K\Gamma(G)$.

Para isso, precisamos olhar para $K\Gamma(G)$ de um ponto vista geométrico e utilizar uma nova apresentação para a álgebra parcial, introduzindo uma nova notação: Dado um grupo H

(nossos grupos continuam sendo finitos, salve menção contrária e denotaremos 1_H por e para simplificar a notação) e um inteiro positivo m, então Γ_m^H denotará o grupoide cujos elementos são triplas (g, i, j), com $g \in H$ e $i, j = 1, 2, ..., m$. O domínio e a imagem em Γ_m^H são definidos, respectivamente, por $d(g, i, j) = (e, j, j)$ e $i(g, i, j) = (e, i, i)$.

O produto em Γ_m^H é o seguinte:

$$(g, i, j)(h, j, k) = (gh, i, k)$$

Assim, as unidades em Γ_m^H são os elementos na forma (e, i, i), simplesmente denotados por e_i, para $i = 1, 2, ..., m$.

Vejamos primeiro que, de fato, Γ_m^H satisfaz as quatro propriedades da definição de grupoide. Sejam $x_g = (g, i, j), x_h = (h, r, s), x_l = (l, t, u) \in \Gamma_m^H$,

i) $(x_g, x_h x_l) \in (\Gamma_m^H)^{(2)} \Leftrightarrow (x_g x_h, x_l) \in (\Gamma_m^H)^{(2)}$:

Observe que, para que $(x_g, x_h x_l)$ pertença a $(\Gamma_m^H)^{(2)}$, primeiramente $x_h x_l$ precisa estar definido, ou seja, precisamos ter $s = t$. Assim, $x_h x_l = (h, r, s)(l, s, u) = (hl, r, u)$. Agora, para que $(x_g, x_h x_l)$ esteja definido, precisamos ter $j = r$.

De $j = r$, segue que o produto $x_g x_h$ está definido, e $x_g x_h = (g, i, j)(h, j, s) = (gh, i, s)$. E $(x_g x_h)x_l$ está definido pois temos $s = t$.

Como a volta é análoga, vale a equivalência.

ii) $(x_g, x_h x_l) \in (\Gamma_m^H)^{(2)} \Leftrightarrow (x_g, x_h), (x_h, x_l) \in (\Gamma_m^H)^{(2)}$:

Segue imediatamente das contas do item anterior.

iii) Existem únicos $d(x_g), i(x_g) \in \Gamma_m^H$ tais que $(x_k, d(x_g)), (i(x_g), x_g) \in (\Gamma_m^H)^{(2)}$ e $x_g d(x_g) = x_g = i(x_g)x_g$:

Tome $d(x_g) = (h, k, l) \in \Gamma_m^H$. Para que tenhamos $x_g d(x_g) = (g, i, j)(h, k, l)$ definidos, precisamos ter $j = k$ e, assim, para termos $x_g d(x_g) = x_g$, precisamos ter $(gh, i, l) = (g, i, j)$, o que vale se, e somente se, $d(x_g) = (e, j, j)$

Para mostrar que $i(x_g) = (e, i, i)$ e $i(x_g)x_g = x_g$ basta seguir o mesmo raciocínio.

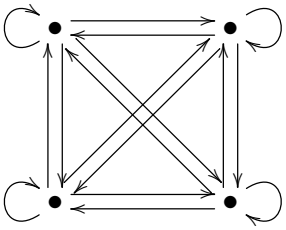
iv) Existe um único $x_g^{-1} \in \Gamma_m^H$ tal que $d(x_g) = x_g^{-1} x_g$ e $i(x_g) = x_g x_g^{-1}$:

Tome $x_g^{-1} = (h, k, l) \in \Gamma_m^H$. $d(x_g) = x_g^{-1} x_g \Leftrightarrow (e, j, j) = (h, k, l)(g, i, j)$. Então, precisamos ter $l = i$ para que o produto $(h, k, l)(g, i, j)$ esteja definido e , neste caso,

$(h,k,i)(g,i,j) = (hg,k,j)$. Agora, $(e,j,j) = (hg,k,j)$ se, e somente se, $h = g^{-1}$ e $k = j$. Portanto, $x_g^{-1} = (g^{-1},j,i)$.

Analogamente, mostra-se que $i(x_g) = x_g x_g^{-1}$, ou seja, $(e,i,i) = (g,i,j)(g^{-1},j,i)$.

Geometricamente, podemos representar um grupoide Γ como um grafo orientado E_Γ, cujos vértices são as unidades do grupoide e cada elemento $g \in \Gamma$ é uma aresta orientada de E_Γ do vértice $d(g)$ ao vértice $i(g)$. Assim, cada componente conexa de E_Γ é um subgrupoide de Γ.



No caso específico do grupoide Γ_m^H, o grafo $E_{\Gamma_m^H}$ tem m vértices e entre cada dois vértices há $|H|$ arestas, que podem ser rotulados pelos elementos de H.

Antes de podermos enunciar o principal resultado, precisamos de uma proposição anterior, que conecta os grupoides às álgebras de matrizes.

Proposição 3.16 *Sejam Γ um grupoide tal que E_Γ é conexo por caminhos e $m = |\Gamma_0|$ é finito. Sejam e_1 um vértice qualquer de E_Γ e H o grupo de isotropia de e_1, que é definido por*

$$H = \{g \in \Gamma : d(g) = i(g) = e_1\}$$

Então

i) $\Gamma \cong \Gamma_m^H$

ii) $K\Gamma \cong Mat_m(KH)$

Prova: Considere $e_1, e_2, ..., e_m$ as unidades de Γ. Para todos $i,j = 1,2,...,m$, defina $\mathscr{E}_{ij}$ por

$$\mathscr{E}_{ij} = \{g \in \Gamma : d(g) = e_j, i(g) = e_i\}.$$

Observe que, para todo $i,j = 1,2,...,m$, $\mathscr{E}_{ij}$ é não vazio, pois Γ é conexo por caminhos. Com efeito, se y_1=$e_i, y_2, ..., y_{k+1} = e_j$ é uma sequência em Γ_0 e $g_1, g_2, ..., g_k$ é uma sequência em Γ tal que $d(g_i) = y_i$ e $i(g_i) = y_{i+1}$ para todo i. Então, o elemento $g = g_k ... g_2 g_1$ pertence à $\mathscr{E}_{ij}$.

Claramente Γ é a união disjunta de todos os conjuntos $\mathscr{E}_{ij}$, para $i,j = 1,2,...,m$. Então, considere uma família fixada de elementos $g_i \in \mathscr{E}_{i1}$, com $i = 1,2,...,m$. Para $d(g) = e_i$

e $i(g) = e_j$ e para cada $g \in \Gamma$, $g_j^{-1} g g_i = h \in H$ e g pode ser escrito de maneira única como $g = g_j h g_i^{-1}$ com $h \in H$. Por outro lado, cada elemento na forma $g_j h g_i^{-1}$, com $h \in H$, pertence a $\mathscr{E}_{ij}$. Note que, em particular, $|\mathscr{E}_{ij}| = |H|$.

Com isso, temos que a função f definida por $g = g_i h g_j^{-1} \mapsto (h, i, j)$ é uma bijeção entre Γ e Γ_m^H.

O homomorfismo vem de $f(g_1 g_2) = f(g_j h_1 h_2 g_i^{-1}) = (h_1 h_2, i, j) = (h_1, i, k)(h_2, k, j) = f(g_1) f(g_2)$, onde $k = i(g_2) = d(g_1)$.

Já para provar a parte a $ii)$, considere $(E_{ij})_{i,j=1,2,\ldots,m}$ o conjunto de matrizes identidades de $Mat_m(K)$, ou seja, E_{ij} é a matriz com entrada nulas, exceto para a entrada na posição i, j, que é igual a 1_K. Como $(E_{ij})_{i,j=1,2,\ldots,m}$ é uma base de $Mat_m(K)$, a função $(h, i, j) \mapsto h \otimes E_{ij}$ estende por linearidade a um isomorfismo de K-álgebra entre $K\Gamma_m^H$ e $KH \otimes Mat_m(K)$. Por fim, basta observar que $KH \otimes Mat_m(K) \cong^1 Mat_m(KH)$, o que conclui a prova. □

Note que, na proposição anterior, H poderia ser infinito e mesmo assim valeria o resultado uma vez que a demonstração independe deste fato. Outra coisa importante a ser observada é a seguinte proposição.

Proposição 3.17 *Se o grupoide Γ for uma união finita disjunta de subgrupoides Γ_i, com $i \in I$ para algum conjunto finito I, então a álgebra de grupoide $K\Gamma$ é a soma direta das álgebras de cada subgrupoide, ou seja*

$$\Gamma = \bigcup_{i=1}^{N} \Gamma_i \Rightarrow K\Gamma = \bigoplus_{i=1}^{N} K\Gamma_i.$$

Em particular, a álgebra de grupoide $K\Gamma$ é a soma direta de álgebras na forma $Mat_m(KH)$, com $m > 0$ e H grupo.

Prova: Se x, y são elementos de Γ que estão em componentes distintas de Γ, então $xy = 0$ em $K\Gamma$. Com efeito, se x e y estão em componentes distintas de Γ, então $d(x) \neq i(y)$, pois, caso

1- Dada uma K-álgebra A e um corpo K (não necessariamente o mesmo corpo sobre o qual a álgebra está definida), a função

$$\begin{array}{rccc} \zeta: & A \otimes Mat_m(K) & \longrightarrow & Mat_m(A) \\ & 1_A \otimes E_{ij}^K & \longmapsto & E_{ij}^A \end{array}$$

é um isomorfismo entre as álgebras $A \otimes Mat_m(K)$ e $Mat_m(A)$, pois é uma bijeção entre elementos da base da cada álgebra. Observe que tanto $A \otimes Mat_m(K)$ quanto $Mat_m(A)$ estão sendo considerados como A-módulos, e que as bases são as bases dos A-módulos (não dos K-espaços).

contrário, a sequência $d(y), y, i(y) = d(x)$ é um caminho de $d(y)$ a $d(x)$ em Γ, o que é um absurdo, já que $d(y)$ e $d(x)$ pertencem a componentes diferentes de E_Γ. Portanto, segue que $xy = xd(x)i(y)y = x.0.y = 0$.

Supondo que temos um número finito N de componentes do grafo E_Γ, denotadas por $\Gamma_1, \Gamma_2, ..., \Gamma_N$, podemos numerar os elementos de Γ que correspondem aos vértices e arestas de cada componente Γ_j por $g_{1,j}, ..., g_{L_j,j}$.

Levando essa numeração em conta, cada elemento de $K\Gamma$ se escreve de modo único como

$$\sum_{j=1}^{N} \left(\sum_{i=1}^{L_j} k_{i,j} g_{i,j} \right).$$

Agora, o isomorfismo de $K\Gamma$ com $K\Gamma_1 \oplus K\Gamma_2 \oplus ... \oplus K\Gamma_N$ é

$$\Phi \left(\sum_{j=1}^{N} \left(\sum_{i=1}^{L_j} k_{i,j} g_{i,j} \right) \right) = \left(\sum_{i=1}^{L_1} k_{i,1} g_{i,1}, \sum_{i=1}^{L_2} k_{i,2} g_{i,2}, ..., \sum_{i=1}^{L_N} k_{i,N} g_{i,N} \right).$$

O fato de ser isomorfismo K-linear é evidente. Quanto ao produto, basta verificar em pares de elementos de Γ.

Se $x \in \Gamma_j$ e $y \in \Gamma_k$ com $j \neq k$, então $xy = 0$, e também $\Phi(x)\Phi(y) = 0$, pois o produto na soma direta é feito coordenada a coordenada.

Se $x, y \in \Gamma_j$, então

$$\Phi(x)\Phi(y) = (0, ..., 0, x, 0, ..., 0)(0, ...0, y, 0, ..., 0) = (0, ..., 0, xy, 0, ..., 0)$$

onde x, y e xy aparecem na j-ésima posição. Neste caso, se $d(x) = i(y)$ então o produto xy está definido em Γ, e está na mesma componente Γ_j; neste caso, a igualdade acima fornece a igualdade $\Phi(x)\Phi(y) = \Phi(xy)$. E se $d(x) \neq i(y)$, então $xy = 0$ em $K\Gamma$ e, pela equação acima, $\Phi(x)\Phi(y) = 0 = \Phi(xy)$.

Φ também preserva unidade:

$$\begin{aligned} \Phi(1_{K\Gamma}) = \Phi \left(\sum_{e \in \Gamma_0} e \right) &= \left(\sum_{e \in \Gamma_0 \cap \Gamma_1} e, \sum_{e \in \Gamma_0 \cap \Gamma_2} e, ..., \sum_{e \in \Gamma_0 \cap \Gamma_N} e \right) \\ &= 1_{K\Gamma_1} \oplus 1_{K\Gamma_2} \oplus ... \oplus 1_{K\Gamma_N} \\ &= 1_{K\Gamma_1 \oplus K\Gamma_2 \oplus ... \oplus K\Gamma_N}. \end{aligned}$$

Observe que a última igualdade segue da proposição anterior. □

Definição 3.18 *Sejam G um grupo e $\Gamma(G)$ o grupoide construído como anteriormente. Para $1 \leq k \leq |G|$, chamamos de k-ésimo **nível** de $\Gamma(G)$ o subgrupoide de $\Gamma(G)$ constituído por pares (A, g) com $|A| = k$. Analogamente, o k-ésimo **nível** do grafo $E_{\Gamma(G)}$ é o subgrafo de $E_{\Gamma(G)}$ constituído pelos vértices (A, e) e arestas (A, g) tais que $|A| = k$.*

Com esta definição, e o resultado anterior, podemos dar uma descrição mais precisa da álgebra $K\Gamma(G)$, além de um algoritmo para seu cálculo, que apresentaremos posteriormente.

Teorema 3.19 *A álgebra de grupoide $K\Gamma(G)$ é da forma*

$$K\Gamma(G) = \bigoplus_{\substack{H \leq G \\ 1 \leq m \leq (G:H)}} c_m(H) Mat_m(KH)$$

onde $c_m(H)Mat_m(KH)$ significa a soma direta de $c_m(H)$ cópias de $Mat_m(KH)$.

Prova: Seja $A \subseteq G$ com $e \in A$. Identique $A = (A, e) \in E_{\Gamma(G)}$ e observe que podemos tomar $A = e_1$ como na proposição anterior.

Seja $S(A) = \{g \in G : gA = A\}$ o estabilizador de A em G. Identifique $S(A)$ em $E_{\Gamma(A)}$ como o conjunto de arestas da forma (A, g), com $gA = A$, começando e terminando em A. Assim, $S(A) \cong H$, onde H é o grupo de isotropia de A. De fato, claramente

$$\begin{array}{rccc} \varphi: & S(A) & \longrightarrow & H \\ & g & \longmapsto & (A, g) \end{array}$$

é bijetora e $\varphi(g)\varphi(h) = (A, g)(A, h) = (A, gh) = \varphi(gh)$. Assim, podemos identificar $H = S(A)$.

Observe que, como $e \in A$, para $g \in H$, $ge = g \in A$, logo $H \subseteq A$.

Como H age pela esquerda em A, temos

$$A = \bigcup_{i=1}^{m} Ht_i$$

como união de órbitas disjuntas. Como $|Ht_i| = |H|$ para cada i, tem-se que $m = {}^{|A|}/_{|H|}$. Sem perda de generalidade, considere $t_1 = e$.

Vejamos que a componente conexa de A em $E_{\Gamma(G)}$ contém precisamente m vértices, dados pelos subconjuntos de G na forma $A_i = t_i^{-1}A$, com $i - 1, 2, ..., m$.

Note que $A_i \neq A_j$ se $i \neq j$. De fato, suponha $A_i = A_j$ com $i \neq j$,

$$A_i = A_j \Rightarrow t_i^{-1}A = t_j^{-1}A \Rightarrow t_j t_i^{-1}A = A \Rightarrow t_j t_i^{-1} \in H \Rightarrow$$

$$\Rightarrow t_j t_i^{-1} H = H \Rightarrow t_i^{-1} H = t_j^{-1} H \Rightarrow t_i^{-1} = t_j^{-1} \Rightarrow t_i = t_j,$$

uma contradição.

Observe que os vértices que aparecem na componente são da forma $r^{-1}A$, com $r \in A$. Mas, se $r \in A$, então existe t_i tal que $r \in Ht_i$.

Note também que, se $r \in Ht_i$, então $r = ht_i$ para algum $h \in H$, o que implica que $r^{-1}A = t_i^{-1}h^{-1}A = t_i^{-1}A$. Assim, a componente conexa de A só possui elementos na forma A_i.

Por fim, pela proposição anterior, $Mat_m(KH) \cong K\Gamma_m^H$, o que implica

$$K\Gamma(G) = \bigoplus_{\substack{H \leq G \\ 1 \leq m \leq (G:H)}} c_m(H) Mat_m(KH)$$

pois o grupoide $\Gamma(G)$ nada mais é do que a união disjunta de suas componentes conexas e cada componente conexa é da forma $\bigcup_{i=1}^{m} A_i$ com $A_i \neq A_j$ se $i \neq j$. Como podem haver repetições em componentes conexas distintas, temos os índices $c_m(H)$. □

Exemplo 3.20 *Para $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$, calculemos $K\Gamma(S_3)$.*

Vamos calcular Γ_m^H para cada nível k do grupoide $\Gamma(S_3)$, onde $k = |A|$.

Para $k = 1$: Como obrigatoriamente $e \in A$, o único elemento no nível $k = 1$ é $(\{e\}, e)$. Logo, de $m = \frac{|A|}{|H|}$, como $H \leq A$, $|H|$ divide $|A| = k = 1$, então $m = 1$.

Assim, há apenas uma componente conexa no nível 1 com apenas um vértice e uma única aresta começando e terminando nele.

Assim, $K\Gamma_1^{\{e\}} \cong Mat_1(Ke) \cong K$

Para $k = 2$, observe primeiro que o total de vértices no nível k é calculado como sendo a distribuição do número de elementos em S_3 diferentes da identidade em subconjuntos de $k - 1$ elementos, pois a identidade deve obrigatoriamente pertencer ao conjunto. Mais genericamente, para calcular o total de vértices no nível k vale a fórmula

$$\binom{|G| - 1}{k - 1}.$$

Nesse caso,

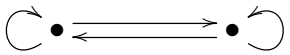
$$\binom{6-1}{2-1} = \binom{5}{1} = 5.$$

Além do mais, para $k = 2$, observe que S_3 possui três subgrupos de ordem dois:

$$\{e, (12)\}, \{e, (13)\}, \{e, (23)\}$$

que são estabilizadores de si mesmos. Os demais vértices no nível 2 possuem estabilizador trivial, pois não são subgrupos.

Da equação $m = \frac{|A|}{|H|}$, temos duas possibilidades para m, $m = 1$ ou $m = 2$. Então, para $m = 2$ temos $|H| = 1$ e temos a componente conexa $\Gamma_2^{\{e\}}$:



Daí, $K\Gamma_2^{\{e\}} \cong Mat_2(Ke) \cong Mat_2(K)$

Neste caso, se tomarmos $v_1 = \{e, (123)\}$, $v_2 = \{e, (132)\}$ e se $\mathscr{E}_{x,y}$ denota o conjunto de arestas de x para y, então

$$\mathscr{E}_{v_1,v_2} = (\{e, (123)\}, (123)),$$

$$\mathscr{E}_{v_2,v_1} = (\{e, (132)\}, (132)).$$

Agora, para $m = 1$, temos $|H| = 2$. Temos as três possibilidades para H:

$$\{e, (12)\}, \{e, (13)\}, \{e, (23)\}.$$

Portanto, temos três componentes conexas, cada uma com um vértice e duas flechas.

Em todos os casos podemos identificar $H \cong \mathbb{Z}_2$ e temos $3K\Gamma_1^{\mathbb{Z}_2} \cong 3Mat_1(K\mathbb{Z}_2) \cong 3(K\mathbb{Z}_2)$.

Já para $k = 3$, temos um total de $\binom{5}{2} = 10$ vértices e da equação $m = \frac{|A|}{|H|}$, segue que podemos ter $|H| = 3$ ou $|H| = 1$. Como H é subgrupo de S_3 e S_3 possui somente um subgrupo de ordem três,

$$H = \{e, (123), (132)\},$$

temos que os demais nove vértices tem estabilizador trivial e distribuem-se em três componentes, cada uma com três vértices.

Portanto, temos as seguintes componentes conexas:

No caso de $H = \{e, (123), (132)\}$*, a componente conexa possui apenas um vértice, o vértice* $v_1 = \{e, (123), (132)\}$ *e três arestas:*

Já no caso $H = \{e\}$*, temos três componentes conexas, cada uma com três vértices. A primeira possui os vértices*

$$v_1 = \{e, (12), (13)\}$$

$$v_2 = \{e, (12), (132)\}$$

$$v_3 = \{e, (13), (123)\}$$

Também temos:

$$\mathscr{E}_{v_1,v_2} = (\{e, (12), (13)\}, (12))$$

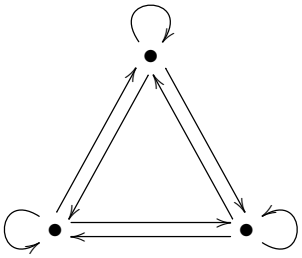
$$\mathscr{E}_{v_1,v_3} = (\{e, (12), (13)\}, (13))$$

$$\mathscr{E}_{v_2,v_1} = (\{e, (12), (132)\}, (12))$$

$$\mathscr{E}_{v_2,v_3} = (\{e, (12), (132)\}, (132))$$

$$\mathscr{E}_{v_3,v_1} = (\{e, (13), (123)\}, (13))$$

$$\mathscr{E}_{v_3,v_2} = (\{e, (13), (123)\}, (123)).$$



Já as outras duas componentes conexas possuem vértices, respectivamente

$$v_1 = \{e, (12), (23)\}$$

$$v_2 = \{e, (12), (123)\}$$

$$v_3 = \{e, (23), (132)\}$$

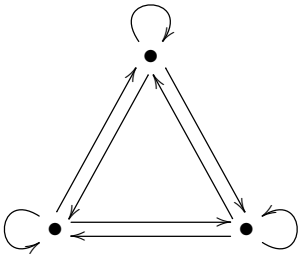
e

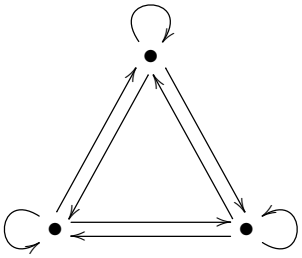
$$v_1 = \{e, (13), (23)\}$$

$$v_2 = \{e, (13), (132)\}$$

$$v_3 = \{e, (23), (123)\}.$$

As arestas deixaremos a cargo do leitor:





Portanto, temos $K\Gamma_1^{\mathbb{Z}_3} \cong Mat_1(K\mathbb{Z}_3) \cong K\mathbb{Z}_3$ *para* $|H| = 3$ *e* $3K\Gamma_3^{\{e\}} \cong 3Mat_3(K)$ *para* $|H| = 1$.

Para $k = 4$*, temos um total de* $\binom{5}{3} = 10$ *vértices. Como* $|H|$ *divide* $|A| = k = 4$*, podemos ter* $|H| = 1$ *ou* $|H| = 2$ *(não podemos ter* $|H| = 4$ *pois* S_3 *não possui subgrupo de ordem* 4 *e* H *deve ser subgrupo de* S_3*). Portanto, para* $|H| = 1$ *temos* $m = 4$ *e para* $|H| = 2$ *temos* $m = 2$*. Assim, surgem as seguintes componentes conexas:*

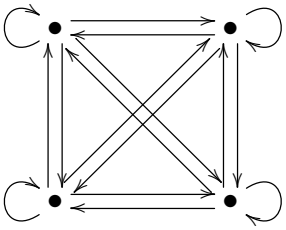
Para o caso $H = \{e\}$*, temos uma componente conexa com os vértices*

$$v_1 = \{e, (12), (13), (23)\}$$

$$v_2 = \{e, (12), (123), (132)\}$$

$$v_3 = \{e, (13), (123), (132)\}$$

$$v_4 = \{e, (23), (123), (132)\}$$



Para

$$H = \{e, (12)\}, H = \{e, (13)\}, H = \{e, (23)\}$$

temos, em cada caso, uma componente conexa com os respectivos vértices

$$v_1 = \{e, (12), (13), (132)\}$$

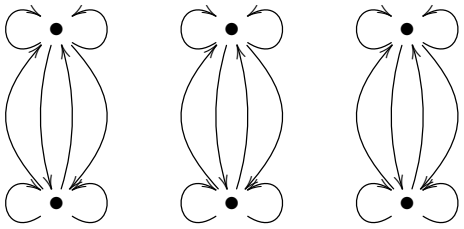
$$v_2 = \{e, (13), (23), (123)\}.$$

$$v_1 = \{e, (13), (12), (123)\}$$

$$v_2 = \{e, (13), (23), (132)\}.$$

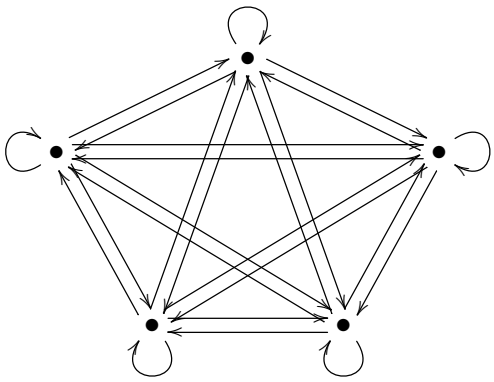
$$v_1 = \{e, (23), (12), (132)\}$$

$$v_2 = \{e, (23), (13), (123)\}.$$



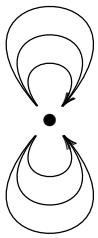
e temos, $K\Gamma_4^{\{e\}} \cong Mat_4(K)$ *e* $3K\Gamma_2^{\mathbb{Z}_2} \cong 3Mat_2(K\mathbb{Z}_2)$.

Para $k = 5$*, temos um total de* $\binom{5}{4} = 5$ *vértices. Como* S_3 *não possui subgrupo de ordem* 5*, temos* $m = 1$*. Logo no nível* 5 *há apenas a componente conexa:*



E, assim, temos $K\Gamma_5^{\{e\}} \cong Mat_5(K)$

Para $k = 6$*, como* $A = S_3$*, o único estabilizador* H *é o próprio* S_3*. Portanto* $m = 1$ *e temos a única componente conexa:*



Portanto, temos $K\Gamma_1^{S_3} \cong Mat_1(KS_3) \cong KS_3$ *e*

Teorema 3.21 *No teorema anterior, vale a seguinte fórmula recursiva:*

$$c_m(H) = \frac{1}{m}\left(\binom{(G:H)-1}{m-1} - \sum_{\substack{H<B\leq G \\ (B:H)|m}} c_{\frac{m}{(B:H)}}(B)\right)$$

Prova: Primeiro, fixe H como nas hipóteses do teorema anterior, ou seja, H é o grupo de isotropia de algum vértice A, isto é, $H = stab(A)$ e seja $m = \frac{|A|}{|H|}$.

Para determinar o número de repetições da álgebra $Mat_m(KH)$ na equação do teorema anterior, precisamos contar o número de vértices no nível $k = m.|H|$ de $E_{\Gamma(G)}$ cujo estabilizador é H. Defina $b_m(H)$ como sendo o número de vértices na forma (A, e) onde A é estabilizado por H. Como a componente conexa de A contém m vértices, pela demonstração do

teorema anterior, o número de componentes conexas em k, que possuem um vértice estabilizado por H, é $\frac{b_m(H)}{m}$.

Como cada A é subconjunto de G, contendo e, que é união de classes à direita de H, então o nível k terá $\binom{(G:H)-1}{m-1}$ vértices.

Suponha que A é um destes vértices e que $stab(A) = B \supseteq H$. Então, existem $r_1, r_2, ..., r_n \in A$ tais que

$$A = \bigcup_{i=1}^{n} Br_i$$

e como $n|B| = k = m|H|$. Então, temos que

$$n(B : H) = n\frac{|B|}{|H|} = m$$

e, em particular, segue que $(B : H)$ divide m.

Logo, temos que o número de vértices no nível k, que são estabilizados por H, mas tem um estabilizador que contém H, é

$$\sum_{\substack{H<B\leq G \\ (B:H)|m}} b_{\frac{m}{(B:H)}}(B).$$

Daí, segue que

$$b_m(H) = \binom{(G : H) - 1}{m - 1} - \sum_{\substack{H<B\leq G \\ (B:H)|m}} b_{\frac{m}{(B:H)}}(B)$$

No entanto, observe que H não é determinado exclusivamente pela componente conexa escolhida H também depende da escolha de um vértice na componente.

Poderiamos ter definido outro índice para contar o número de componentes da forma $\Gamma_m^{H'}$, com H' conjugado ou igual a H. Este número é

$$\frac{\delta(H)b_m(H)}{m},$$

conforme mostraremos a seguir (onde $\delta(H)$ é o número de subgrupos de G conjugados a H). A partir deste, e da escolha igualitária de componentes para cada subgrupo conjugado a H, segue que

$$c_m(H) = \frac{b_m(H)}{m},$$

da onde segue o resultado.

Com efeito, dados os vértices A e gA, que estão na mesma componente, se $Stab(A) = H$, então $Stab(gA) = gHg^{-1}$. Basta notar que $rgA = gA$ implica que $g^{-1}rgA = A$ e, portanto $g^{-1}rg \in H$. Ou seja, $r \in gHg^{-1}$. Reciprocamente vale a volta.

Quando calculamos o fator associado a uma componente com m vértices, escolhemos um vértice A da componente, calculamos seu estabalizador H e, daí, sabemos que o subgrupoide associado a essa componente é isomorfo a Γ_m^H. No entanto, se trocarmos de "vértice inicial", digamos de A para gA, trocamos H por gHg^{-1} (que pode ser igual a H ou não), como vimos acima. Logo, a componente não determina o subgrupo H exatamente; ela determina H a menos de conjugação.

Afirmamos que $b_m(H) = b_m(gHg^{-1})$ para qualquer $g \in G$. De fato, G age no grupoide $\Gamma(G)$ por $g \cdot (A, r) = (gAg^{-1}, grg^{-1})$, e se o estabilizador de um vértice A, com relação à ação do grupoide, é H, então o estabilizador de $g \cdot A = gAg^{-1}$ é gHg^{-1}. Com efeito, se $h \in H = Stab(A)$, então

$$ghg^{-1}(g \cdot A) = ghg^{-1}gAg^{-1} = ghAg^{-1} = gAg^{-1} = g \cdot A,$$

e temos que $gHg^{-1} \subseteq Stab(g \cdot A)$.

E se $r \in Stab(g \cdot A)$, então

$$rgAg^{-1} = gAg^{-1} \Rightarrow rgA = gA \Rightarrow g^{-1}rgA = A,$$

do que segue que $g^{-1}rg \in H$, que é o mesmo que $r \in gHg^{-1}$.

Assim, o número de vértices que tem estabilizador H é o mesmo número de vértices que tem estabilizador gHg^{-1} para qualquer $g \in G$.

Afirmamos também que a ação de G no grupoide preserva componentes. Basta observar que a ação preserva o produto do grupoide. Por isso, a ação preserva arestas do grafo de $\Gamma(G)$ e, portanto, preserva componentes.

Seja $\delta = \delta(H)$ o número de subgrupos de G que são conjugados a H. Sejam

$$r_1Hr_1^{-1}, r_2Hr_2^{-1}, ..., r_\delta Hr_\delta^{-1}$$

estes subgrupos (tome $r_1 = 1_G$). O número de vértices que tem estabilizador igual ou conjugado a H é

$$\sum_{j=1}^{\delta} b_m(r_jHr_j^{-1}) = \sum_{j=1}^{\delta} b_m(H) = \delta(H)b_m(H).$$

Como estes vértices se distribuem em componentes do grafo, cada uma com m elementos, segue que o número de componentes (no nível $k = m|H|$) cujos vértices tem estabilizadores

conjugados a H é

$$\frac{\delta(H)b_m(H)}{m}.$$

O número de componentes no nível k, que possuem um vértice com estabilizador H', é o mesmo para cada subgrupo H' conjugado a H. De fato, da ação de G por conjugação, temos que se

$$C_1, C_2, ..., C_N$$

são as componentes distintas, que têm pelo menos um vértice com estabilizador H, então

$$gC_1g^{-1}, gC_2g^{-1}, ..., gC_Ng^{-1}$$

são componentes distintas que têm pelo menos um vértice com estabilizador $H' = gHg^{-1}$.

Trocando H por H', vemos que o número de tais componentes é igual para H e H'.

Deste modo, como temos $\frac{\delta(H)b_m(H)}{m}$ componentes com estabilizadores de vértices conjugados a H e como cada subgrupo conjugado a H se distribui pelo mesmo número de componentes, podemos associar a cada um destes subgrupos o número de

$$\frac{1}{\delta(H)}\frac{\delta(H)b_m(H)}{m} = \frac{b_m(H)}{m}$$

componentes.

Finalmente, a fórmula recursiva para $c_m(H)$ segue diretamente da fórmula recursiva para $b_m(H)$. □

Mostraremos a seguir que se a característica de K não divide $|G|$, então a álgebra $K\Gamma$ é semissimples. Mas primeiro precisaremos de um resultado sobre álgebras de matrizes.

Proposição 3.22 *Sejam R e S dois anéis e m e n dois inteiros. Então*

i) $Mat_m(R \oplus S) \cong Mat_m(R) \oplus Mat_m(S)$

ii) $Mat_m(Mat_n(R)) \cong Mat_{mn}(R)$

Prova: Para o item $i)$ considere a função

$$\begin{array}{rccc} \varphi: & Mat_m(R \oplus S) & \longrightarrow & Mat_m(R) \oplus Mat_m(S) \\ & \sum_{i,j}(r_{ij}, s_{ij})E_{ij} & \longmapsto & \left(\sum_{i,j} r_{ij}E_{ij}, \sum_{i,j} s_{ij}E_{ij}\right) \end{array}$$

Claramente φ é bijetora e como está definida para elementos da base de ambos os conjuntos, sua extensão por linearidade, denotada da mesma forma, é uma bijeção entre eles.

Resta verificar que φ é um homomorfismo de anéis:

Para a multiplicação

$$\begin{aligned}\varphi\left(\sum_{i,j}(r_{ij},s_{ij})E_{ij}.\sum_{k,l}(t_{kl},u_{kl})E_{kl}\right) &=\varphi\left(\sum_{i,l}\left(\sum_{j=k}(r_{ij},s_{ij})(t_{kl},u_{kl})\right)E_{il}\right)\\ &=\varphi\left(\sum_{i,l}\left(\sum_{j=k}(r_{ij}t_{kl},s_{ij}u_{kl})\right)E_{il}\right)\\ &=\varphi\left(\sum_{i,l}\left(\sum_{j}r_{ij}t_{jl},\sum_{j}s_{ij}u_{jl}\right)E_{il}\right)\\ &=\left(\left(\sum_{i,l}\sum_{j}r_{ij}t_{jl}E_{il},\sum_{i,l}\sum_{j}s_{ij}u_{jl}E_{il}\right)\right).\end{aligned}$$

Por outro lado,

$$\begin{aligned}\varphi\left(\sum_{i,j}(r_{ij},s_{ij})E_{ij}\right)\varphi\left(\sum_{k,l}(t_{kl},u_{kl})E_{kl}\right) &=\left(\sum_{i,j}r_{ij}E_{ij},\sum_{i,j}s_{ij}E_{ij}\right)\left(\sum_{k,l}t_{kl}E_{kl},\sum_{k,l}u_{kl}E_{kl}\right)\\ &=\left(\sum_{i,j}r_{ij}E_{ij}\sum_{k,l}t_{kl}E_{kl},\sum_{i,j}s_{ij}E_{ij}\sum_{k,l}u_{kl}E_{kl}\right)\\ &=\left(\left(\sum_{i,l}\sum_{j}r_{ij}t_{jl}E_{il},\sum_{i,l}\sum_{j}s_{ij}u_{jl}E_{il}\right)\right).\end{aligned}$$

Já para a soma

$$\begin{aligned}\varphi\left(\sum_{i,j}(r_{ij},s_{ij})E_{ij}+\sum_{k,l}(t_{ij},u_{ij})E_{ij}\right) &=\varphi\left(\sum_{i,j}((r_{ij},s_{ij})+(t_{ij},u_{ij}))E_{ij}\right)\\ &=\varphi\left(\sum_{i,j}(r_{ij}+t_{ij},s_{ij}+u_{ij})E_{ij}\right)\\ =\left(\sum_{i,j}(r_{ij}+t_{ij})E_{ij},\sum_{i,j}(s_{ij}+u_{ij})E_{ij}\right).&\end{aligned}$$

Por outro lado,

$$\begin{aligned}&\varphi\left(\sum_{i,j}(r_{ij},s_{ij})E_{ij}\right)+\varphi\left(\sum_{k,l}(t_{ij},u_{ij})E_{ij}\right)=\\ &=\left(\sum_{i,j}r_{ij}E_{ij},\sum_{i,j}s_{ij}E_{ij}\right)+\left(\sum_{i,j}t_{ij}E_{ij},\sum_{i,j}u_{ij}E_{ij}\right)=\\ &=\left(\sum_{i,j}(r_{ij}+t_{ij})E_{ij},\sum_{i,j}(s_{ij}+u_{ij})E_{ij}\right).\end{aligned}$$

Além disso

$$\begin{aligned}\varphi(1_{Mat_m(R\oplus S)}) =& \varphi\left(\sum_{i,j}(1_R,1_S)E_{ij}\right)\\ =& \left(\sum_{i,j}1_RE_{ij},\sum_{i,j}1_SE_{ij}\right)=1_{Mat_m(R)\oplus Mat_m(S)}.\end{aligned}$$

o que prova o item $i)$.

Para provar o item $ii)$ faremos um passo intermediário, mostraremos que

$$Mat_m(Mat_n(R))\cong Mat_n(R)\otimes Mat_m(R)$$

para depois mostrar que

$$Mat_n(R)\otimes Mat_m(R)\cong Mat_{mn}(R).$$

Primeiro, considere a seguinte função

$$\begin{array}{rccc}\phi: & Mat_m(Mat_n(R)) & \longrightarrow & Mat_n(R)\otimes Mat_m(R)\\ & \sum\limits_{i,j}^{m}A_{ij}E_{ij} & \longmapsto & \sum\limits_{i,j}^{m}A_{ij}\otimes E_{ij}\end{array}$$

onde $A_{ij}\in Mat_n(R)$ para todo $i,j=1,2,...,m$ e E_{ij} são os elementos da base canônica de $Mat_m(Mat_n(R))$.

ϕ é aditiva pois

$$\begin{aligned}\phi\left(\sum_{i,j}^{m}A_{ij}E_{ij}+\sum_{i,j}^{m}B_{ij}E_{ij}\right) =& \phi\left(\sum_{i,j}^{m}(A_{ij}+B_{ij})E_{ij}\right)\\ =& \sum_{i,j}^{m}E_{ij}\otimes(A_{ij}+B_{ij})\\ =& \sum_{i,j}^{m}E_{ij}\otimes A_{ij}+\sum_{i,j}^{m}E_{ij}\otimes B_{ij}\\ =& \phi\left(\sum_{i,j}^{m}A_{ij}E_{ij}\right)+\phi\left(\sum_{i,j}^{m}B_{ij}E_{ij}\right)\end{aligned}$$

ϕ é multiplicativa, pois

$$\begin{aligned}\phi\left(\left(\sum_{i,j}^{m}A_{ij}E_{ij}\right)\left(\sum_{k,l}^{m}B_{kl}E_{kl}\right)\right) =& \phi\left(\sum_{i,j,k,l}^{m}A_{ij}B_{kl}E_{ij}E_{kl}\right)\\ =& \phi\left(\sum_{i,j,l}^{m}A_{ij}B_{jl}E_{il}\right)\\ =& \sum_{i,l}^{m}E_{il}\otimes\sum_{j}^{m}A_{ij}B_{jl}\end{aligned}$$

Por outro lado,

$$\begin{aligned}\phi\left(\sum_{i,j}^{m} A_{ij}E_{ij}\right)\phi\left(\sum_{k,l}^{m} B_{kl}E_{kl}\right) &= \left(\sum_{i,j,k,l}^{m}(E_{ij}\otimes A_{ij})(E_{ij}\otimes B_{kl})\right)\\ &= \sum_{i,j,k,l}^{m}(E_{ij}\otimes A_{ij})(E_{kl}\otimes B_{kl})\\ &= \sum_{i,j,k,l}^{m} E_{ij}E_{kl}\otimes A_{ij}B_{kl}\\ &= \sum_{i,j,l}^{m} E_{il}\otimes A_{ij}B_{jl}\\ &= \sum_{i,l}^{m} E_{il}\otimes \sum_{j}^{m} A_{ij}B_{jl}\end{aligned}$$

Também, ϕ é unitária pois

$$\phi(1_{Mat_m(Mat_n(R))}) = \phi\left(\sum_{i}^{m} I_nE_{ii}\right) = \sum_{i}^{m} E_{ii}\otimes I_n =$$

$$\left(\sum_{i}^{m} E_{ii}\right)\otimes I_n = I_m\otimes I_n = 1_{Mat_m(R)\otimes Mat_n(R)}.$$

(Usaremos agora as notações E_{ij}^n, E_{kl}^m e E_{rs}^{mn} para os elementos das bases de $Mat_n(R)$, $Mat_m(Mat_n(R))$ e de $Mat_{mn}(R)$ respectivamente.)

Além do mais, ϕ é sobrejetora, já que todos os elementos de $Mat_m(R)\otimes Mat_n(R)$ são da forma $\sum\limits_{i,j,k,l} a_{i,j,k,l}(E_{ij}^m\otimes E_{kl}^n)$, mas

$$\begin{aligned}\sum_{i,j,k,l} a_{i,j,k,l}(E_{ij}^m\otimes E_{kl}^n) &= \sum_{k,l}^{n}\left(\sum_{i,j}^{m} a_{i,j,k,l}(E_{ij}^m\otimes E_{kl}^n)\right)\\ &= \sum_{k,l}^{n}\left(\sum_{i,j}^{m} a_{i,j}E_{ij}^m\right)\otimes E_{k,l}^n\\ &= \phi\left(\sum_{k,l}^{m}\left(\sum_{i,j}^{n} a_{i,j}E_{ij}^m\right)E_{k,l}^n\right).\end{aligned}$$

O núcleo de ϕ é 0 pois $\sum\limits_{i,j} A_{ij}\otimes E_{ij} = 0$ se, e somente se, A_{ij} é nulo para cada i,j, o que implica $\sum\limits_{i,j} A_{ij}E_{ij} = 0$.

Já para mostrar que $Mat_n(R)\otimes Mat_m(R)\cong Mat_{mn}(R)$, considere, primeiramente, a bijeção nos índices

$$\begin{array}{rccc}\phi: & [n]\times[m] & \longrightarrow & [mn]\\ & (i,k) & \longmapsto & (k-1)m+i\end{array}$$

Onde $[n] = \{1, 2, .., n\}$.

ϕ é injetora. De fato, considere $\phi(l, k) = \phi(t, r)$, isto é, $(k-1)m + l = (r-1)m + t$. Dessa igualdade, segue que $(k-r)m = (t-l)$, o que implica que m divide $t-l$. Mas, $1 \leq t$ e $l \leq m$, logo $|t-l| < m$. Portanto, temos que ter $k - r = t - l = 0$.

Como $|[n] \times [m]| = |[mn]| = mn$, segue que ϕ também é sobrejetora.

Defina agora a função:

$$\begin{array}{rccc} \varphi: & Mat_n(R) \otimes Mat_m(R) & \longrightarrow & Mat_{mn}(R) \\ & E^n_{ij} \otimes E^m_{kl} & \longmapsto & E^{mn}_{\phi(i,k)\phi(j,l)} \end{array}$$

φ está bem definida e é multiplicativa:

Por um lado,

$$(E^n_{a,b} \otimes E^m_{k,l}).(E^n_{c,d} \otimes E^m_{r,s}) = \delta_{b,c}\delta_{l,r}E^n_{a,d} \otimes E^m_{k,s}.$$

Por outro lado,

$$E^{mn}_{\phi(a,k)\phi(c,r)}.E^{mn}_{\phi(c,r)\phi(d,s)} = \delta_{\phi(b,l)\phi(c,r)}E^{mn}_{\phi(a,k)\phi(d,s)}$$

e $\phi(b, l) = \phi(c, r) \Leftrightarrow b = c$ e $l = r$.

Com isso, temos que $\varphi(\delta_{b,c}\delta_{l,r}E^n_{a,d} \otimes E^m_{k,s}) = \delta_{\phi(b,l)\phi(c,r)}E^{mn}_{\phi(a,k)\phi(d,s)}$.

φ também é bijetora. Como ϕ tem inversa

$$\begin{array}{rccc} \phi^{-1}: & [mn] & \longrightarrow & [n] \times [m] \\ & i & \longmapsto & (\phi_1^{-1}(i), \phi_2^{-1}(i)) \end{array}$$

segue que

$$E^{mn}_{ij} \to E^n_{\phi_1^{-1}(i)\phi_1^{-1}(j)} \otimes E_{\phi_2^{-1}(i)\phi_2^{-1}(j)}$$

define a inversa de φ.

Como φ é uma bijeção entre elementos das bases de $Mat_n(R) \otimes Mat_m(R)$ e $Mat_{mn}(R)$, então é um isomorfismo, o que conclui a prova. □

Corolário 3.23 *Sejam G um grupo finito e K um corpo algebricamente fechado tais que a característica de K não divida a ordem de G. Então, a álgebra parcial $K_{par}(G)$ é semissimples. Em particular, $\mathbb{C}_{par}(G)$ é semissimples para qualquer grupo finito G.*

Prova: Pelo teorema anterior, sabendo que $K_{par}(G) \cong K\Gamma(G)$, temos que

$$K_{par}(G) \cong \bigoplus_{\substack{H \leq G \\ 1 \leq m \leq (G:H)}} c_m(H) Mat_m(KH)$$

Pelo teorema de Molien, temos que cada álgebra de grupo KH é da forma:

$$KH = \bigoplus_{k=1}^{n} Mat_{r_k}(K)$$

onde n depende de H. Pela proposição anterior, temos

$$Mat_m(KH) = Mat_m\left(\bigoplus_{k=1}^{n} Mat_{r_k}(K)\right) \cong \bigoplus_{k=1}^{n} Mat_m(Mat_{r_k}(K)) \cong \bigoplus_{k=1}^{n} Mat_{mr_k}(K).$$

Segue, que $K_{par}(G)$ é uma soma direta de álgebras de matrizes com entradas em K, e aí, pela recíproca do Teorema de Wedderburn-Artin, $K_{par}(G)$ é semissimples. □

3.4 Exemplos de Álgebra Parcial de Grupo

Para apresentar mais alguns exemplos de álgebra parcial de grupo precisamos manter a seguinte notação: $b_m(H)$ indica o número de vértices de $E_{\Gamma(G)}$ no nível $k = m.|H|$ cujo estabilizador é H. Então, o somando direto de $K\Gamma(G)$ correspondente às componentes destes vértices é

$$\frac{b_m(H)}{m} Mat_m(KH).$$

Note que, para todo grupo finito G, no nível $k = 1$, temos apenas um vértice, o vértice $A = (\{e\}, e)$, e, assim, $H = \{e\}$ e $m = 1$. Daí temos $b_1(\{e\}) = 1$. Portanto, a componente conexa correspondente à $H = \{e\}$ é

$$\frac{b_1(\{e\})}{1} Mat_1(Ke) = \frac{1}{1}(K) = K.$$

No nível $k = |G|$, temos $H = G$ e $m = 1$. Como o único vértice no nível $k = |G|$ é o vértice $A = (G, e)$, também temos $b_1(G) = 1$. Logo, a componente conexa correspondente à $H = G$ é

$$\frac{b_1(G)}{1} Mat_1(KG) = \frac{1}{1}(KG) = KG.$$

Assim, $K\Gamma(G)$ sempre contém um cópia de K e uma cópia da álgebra de grupo KG como somando diretos.

Também vale a pena recordar que o número de vértices no nível k em $E_{\Gamma(G)}$ é dado pela fórmula

$$\binom{|G|-1}{k-1}.$$

Exemplo 3.24 *Considere p um número primo e o grupo cíclico $G = \mathbb{Z}_p$ de ordem p. Como, para cada H subgrupo de G, a ordem de H divide a ordem de G, temos que $\mathbb{Z}_p$ não tem nenhum subgrupo não trivial. Assim, em cada nível $k < p$, os vértices de $E_{\Gamma(\mathbb{Z}_p)}$ tem estabilizador trivial, logo temos $m = k$ e, portanto, o somando direto correspondente à cada $k < p$ é*

$$\frac{1}{k}\binom{p-1}{k-1} Mat_k(K).$$

(Observe que para $k = 1$ temos o somando direto K na álgebra do grupoide.)

Assim, temos

$$K\Gamma(\mathbb{Z}_p) = \bigoplus_{k=1}^{p-1} \frac{1}{k}\binom{p-1}{k-1} Mat_k(K) \oplus K\mathbb{Z}_p.$$

Exemplo 3.25 *Considere novamente p um número primo e o grupo $G = \mathbb{Z}_p \times \mathbb{Z}_p$. Vejamos que o grupo $\mathbb{Z}_p \times \mathbb{Z}_p$ tem*

$$\frac{p^2-1}{p-1} = p+1$$

subgrupos não triviais, que podemos denotar por $H_1, H_2, ..., H_{p+1}$, com $H_i \cong \mathbb{Z}_p$ para todo $i = 1, 2, ..., p+1$:

Se H_i e H_j são dois subgrupos de ordem p distintos, então $H_i \cap H_j = \{0\}$. De fato, $H_i \cap H_j$ é um subgrupo de H_i, e de H_j também, e como H_i tem p elementos, ou $H_i \cap H_j = H_i$ ou $H_i \cap H_j = \{0\}$.

Se $H_1, H_2, ..., H_N$ são os subgrupos de ordem p de $G = \mathbb{Z}_p \times \mathbb{Z}_p$, temos que

$$G = \bigcup_{i=1}^{N} H_i,$$

pois cada elemento de G, diferente de 0, gera um subgrupo de ordem p e, portanto, pertence a algum dos H_i's. Como nesta união o elemento 0 aparece em cada um dos H_i's, temos que

$$p^2 = |G| = Np - N + 1$$

($Np - N = N(p-1)$ é o número de elementos na união $\bigcup_{i=1}^{N}(H_i \setminus \{0\})$) e, logo

$$N(p-1) = Np - N = p^2 - 1 \Rightarrow N(p-1) = (p-1)(p+1) \rightarrow N = p+1.$$

Os vértices de $E_{\Gamma(\mathbb{Z}_p\times\mathbb{Z}_p)}$ no nível k, para todo k não múltiplo de p, tem estabilizador trivial. Logo, os somandos diretos de $K\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p)$ correspondentes a estes níveis são

$$\bigoplus_{\substack{k=1\\ p\nmid k}}^{p^2-1} \frac{1}{k}\binom{p^2-1}{k-1} Mat_k(K).$$

Para $k = mp$, com $m = 1, 2, ..., p-1$, temos dois casos: o caso dos vértices que são estabilizados por H_i e os vértices que tem estabilizador trivial.

O número de vértice que tem estabilizador H_i pode ser calculado como

$$b_m(H_i) = \binom{(G:H)-1}{m-1} = \binom{p-1}{m-1}$$

Assim, os somandos diretos correspontes a tais álgebras, lembrando que $H_i \cong \mathbb{Z}_p$, é:

$$\bigoplus_{m=1}^{p-1} \frac{p+1}{m}\binom{p-1}{m-1} Mat_m(K\mathbb{Z}_p).$$

Os demais vértices no nível mp tem estabiliador trivial, e podemos calcular seu número como sendo

$$\begin{aligned} b_{mp}(\{e\}) &= \binom{|G|-1}{mp-1} - \sum_{i=1}^{p+1} b_m(H_i) \\ &= \binom{p^2-1}{mp-1} - (p+1)\binom{p-1}{m-1}, \end{aligned}$$

e os somandos diretos correspondentes a estas álgebras são

$$\bigoplus_{m=1}^{p-1} \frac{1}{mp}\left[\binom{p^2-1}{mp-1} - (p+1)\binom{p-1}{m-1}\right] Mat_{mp}(K).$$

Por fim, juntando todas os somandos diretos, temos

$$\begin{aligned} K\Gamma(\mathbb{Z}_p \times \mathbb{Z}_p) \cong & \bigoplus_{\substack{k=1\\ p\nmid k}}^{p^2-1} \frac{1}{k}\binom{p^2-1}{k-1} Mat_k(K) \bigoplus_{m=1}^{p-1} \frac{p+1}{m}\binom{p-1}{m-1} Mat_m(K\mathbb{Z}_p) \\ & \bigoplus_{m=1}^{p-1} \frac{1}{mp}\left[\binom{p^2-1}{mp-1} - (p+1)\binom{p-1}{m-1}\right] Mat_{mp}(K) \\ & \oplus K(\mathbb{Z}_p \times \mathbb{Z}_p) \end{aligned}$$

No caso particular de $K = \mathbb{C}$, temos que

Os fatores que aparecem são

$Mat_k(\mathbb{C})$*, para* $k = 1, 2, ..., p^2 - 1$*;*

$Mat_{mp}(\mathbb{C})$, *para* $m = 1, 2, ..., p-1$;

$Mat_m(\mathbb{C}\mathbb{Z}_p)$, *para* $m = 1, 2, ..., p-1$;

$\mathbb{C}(\mathbb{Z}_p \times \mathbb{Z}_p)$.

Os dois últimos fatores podem ser reescritos. Usando a proposição **??** *e e observando que se* G *é abeliano de ordem* n *então* $\mathbb{C}G \cong n\mathbb{C}$*, teremos*

$Mat_m(\mathbb{C}\mathbb{Z}_p) \cong Mat_m(p\mathbb{C}) \cong pMat_m(\mathbb{C})$;

$\mathbb{C}(\mathbb{Z}_p \times \mathbb{Z}_p) \cong p^2\mathbb{C}$.

Assim, os fatores que aparecem na decomposiçao de Wedderburn-Artin são

$\mathbb{C}$;

$Mat_r(\mathbb{C})$ *com* $r = 1, 2, ..., p-1$;

$Mat_r(\mathbb{C})$ *com* $r = mp$ *e* $m = 1, 2, ..., p-1$.

Exemplo 3.26 *Sejam* p *e* q *dois primos distintos. Considere* $G = \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$*. O grupo* G *tem dois subgrupos não triviais, isomorfos à* $\mathbb{Z}_p$ *e* $\mathbb{Z}_q$*, ambos maximais. Podemos dividir nosso problema em três casos: o primeiro para* k *não múltiplo de* p *e nem* q*, o segundo para* k *múltiplo de* p *e o terceiro para* k *múltiplo de* q*. Assim, usando os mesmos argumentos do exemplo anterior, temos:*

$$
\begin{aligned}
K\Gamma(\mathbb{Z}_p \times \mathbb{Z}_q) \cong & \bigoplus_{\substack{k=1 \\ p,q\nmid k}}^{pq-1} \frac{1}{k}\binom{pq-1}{k-1} Mat_k(K) \\
& \bigoplus_{m=1}^{p-1} \frac{1}{m}\binom{p-1}{m-1} Mat_m(K\mathbb{Z}_q) \bigoplus_{m=1}^{q-1} \frac{1}{m}\binom{q-1}{m-1} Mat_m(K\mathbb{Z}_p) \\
& \bigoplus_{m=1}^{p-1} \frac{1}{mq}\left[\binom{pq-1}{mq-1} - \binom{p-1}{m-1}\right] Mat_{mq}(K) \\
& \bigoplus_{m=1}^{q-1} \frac{1}{mp}\left[\binom{pq-1}{mp-1} - \binom{q-1}{m-1}\right] Mat_{mp}(K) \\
& \oplus K(\mathbb{Z}_p \times \mathbb{Z}_q)
\end{aligned}
$$

Exemplo 3.27 *Tome* p *primo e considere o grupo* $\mathbb{Z}_{p^2}$ *que tem apenas um subgrupo não trivial,* $\mathbb{Z}_p$*. Então recaímos em dois casos dos exemplos anteriores, o caso em que* k *não é múltiplo de* p *e o caso em que é múltiplo de* p*. Usando o mesmo raciocínio anterior, temos:*

$$K\Gamma(\mathbb{Z}_{p^2}) \cong \bigoplus_{\substack{k=1 \\ p\nmid k}}^{p^2-1} \frac{1}{k}\binom{p^2-1}{k-1} Mat_k(K) \bigoplus_{m=1}^{p-1} \frac{1}{m}\binom{p-1}{m-1} Mat_m(K\mathbb{Z}_p)$$
$$\bigoplus_{m=1}^{p-1} \frac{1}{mp}\left[\binom{p^2-1}{mp-1} - \binom{p-1}{m-1}\right] Mat_{mp}(K)$$
$$\oplus\, K(\mathbb{Z}_{p^2})$$

Para $K = \mathbb{C}$, os fatores são

$Mat_k(\mathbb{C})$ *para* $k = 1, 2, ..., p^2 - 1$*;*

$Mat_{mp}(\mathbb{C})$ *para* $m = 1, 2, ..., p - 1$*;*

$Mat_m(\mathbb{C}\mathbb{Z}_p)$ *para* $m = 1, 2, ..., p - 1$*;*

$\mathbb{C}\mathbb{Z}_{p^2}$.

Traduzindo o terceiro e quarto fator, temos

$Mat_m(\mathbb{C}\mathbb{Z}_p) \cong pMat_m(\mathbb{C})$ *e*

$\mathbb{C}(\mathbb{Z}_{p^2}) \cong p^2\mathbb{C}$.

Como no caso anterior de $G = \mathbb{Z}_p \times \mathbb{Z}_p$. Portanto os fatores na decomposição de Wedderburn-Artin são os mesmos.

Olhando com cuidado, vê-se que apenas os termos listados como $Mat_{mp}(\mathbb{C})$ na decomposição apresentada nos exemplos contribuem com termos $Mat_{mp}(\mathbb{C})$ na decomposiçao de Wedderburn-Artin. Comparando as multiplicidades do termo $Mat_{mp}(\mathbb{C})$ nas decomposições relativas a $\mathbb{Z}_p \times \mathbb{Z}_p$ e $\mathbb{Z}_{p^2}$ vê-se que elas não são as mesmas para nenhum $m = 1, 2..., p - 1$.

Como a multiplicidade de um fator na decomposicao de Wedderburn-Artin de uma álgebra semissimples é invariante, segue que $K_{par}(\mathbb{Z}_p \times \mathbb{Z}_p)$ e $K_{par}(\mathbb{Z}_{p^2})$ não são isomorfos. Este é, na verdade, um caso particular do teorema 4.4 [4], que segue enunciado abaixo

Teorema 3.28 *Sejam G e H dois grupos abelianos finitos e K um corpo cuja característica não divide $|G|$ tais que as álgebras parciais $K_{par}(G)$ e $K_{par}(H)$ são isomorfas. Então G e H são grupos isomorfos.*

Exemplo 3.29 *Retornando ao caso de $G = S_3$, na seção anterior calculamos*

$$K\Gamma(S_3) \cong K \oplus Mat_2(K) \oplus 3Mat_3(K) \oplus Mat_4(K) \oplus Mat_5(K) \oplus$$
$$\oplus\, 3K\mathbb{Z}_2 \oplus K\mathbb{Z}_3 \oplus 3Mat_2(K\mathbb{Z}_2) \oplus KS_3.$$

No caso particular de $K = \mathbb{C}$, utilizando o teorema de Molien e a proposição **??**, *temos que*

$$\mathbb{C}\mathbb{Z}_2 \cong Mat_1(\mathbb{C}) \oplus Mat_1(\mathbb{C}) \cong \mathbb{C} \oplus \mathbb{C} = 2\mathbb{C}$$

$$\mathbb{C}\mathbb{Z}_3 \cong Mat_1(\mathbb{C}) \oplus Mat_1(\mathbb{C}) \oplus Mat_1(\mathbb{C}) \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} = 3\mathbb{C}$$

$$Mat_2(\mathbb{C}\mathbb{Z}_2) \cong Mat_2(\mathbb{C} \oplus \mathbb{C}) \cong Mat_2(\mathbb{C}) \oplus Mat_2(\mathbb{C}) = 2Mat_2(\mathbb{C})$$

$$\mathbb{C}S_3 \cong Mat_1(\mathbb{C}) \oplus Mat_1(\mathbb{C}) \oplus Mat_2(\mathbb{C}) \cong \mathbb{C} \oplus \mathbb{C} \oplus Mat_2(\mathbb{C})$$

Daí,

$$\mathbb{C}\Gamma(S_3) \cong 12\mathbb{C} \oplus 8Mat_2(\mathbb{C}) \oplus 3Mat_3(\mathbb{C}) \oplus Mat_4(\mathbb{C}) \oplus Mat_5(\mathbb{C})$$

Referências Bibliográficas

[1] ASSEM, I. ***Algèbres et modules***. Ed. Masson, 1997.

[2] BIRGET, J.; RHODES, J. ***Almost finite expansions of arbitrary semigroups***. Journal of Pure and Applied Algebra, 32 (1984), pg239-287.

[3] DOKUCHAEV, M.; EXEL R., ***Associativity of crossed products by partial actions, enveloping actions and partial representations***. Transactions of the American Mathematical. Society 357 (2005), pg1931-1952.

[4] DOKUCHAEV, M.; EXEL R.; PICCIONE, P., ***Partial Representations and Partial Group Algebras***. Journal of Algebra 226, (2000), pg505-532.

[5] EXEL, R. ***Partial actions of groups and actions of inverse semigroups***. Proceedings of the American Mathematical Society 126 (1998), no. 12, pg3481-3494.

[6] EXEL, R. ***Circle actions on C^*-algebras, partial automorphisms, and a generalized Pimsner-Voiculescu exact sequence***. Journal of Funcional Analysis, 122 (1994), pg361-401.

[7] FLÔRES,D.; PAQUES, A. ***Duality for groupoid (co)actions***. (2012)

[8] HOWIE, J. M. ***An introduction to semigroup theory***. L.M.S. monographs, Academic Press, (1976).

[9] KELLENDONK, J.; LAWSON, M. V. ***Partial actions of groups*** International Journal of Algebra and Computation Vol. 14, (2004), no. 1, pg87-114.

[10] MAKUTA, T. M. B. ***Cohomologia para ações parciais de grupos***. Dissertação em Matemática, Programa de Pós-Graduação em Matemática Aplicada, Universidade Federal do Paraná, Curitiba, (2015).

[11] RENAUT, J. ***A groupoid approach to C^*-algebras***. Springer-Verlag, (1980).

[12] ROTMAN, J. J. ***Advanced Modern Algebra***. Prentice Hall. 2nd printing. (2003), 1040p.

[13] SZENDREI, M. B. ***A note on BIRGET-RHODES expansion of groups***. Journal of Pure and Applied Algebra no.58 (1989), pg93-99.